ComCERT

APATOR

# EKSPERTYZA

## Zagrożenia dla cyberbezpieczeństwa inteligentnych sieci w Polsce w związku z rolloutem liczników smart

wraz z rekomendacjami w zakresie przeciwdziałania zagrożeniom

Materiał ekspercki powstał we współpracy ComCERT SA i Apator SA
sierpień 2023 r.

# 1. PODSUMOWANIE ZARZĄDCZE

1. W Polsce trwa masowa wymiana liczników energii elektrycznej na urządzenia ze zdalnym odczytem (LZO). Do 2028 roku zostanie zamontowanych w sieci energetycznej ok. 16 mln liczników wyposażonych w moduł komunikacyjny. Z zainstalowanych do tej pory ok. 4 mln urządzeń ponad połowa pochodzi spoza EOG, od dostawców niezweryfikowanych pod kątem cyberbezpieczeństwa.
2. Najbliższe miesiące będą decydujące dla przyszłości i bezpieczeństwa inteligentnych sieci w Polsce. Brak regulacji w zakresie cyberbezpieczeństwa liczników LZO stosowanych w sektorze energii stanowi poważne zagrożenie dla stabilności i bezpieczeństwa całego systemu.
3. Istnieje pilna potrzeba działania ze strony Polskiego Rządu i powołanych do tego celu instytucji i służb, aby stworzyć optymalne warunki dla transformacji energetycznej, która wymaga bezpiecznej, odpornej na cyfrowe zagrożenia infrastruktury energetycznej.
4. Suwerenność technologiczna powinna być uwzględniona w procesie transformacji energetycznej na tych samych zasadach, jak w przypadku technologii informatycznych.
5. Postępujący proces transformacji energetycznej pociąga za sobą konieczność digitalizacji sektora, będącej warunkiem jego dynamicznego rozwoju, a jednocześnie rodzącej wyzwania związane z odpornością na fizyczne i cyfrowe zagrożenia.
6. Technologie teleinformatyczne były, są i będą przedmiotem ataków grup przestępczych, aktorów sponsorowanych przez państwa lub wprost przez służby nieprzyjaznych państw.
7. Liczniki inteligentne są istotnym ogniwem w łańcuchu zaopatrzenia w energię elektryczną, a ich zdalne lub zaplanowane zakłócenie może wywołać rozległe awarie energetyczne w sieciach dystrybucyjnych, wpływając negatywnie na duże grupy odbiorców i przedsiębiorstw.
8. Największym i niezaadresowanym obecnie w Polsce ryzykiem w kontekście liczników inteligentnych jest atak na łańcuch dostaw – implementacja backdoorów lub bomb logicznych w licznikach dostarczanych operatorom systemów dystrybucyjnych (OSD).
9. Motywacje i zasoby, by taki atak przeprowadzić, mają państwa rywalizujące, nieprzychylne lub wręcz wrogie szeroko rozumianemu Zachodowi, które sukcesywnie zwiększają swoją pozycję na polskim rynku zaawansowanej infrastruktury pomiarowej (AMI, z ang. Advanced Metering Infrastructure). W obserwowanych ostatnio przetargach ich obecność jest wręcz dominująca.
10. Dyrektywa NIS2 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (konieczność implementacji w Polsce do października 2024 roku), wymaga zapewnienia bezpieczeństwa łańcucha dostaw przez wszystkie podmioty należące do tzw. grupy podmiotów kluczowych, do których należą OSD.
11. Środowisko europejskich dostawców i ekspertów ds. cyberbezpieczeństwa (poparte również stanowiskiem Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji z dn. 4.08.2023 r.[1]) apelują o przygotowanie propozycji zmian legislacyjnych w zakresie cyberbezpieczeństwa, z uwzględnieniem bezpieczeństwa łańcucha dostaw liczników inteligentnych.
12. W związku z długim czasem przygotowania i implementacji przedmiotowych regulacji oraz koniecznością podjęcia PILNYCH działań, uzasadnione jest przyjęcie w okresie przejściowym mechanizmów nieregulacyjnych (na wzór innych rynków europejskich). Mogą nim być rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa, które służą zwróceniu uwagi i przeciwdziałaniu konkretnym, realnym zagrożeniom dla kluczowej infrastruktury państwa.

**Rekomendacja, aby w krajowym systemie energetycznym nie stosować urządzeń lub oprogramowania pochodzących spoza Europejskiego Obszaru Gospodarczego mogłaby w znaczący sposób zredukować ryzyko dla łańcucha dostaw liczników zdalnego odczytu i przyczynić się do bezpieczeństwa krajowej sieci energetycznej w dzisiejszym, niezwykle wymagającym i niepewnym otoczeniu geopolitycznym i makroekonom**

1 https://kigeit.org.pl/FTP/if/SIS-SG/230804_Stanowisko_KIGEiT_Bezp_liczn_e.e.pdf - dostęp 12.09.2023 r.

# 2. WSTĘP

W wydanych przez Ministerstwo Środowiska i Klimatu "Rekomendacjach dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytycznych sektorowych dotyczących zgłaszania incydentów" można przeczytać m.in.: "Rozwój polskiej energetyki oraz postępujący proces jej informatyzacji, skutkuje większą podatnością świadczonych usług na zagrożenia cyberbezpieczeństwa. Zmiany Prawa energetycznego, wprowadzone w 2021 r. określają nie tylko kierunek rozwoju polskiego systemu energetycznego, ale także umożliwią dalszą bezpieczną integrację odnawialnych źródeł energii w systemie oraz wykorzystanie synergii w sektorze – w tym, zwiększenie elastyczności systemu energetycznego oraz wykorzystanie potencjału aktywnych odbiorców. Dodatkowo, należy wspomnieć o zaproponowanych kompleksowych rozwiązaniach usuwających bariery prawne dla rozwoju magazynów energii umożliwiające dalszy rozwój energetyki rozproszonej (prosumenckiej) i OZE (odnawialne źródła energii).
Jednakże, co kluczowe z punktu widzenia cyberbezpieczeństwa, przygotowane rozwiązania są niezbędnym punktem wyjścia do **transformacji sektora energetycznego, opartej między innymi o jego cyfryzację, inteligentne sieci i inteligentne liczniki zdalnego odczytu,** a także tworzą ramy prawne dla funkcjonowania systemu inteligentnego opomiarowania w elektroenergetyce. Inwestycje w rozwój inteligentnych sieci, w tym liczniki zdalnego odczytu, stanowią ogólny kierunek przyjęty w Unii Europejskiej, skutkujący powstaniem obowiązku instalacji przez operatorów systemów dystrybucyjnych do końca 2028 roku liczników inteligentnych u co najmniej 80% odbiorców końcowych"[2].

W kontekście transformacji energetycznej pojawia się również zagadnienie suwerenności technologicznej jako jednego z wielu wyzwań, które powinny być uwzględnione w tym procesie. Celami niniejszego dokumentu jest diagnoza zjawiska **suwerenności technologicznej w kontekście bezpieczeństwa energetycznego Polski,** a w szczególności analiza, jak technologiczna suwerenność manifestuje się w sektorze energetycznym na przykładzie inteligentnych liczników energii, jakie wynikają z tego zagrożenia i ryzyko dla Krajowego Systemu Elektroenergetycznego oraz przedstawienie propozycji minimalizacji tego ryzyka.

Dokument nie jest skierowany przeciwko jakiejkolwiek firmie. Przedstawia obiektywnie rosnące ryzyko dla łańcucha dostaw bez względu na kraj pochodzenia dostawcy lub jego powiązania biznesowe.

- **Rozdział 2** przedstawia najważniejsze wnioski stanowiące podsumowanie analiz przeprowadzonych w niniejszym dokumencie.

- **Rozdział 3** przedstawia definicję suwerenności technologicznej oraz wyzwania związane z wdrażaniem nowych technologii w sektorze elektroenergetycznym.

- **Rozdział 4** zawiera główne zagrożenia, które mogą wpływać na stabilność, niezawodność oraz bezpieczeństwo Krajowego Systemu Elektroenergetycznego. Przedstawiono w nim również największe ataki, które były przeprowadzone na przedsiębiorstwa sektora energetycznego na przestrzeni ostatnich lat. Rozdział zawiera również informacje nt. czynników ryzyka i potencjalnych skutków udanego ataku zagrażających cyberbezpieczeństwu sektora energetycznego.

- **Rozdział 5** przedstawia analizę możliwych wektorów ataku na system dystrybucji energii elektrycznej, w których wykorzystane mogą zostać inteligentne urządzenia pomiarowe. W rozdziale zawarto również podsumowanie analizy, w których zestawiono obecnie istniejące środki ochrony przeciw potencjalnemu typowi ataku oraz jego potencjalne następstwa.

2 https://www.gov.pl/web/klimat/rekomendacje-dotyczace-dzialan-majacych-na-celu-wzmocnienie-cyberbezpieczenstwa-w-sektorze-energii-oraz-wytyczne-sektorowe-dotyczace-zglaszania-incydentow - dostęp 23.08.2023 r.

- **Rozdział 6** zawiera propozycje minimalizacji ryzyka związanego z łańcuchem dostaw. Propozycja została opracowana z wykorzystaniem techniki SWOT.

- **Rozdział 7** zawiera rekomendowane działania w zakresie minimalizacji ryzyka związanego z łańcuchem dostaw. Zostały one podzielone na działania do zrealizowania w bliskiej oraz długiej perspektywie czasowej.

- **Rozdział 8** zawiera apel o podjęcie działań na rzecz poprawy cyberbezpieczeństwa w sektorze energetycznym.

W niniejszym dokumencie pojęcia: inteligentny licznik energii, licznik zdalnego odczytu (LZO), licznik smart są stosowane zamiennie.

# 3. SUWERENNOŚĆ TECHNOLOGICZNA

W związku z trudną sytuacją geopolityczną i niepewnością z niej wynikającą, wzmocnioną agresją Rosji w Ukrainie, wzmogła się ostatnio, tocząca się na świecie od kilku lat, dyskusja na temat suwerenności technologicznej.

Pojęcie „suwerenności technologicznej" nie jest nowe, ale jego precyzyjne zdefiniowane stanowi kwestię sporną. Przez niektórych postrzegana jest głównie jako zachowanie kontroli nad kluczowymi sektorami gospodarki (w ujęciu strategii gospodarczej), dla innych natomiast najistotniejsze są niezależność, kontrola i autonomia w zakresie technologii i rozwiązań produkcyjnych (ujęcie techniczno-technologiczne).

W opracowaniu European Sovereignty Index[3], przygotowywanym przez The European Council on Foreign Relations (ECFR), suwerenność technologiczna zdefiniowana jest jako: „zdolność do kształtowania krytycznych technologii zgodnie z interesami i wartościami Unii Europejskiej. UE byłaby suwerenna technologicznie, gdyby rozwijała konkurencyjne w skali światowej technologie krytyczne, skutecznie regulowała ich rozpowszechnianie i wykorzystywanie oraz unikała nadmiernej zależności od innych potęg w zakresie technologii, które są niezbędne dla jej dobrobytu gospodarczego, politycznego i społecznego".

Należy zatem przyjąć, że w ten sposób rozumiana suwerenność technologiczna oznacza nie tylko zdolność do opracowania i wdrożenia technologii wytworzenia w kraju wysoko zaawansowanych urządzeń lub produktów, niezależnie od zagranicznych dostawców, ale również zdolności podmiotu (kraju, organizacji lub społeczeństwa) do nadzorowania i zarządzania (w tym dystrybucją) swoimi technologiami, infrastrukturą oraz danymi w sposób możliwie niezależny i autonomiczny.

We wspomnianym wyżej opracowaniu indeks suwerenności UE był oceniany w 6 obszarach: klimat, obronność, gospodarka, zdrowie, migracje i technologia. W obszarze suwerenność technologiczna państwa członkowskie uzyskały średni wynik zaledwie 4,8 (ważony liczbą ludności) na 10[4]. To jest najniższy średni wynik ze wszystkich sześciu domen w indeksie. Warto dodać, że żaden z pięciu największych krajów UE – Niemcy, Francja, Włochy, Hiszpania i Polska – nie znalazł się pod tym względem w pierwszej trójce[5] .

Autorzy European Sovereignty Index, oceniając wkład państw członkowskich w europejską suwerenność technologiczną, skoncentrowali się na: sztucznej inteligencji, dużych zbiorach danych (big data), przetwarzaniu w chmurze, półprzewodnikach, robotyce, Internecie Rzeczy, obliczeniach o wysokiej wydajności, zaawansowanej telekomunikacji i cyberbezpieczeństwie. Jak widać, wszystkie brane pod uwagę dziedziny powiązane są z teleinformatyką. Wynika to, w opinii autorów, z faktu, że w coraz bardziej zdigitalizowanych gospodarkach i wzajemnie połączonych społeczeństwach technologie te odgrywają fundamentalną rolę w rozwoju gospodarczym i politycznym, zajmują centralne miejsce w rywalizacji technologicznej między wielkimi mocarstwami i ogólnie znajdują się w centrum europejskich dyskusji na temat suwerenności technologicznej.

Indeks mierzy zdolności technologiczne państw członkowskich oraz ich zaangażowanie w suwerenność technologiczną za pomocą wskaźników[6]. W przypadku zdolności technologicznych wzięte pod uwagę zostały m.in.:

- wkład w badania, patenty i standardy;
- liczba firm technologicznych i specjalistów;
- udziały rynkowe firm;
- inwestycje typu venture capital w ww. technologie;
- absorpcja technologii;

3 https://ecfr.eu/wp-content/uploads/2022/06/European-Sovereignty-Index.pdf oraz https://ecfr.eu/special/sovereignty-index/ - dostęp 19.08.2023 r.
4 Polska w tej domenie uzyskała średni wynik na poziomie 3,6 – tamże
5 Polska plasuje się na końcu stawki – w ostatniej piątce, a wyprzedzają nas np. Słowenia, Grecja i Litwa
6 Lista wskaźników jest dostępna po rozwinięciu w części dotyczącej obszaru technologii: https://ecfr.eu/special/sovereignty-index/#terrain-technology – dostęp 19.08.2023 r.

- zdolności w obszarze cyberbezpieczeństwa.

Natomiast zaangażowanie w suwerenność technologiczną oceniane jest za pomocą m.in.:

- stanowisk w sprawie przepisów UE i współpracy;
- zaangażowania na międzynarodowych forach technologicznych;
- udziału w europejskich badaniach i rozwoju;
- wkładzie w międzynarodowe inicjatywy technologiczne UE;
- danych sondażowych dotyczących społecznego poparcia dla rozwoju technologicznego.

Temat suwerenności technologicznej szczególnie gorąco był omawiany wraz z debatą dotyczącą technologii 5G (zaistniał również w świadomości polityków i szerszej opinii publicznej). Można zaryzykować twierdzenie, że debaty prowadzone na szczeblu Unii Europejskiej oraz w polskiej przestrzeni publicznej otworzyły oczy na to zagadnienie i realne zagrożenia płynące z niedostrzegania lub koncentracji wyłącznie na aspekcie ekonomicznym wdrażanych w krajach zachodnich technologii. W rezolucji Parlamentu Europejskiego z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(rsp))[7] można przeczytać, że:

- nie ma gwarancji, iż przepisy obowiązujące podmioty oferujące technologię 5G w państwach pochodzenia[8] nie są stosowane eksterytorialnie i mogą zagrażać bezpieczeństwu UE,
- centra kompetencji w dziedzinie cyberbezpieczeństwa i sieci krajowych ośrodków koordynacji powinny wspierać UE w utrzymaniu i rozwoju zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa, niezbędnych do zabezpieczenia jednolitego rynku cyfrowego UE,
- należy kontynuować pracę nad stworzeniem systemu certyfikacji sprzętu (w tym przypadku 5G),
- certyfikacja nie powinna wykluczać monitorowania łańcucha dostaw przez właściwe organy i operatorów w celu zapewnienia integralności i bezpieczeństwa urządzeń działających w krytycznych środowiskach i sieciach telekomunikacyjnych.

Wyzwania związane z wdrażaniem nowych technologii zostały również dostrzeżone w sektorze elektroenergetycznym. Już na początku poprzedniej dekady została wydana seria stanowisk Prezesa Urzędu Regulacji Energetyki w sprawie niezbędnych wymagań wobec wdrażanych przez OSD E inteligentnych systemów pomiarowo-rozliczeniowych tzw. stanowisk ws. AMI[9]. W stanowiskach tych system AMI (z ang. Advanced Metering Infrastructure – zaawansowana infrastruktura pomiarowa) zostały zdefiniowane jako: „System pomiarowo-rozliczeniowy, składający się z aplikacji centralnej, infrastruktury komunikacji dwukierunkowej, infrastruktury pomiarowej oraz pozostałych elementów służących do zdalnego pomiaru, przesyłania, przechowywania i przetwarzania danych pomiarowych dotyczących energii elektrycznej oraz ewentualnie innych mediów, a także stosownych informacji i komend". Cechami charakterystycznymi AMI (odróżniającą od AMR – automatycznego odczytu liczników) są[10]:

- możliwość komunikacji dwukierunkowej z licznikiem,
- gotowość do współpracy z siecią inteligentnego domu HAN (z ang. Home Area Network),
- większa złożoność sieci,
- możliwość współpracy z siecią inteligentną (Smart Grid).

Powiązanie zagadnienia suwerenności technologicznej i bezpieczeństwa Krajowego Systemu Elektroenergetycznego (KSE) w kontekście inteligentny liczników będzie przedmiotem rozważań w kolejnych rozdziałach niniejszego dokumentu.

7 Dz. Urz. UE. C z dnia 21 stycznia 2021 r. nr 23, str. 2 - https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:C:2021:023:FULL&from=NL – dostęp 14.08.2023 r.

8 Rezolucja odwołuje się do przykładu chińskiej ustawy o bezpieczeństwie państwowym, która zobowiązuje wszystkich obywateli, przedsiębiorstwa i inne podmioty do współpracy z państwem w ochronie bezpieczeństwa państwowego, w powiązaniu z bardzo szeroką definicją bezpieczeństwa narodowego – tamże

9 Np. stanowiska Prezesa URE z 31.05.2011 r., 10.07.2013 r.

10 https://pl.wikipedia.org/wiki/Zaawansowana_infrastruktura_pomiarowa

# 4. ZNACZENIE CYBERBEZPIECZEŃSTWA W ENERGETYCE

Krajowy System Elektroenergetyczny (KSE) to ""system systemów", łączący w sobie systemy (lub podsystemy) wytwarzania, przesyłu, dystrybucji oraz poboru energii elektrycznej. Istnieje wiele różnych zagrożeń, które mogą wpływać na stabilność, niezawodność i bezpieczeństwo KSE. Część z nich to zagrożenia związane z warstwą techniczną, pogodową, inne dotyczą kwestii geopolitycznych, a jeszcze inne umiejętności administrowania nią. Niektóre z głównych zagrożeń to:

- **Awaria infrastruktury:** Uszkodzenie elementów infrastruktury, takich jak linie przesyłowe, stacje transformatorowe czy generatory, może prowadzić do przerw w dostawie energii, zwłaszcza jeśli nie ma wystarczających systemów zabezpieczających i rezerwowych. W przypadku awarii istotna jest pierwotna przyczyna jej wystąpienia, ponieważ może to być zarówno defekt sprzętu spowodowany jego wadą, jak również sabotaż, którego skutkiem będzie techniczne stwierdzenie awarii. Wystąpienie awarii lub zakłóceń w jednym obszarze sieci może mieć efekt kaskadowy na inne obszary, co może prowadzić do rozległych terytorialnie przerw w dostawie energii.
- **Zdarzenia pogodowe:** Warunki pogodowe, takie jak burze, wichury, opady deszczu lub śniegu, mogą powodować uszkodzenia infrastruktury energetycznej i przerwy w dostawie energii.
- **Zakłócenia elektromagnetyczne:** Wybuchy elektromagnetyczne, spowodowane na przykład przez burze słoneczne lub wybuchy jądrowe, mogą zakłócać pracę systemu energetycznego, uszkadzać urządzenia elektroniczne i powodować awarie. Należy w tym wypadku wziąć pod uwagę również możliwość wykorzystania technologii wojskowych służących do walki radioelektronicznej.
- **Niezbilansowanie systemu:** W okresach dużego zapotrzebowania na energię mogą występować niedobory mocy, co może prowadzić do konieczności wprowadzania ograniczeń w dostawie energii lub nawet do awarii.
- **Zależność od importu/eksportu:** Polska importuje/eksportuje część energii elektrycznej, co naraża ją na ryzyko zakłóceń w dostawie/odbiorze energii z zagranicy, co z kolei może wpływać na destabilizację KSE.
- **Starzenie się infrastruktury:** Część infrastruktury energetycznej jest przestarzała, nie odpowiada aktualnym warunkom i wymaganiom pracy KSE oraz wymaga modernizacji. Niedopasowanie do nowoczesnych standardów lub zastosowanie nieodpowiednich, niesprawdzonych rozwiązań może zwiększać ryzyko awarii i zakłóceń.

Najważniejszym aspektem bezpieczeństwa KSE jest utrzymanie stabilności sieci (zbilansowania). Inteligentne systemy monitorowania i zarządzania mogą pomóc w przewidywaniu i dostosowywaniu się do zmian w produkcji i konsumpcji energii elektrycznej, a także we wdrożeniu elastycznych mechanizmów, takich jak awaryjne odłączenia odbiorów, aby zapobiegać przeciążeniu sieci. Jednakże wdrożenie na szeroką skalę inteligentnych systemów monitorowania i zarządzania generuje nowe zagrożenia, wynikające z samej tej technologii. Masowe odłączenie odbiorców ze względu na awarię lub też celowe działania aktorów zewnętrznych może skutkować niestabilnością, a w przypadku braku wystarczających mechanizmów regulacyjnych i zapasowych, może spowodować rozległą awarię systemową, zwaną potocznie blackoutem.

Wdrażanie technologii inteligentnych systemów monitorowania i zarządzania w sektorze energetycznym powoduje również ryzyko wynikające ze sprzecznych wymagań pomiędzy dążeniem do obniżenia kosztów a zapewnieniem bezpieczeństwa i skuteczności rozwiązań technologicznych. W celu osiągnięcia niższych kosztów, niektórzy dostawcy mogą decydować się na zastosowanie tańszych, niespełniających wymagań komponentów lub ograniczenie kosztów w obszarach związanych z bezpieczeństwem czy jakością. Takie postępowanie może prowadzić do awarii, cyberataków lub niskiej efektywności energetycznej. Właściwe wyważenie tych wymagań jest kluczowe dla zrównoważonego rozwoju sektora, zapewniając jednocześnie oszczędności i bezpieczeństwo dla użytkowników i infrastruktury państwowej. Dlatego dobrym rozwiązaniem wydaje się zastosowanie wymagań związanych z jakością i bezpieczeństwem (w tym cyberbezpieczeństwem) w procesie zamówień publicznych, co zostanie omówione w dalszej części niniejszego opracowania.

Cyberbezpieczeństwo stanowi kolejne istotne wyzwanie, które musi zostać uwzględnione w kontekście bezpieczeństwa KSE. Cyberzagrożenia to zagadnienie aktualne dla każdego sektora gospodarki, którego stopień cyfryzacji pozwala cyberprzestępcom na przeprowadzenie ataku w jakikolwiek sposób zakłócającego pracę tego sektora lub jego poszczególnych składowych. Sektor energetyczny jest jednak jedną z gałęzi gospodarki szczególnie narażoną na cyberataki, ponieważ jest on strategiczny dla funkcjonowania zarówno struktur państwowych, lokalnych, a nawet pojedynczych osób. Na przestrzeni ostatnich lat zarówno energetyka konwencjonalna, jak i odnawialna zdecydowanie zwiększyły swój stopień cyfryzacji, a co za tym idzie, także rozproszenia swoich struktur. Przedsiębiorstwa z sektora energetycznego należą do jednych z najczęściej atakowanych. Ataki te są najczęściej przeprowadzane przez aktorów wspieranych organizacyjnie i finansowo przez nieprzyjazne państwa i dążą do zakłócenia, a nawet zniszczenia infrastruktury związanej z procesem dystrybucji lub przesyłu energii elektrycznej. Do największych z nich możemy zaliczyć:

- 2001 r. – dostawca energii elektrycznej California Independent System Operator – atakujący uzyskali dostęp do jednej z wewnętrznych sieci. Atak wpłynął na sieć elektroenergetyczną ofiary zanim został wykryty, w efekcie powodując przerwę w dostawie energii elektrycznej dla ok. 400 tys. odbiorców. Prawdopodobnie był sponsorowany przez Chiny.
- 2003 r. – elektrownie nuklearna Davis-Besse w USA – atakujący wyłączył na cztery godziny system wyświetlający parametry pracy reaktorów przy pomocy oprogramowania złośliwego, nie wykradziono danych, brak danych o atrybucji.
- 2008 r. – elektrownia nuklearna Hatch w USA – błąd podczas aktualizacji oprogramowania zarządzającego doprowadził do błędu w systemie sterowania reaktorem, co doprowadziło do 2-dniowej przerwy w dostawie prądu, brak danych o atrybucji oraz o ewentualnym złośliwym oprogramowaniu (malware) wykorzystanym do ataku.
- 2014 r. – Korea Hydro and Nuclear Power (KHNP) w Korei Południowej – kradzież planów i instrukcji dwóch reaktorów, instalacji energetycznych oraz wyników pomiarów ekspozycji na promieniowanie w strefie, a także danych ponad 10 tys. pracowników koncernu. Atakujący następnie zażądał wyłączenia trzech reaktorów pod groźbą publikacji skradzionych materiałów.
- 2015 r. – trzech operatorów sieci dystrybucyjnej (OSD) w Ukrainie – ponad 50 podstacji elektroenergetycznych zostało odłączonych od sieci. Braki w zasilaniu dotknęły około 225 tys. odbiorców. System automatyki przemysłowej został fizycznie uszkodzony. Podstacje musiały być obsługiwane ręcznie przez kilka tygodni po zdarzeniu. Atakujący wykorzystał malware o nazwie BlackEnergy, atak prawdopodobnie sponsorowany przez Rosję.
- 2016 r. – operator sieci przesyłowej (OSP) w Ukrainie – celem ataku stała się część systemu odpowiedzialna za dostarczanie energii do ukraińskiej stolicy. Konsekwencją ataku były poważne ograniczenia w dostawach prądu dla tysięcy odbiorców w północnej części Kijowa. Atak prawdopodobnie sponsorowany przez Rosję, co wykazało przeprowadzone międzynarodowe śledztwo (w 2016 r. doszło również do podobnych ataków na sieć energetyczną w USA przeprowadzonych przez tego samego aktora).
- 2016 r. – sieci elektroenergetyczne w Izraelu – w wyniku ataku nie doszło do przerw w dostawach energii elektrycznej, jednak skompromitowano systemy rządowe związane z energetyką, brak atrybucji.
- 2020 r. – atak na dostawcę energii elektrycznej Energias de Portugal (EDP) – atak typu ransomware prawdopodobnie z wykorzystaniem skradzionych danych uwierzytelniających. Atakujący wykradli 10 TB danych, w tym dane osobowe klientów, brak atrybucji.
- 2022 r. – atak na amerykańskiego dostawcę energii elektrycznej Delta-Montrose Electric Association (DMEA) – w wyniku ataku dostawca był zmuszony do wyłączenia 90% infrastruktury IT, ze względu na bezpowrotną utratę danych. Atakujący usunęli bazy danych zawierające informacje z 25 lat funkcjonowania firmy, atrybucja nieznana.
- 2022 r. – seria ataków na turbiny wiatrowe różnych operatorów w Europie – w wyniku ataków jeden

z operatorów utracił połączenie z 6 tys. turbin wiatrowych, inny padł ofiarą ataku ransowmare, zaś kolejny na 24 godziny był zmuszony wyłączyć wszystkie urządzenia zarządzane zdalnie. Ataki te związane były prawdopodobnie z wybuchem wojny w Ukrainie i były realizowane przy wsparciu rosyjskim.

Należy zaznaczyć, że rozwój nowoczesnych technologii teleinformatycznych rodzi także zagrożenia na polu szpiegostwa. Władze amerykańskie przestrzegały rządy Niemiec przed wpuszczaniem zbyt dużej ilości chińskiego kapitału do swojej infrastruktury o charakterze krytycznym[11]. W marcu 2023 r. pojawiły się doniesienia o „koniu trojańskim w Hamburgu", gdy okazało się, że chińskie dźwigi kontenerowe pracujące w niemieckim porcie są wyposażone w zaawansowane czujniki, które mogą zbierać wrażliwe dane, w tym informacje o transportowanym sprzęcie wojskowym[12].
Jak podaje Check Point Research, liczba cyberataków na świecie jest najwyższa od 2 lat i wynosi średnio 1258 tygodniowo. Co istotne, w samym II kw. 2023 r. wzrosła o 8% w porównaniu do analogicznego okresu w roku ubiegłym. Za region o najwyższym wzroście ataków – ponad 21% – uznaje się Europę. Natomiast w samej Polsce w II kw. 2023 r. odnotowano o 33% więcej cyberincydentów niż w II kw. 2022 r.[13]

Wśród czynników ryzyka zagrażających cyberbezpieczeństwu sektora energetycznego zazwyczaj wymienia się takie, jak:

- duża dynamika cyfryzacji w sektorze energetycznym – transformacja systemów energetycznych niesie ze sobą konieczność wdrożenia szerszego dostępu do bezpiecznej energii. Proces ten jest realizowany na drodze rozwoju nowych technologii, które wnoszą dodatkowo nowy wektor cyberzagrożeń. Przykładem takich działań może być zastosowanie technologii Smart Grid, czyli inteligentnych sieci przesyłowych, które pozwolą na podniesienie efektywności systemu. Głównymi zaletami tego rozwiązania jest: poprawa bezpieczeństwa dostaw i niezawodności systemu elektroenergetycznego, możliwość informowania odbiorców o aktualnej cenie energii elektrycznej, ułatwienia rozwoju źródeł generacji rozproszonej i ich przyłączenia do sieci elektroenergetycznej, a także poprawa świadomości odbiorców w zakresie optymalizacji zużycia energii. Technologia ta umożliwia także zdalne wykrywanie awarii sieci oraz usuwanie problemów z tym związanych na bieżąco. Niestety jej największą wadą jest podatność na cyberataki. Z tej właśnie przyczyny konieczne jest opracowywanie i wdrażanie skutecznych strategii z dziedziny cyberbezpieczeństwa w każdej organizacji funkcjonującej w sektorze energetycznym.
- ataki teleinformatyczne (cyberataki) na zaawansowanym poziomie – wraz z ciągłym rozwojem technologii wzrasta także intensywność prób przeprowadzenia cyberataków oraz stopień ich zaawansowania. Cyberprzestępcy także korzystają z bardziej wyrafinowanych metod i narzędzi, tym samym ich działania są coraz trudniejsze do wykrycia w relatywnie krótkim okresie czasu. Ponadto wiele incydentów bezpieczeństwa to efekt działań zorganizowanych grup przestępczych specjalizujących się w cyberatakach, w tym sponsorowanych przez rządy (ataki APT). Jest to ogromne wyzwanie nie tylko dla samych przedsiębiorstw energetycznych, ale także dla podmiotów zajmujących się produkcją i dostawą urządzeń oraz oprogramowania wykorzystywanych w systemach energetycznych.
- sektor energetyczny jest atrakcyjnym celem ataku – energetyka to kluczowy element strategiczny w bezpieczeństwie państwa, ale także zapewnia ona bezpieczeństwo na poziomie lokalnym i indywidualnym. Fakt ten sprawia, że stanowi ona szczególnie kuszący cel dla cyberprzestępców gwarantujący, w przypadku udanego ataku, duże korzyści. To od sektora energetycznego, sprawnej dystrybucji energii zależy bowiem działalność praktycznie wszystkich podmiotów publicznych i gospodarczych.

11 https://www.euractiv.pl/section/gospodarka/news/czy-chinskie-dzwigi-szpieguja-port-w-hamburgu/ - dostęp 17.08.2023 r.
12 https://wgospodarce.pl/informacje/124564-chinskie-dzwigi-szpieguja-kon-trojanski-w-hamburgu - dostęp 17.08.2023 r.
13 https://crn.pl/aktualnosci/najwyzszy-poziom-cyberatakow-od-dwoch-lat/ - dostęp 07.08.2023 r.

Skutków udanego cyberataku, którego celem jest system energetyczny, może być wiele – podmiot będący ofiarą ataku zmierzy się z pewnością z konsekwencjami prawnymi, finansowymi oraz reputacyjnymi. Konsekwencje te należy rozpatrywać także w kategoriach ekonomicznych, a nawet politycznych. Atakujący pragną osiągnąć cele, które w przypadku sektora energetycznego mogą być scharakteryzowane następująco:

- osiągnięcie korzyści finansowych – najczęściej okup, jaki podmioty sektora energetycznego zapłacą za odzyskanie dostępu do strategicznych systemów zarządzania, systemów dystrybucji i systemów usług;
- destabilizacja i wywołanie niepokojów społecznych poprzez atak na struktury przemysłu energetycznego odpowiedzialne za dostarczanie energii elektrycznej i cieplnej odbiorcom instytucjonalnym i prywatnym. Działania takie mają zazwyczaj za zadanie wpłynąć negatywnie na gospodarkę państwa lub wywołać kryzys polityczny. Są one często inicjowane na zlecenie wrogich temu państwu rządów lub organizacji;
- wywołanie pożądanej dla atakującego, a niekorzystnej dla poszczególnych podmiotów energetycznych, sytuacji na giełdach. Cyberataki mogą być elementem wojen biznesowych pomiędzy konkurencyjnymi instytucjami;
- generowanie strat finansowych w przedsiębiorstwach energetycznych, których celem jest zachwianie rynkową pozycją instytucji, osłabienie w stosunku do jej usług zaufania społecznego ze strony klientów;
- kradzież własności intelektualnej.

Najistotniejsze wydają się jednak skutki społeczne. Poziom uzależnienia odbiorców indywidualnych oraz całych gałęzi przemysłu od energii elektrycznej sprawia, że rozległa awaria systemowa (blackout) spowodowana skutecznym cyberatakiem, może natychmiastowo dotknąć wielu milionów ludzi oraz zakłócić działanie/dostawy niezbędnych do funkcjonowania współczesnych społeczeństw usług np. zaopatrzenia w wodę i odprowadzania ścieków, systemu ochrony zdrowia, transportu zbiorowego, telekomunikacji. Współczesne gospodarstwa domowe coraz bardziej polegają na energii elektrycznej, co jest wynikiem dynamicznego rozwoju technologii domowego użytku, a jednocześnie wzrastającej w społeczeństwie świadomości ekologicznej. W ostatnim czasie tendencje przechodzenia na energię elektryczną zostały wzmocnione ryzykiem związanym z dostawami paliw gazowych w związku z konfliktem za naszą wschodnią granicą. Zwiększone korzystanie z energii elektrycznej generuje także transport indywidualny i pojawienie się w naszych garażach elektrycznych samochodów, które stają się popularną alternatywą dla pojazdów spalinowych, przyczyniając się do redukcji emisji szkodliwych substancji. Zmiany zauważane są także w ogrzewaniu. Choć wciąż dostępne są rozwiązania na gaz, współczesne piece gazowe i tak wymagają niezakłóconego zasilania w energię elektryczną, niezbędną do działania układów elektronicznych w nich zaimplementowanych. Ze względu na postępujące zmiany klimatyczne w Polsce rozpowszechniają się, nieodzowne w wielu regionach i nierozpatrywane wcześniej jako wyzwanie dla systemu elektroenergetycznego, systemy klimatyzacji.

**W świetle powyższego, cyberbezpieczeństwo w sektorze energetycznym staje się kluczowym zagadnieniem, koniecznym do zapewnienia ciągłości zaopatrzenia w energię elektryczną.**

# 5. ZAGROŻENIA DLA URZĄDZEŃ I SYSTEMÓW POMIAROWYCH

Krajowy System Elektroenergetyczny (KSE) stoi u progu transformacyjnych zmian, które muszą zostać wprowadzone w nadchodzących latach. Do 2030 roku konieczne będzie przyłączenie do niego:

- ponad 20 GW źródeł słonecznych (bez uwzględniania instalacji prosumenckich powstałych po 31.12.2021 r.) o potencjale produkcyjnym 21 TWh rocznie,
- ponad 14 GW lądowych elektrowni wiatrowych o potencjale produkcyjnym 37 TWh rocznie,
- prawie 11 GW morskich elektrowni wiatrowych o potencjale produkcyjnym 40 TWh/rok.

Przewiduje się, że w tym czasie liczba odbiorców przyłączonych do sieci wzrośnie o ponad 2 mln. Z uwagi na rozwój sektora elektromobilności konieczna będzie również instalacja coraz większej liczby punktów ładowania pojazdów elektrycznych. **Wszyscy odbiorcy energii elektrycznej, których w Polsce jest 18 milionów, zostaną w tym czasie opomiarowani licznikami zdalnego odczytu** (licznikami inteligentnymi lub tzw. smart meters)[14].

Obecnie, w ramach infrastruktury IT wykorzystywanej w systemie dystrybucji energii elektrycznej oraz w systemach pomiarowych z nim powiązanych, stosuje się coraz więcej rozwiązań zautomatyzowanych lub inteligentnych. Systemy Smart Grid oraz Smart Metering z pomocą sztucznej inteligencji (AI) oraz uczenia maszynowego (ML) wykorzystuje się do monitoringu i kontrolowania przepływu energii w czasie rzeczywistym. Adaptacja coraz nowszych, bardziej zautomatyzowanych i zaawansowanych rozwiązań zapewnia wiele benefitów dla sektora energetycznego, ale jednocześnie wprowadza ona dodatkowe zagrożenia dla bezpieczeństwa. Przywołana powyżej technologia Smart Grid (SG) ma odpowiadać skali wyzwań stojącym przed infrastrukturą sieciową w polskiej elektroenergetyce. SG opiera się na modyfikacji istniejącej sieci energetycznej. Jedną z nich jest wprowadzenie do sieci zaawansowanej infrastruktury pomiarowej – AMI. AMI wykorzystuje jedno- lub dwukierunkową komunikację pomiędzy dostawcami a inteligentnymi licznikami energii elektrycznej konsumentów oraz implementuje inteligentne techniki gromadzenia danych.

Inteligentne liczniki to systemy pomiarowe, które umożliwiają automatyczne zbieranie, przechowywanie i transfer szczegółowych danych o zużyciu energii elektrycznej. Mierzą głównie zużycie energii elektrycznej przez konsumentów w czasie rzeczywistym, a także jakość zasilania i chwilowe pomiary elektryczne, takie jak napięcie i natężenie prądu w ich punktach przyłączeniowych, i z określoną częstotliwością zgłaszają je podmiotom dostarczającym energię elektryczną. W ten sposób zakłady energetyczne mogą monitorować i dostosowywać zapotrzebowanie na energię w krótkich okresach (reakcja na popyt), zapewniać dokładniejsze rozliczenia i wykorzystywać dynamiczne ceny w celu ułatwienia zmniejszenia zużycia energii w szczycie zapotrzebowania. Eliminują potrzebę manualnej kontroli stanu liczników, a poprzez transfer danych pozwalają na bieżąco monitorować dane na temat stanu zużycia energii. Fakt, iż inteligentne liczniki przesyłają dane do podmiotów realizujących funkcje o znaczeniu strategicznym – zakładów energetycznych, czyni je celem dla cyberprzestępców. Dane transmitowane przez liczniki to szczegółowe dane dotyczące zużycia energii elektrycznej przez konsumenta, a więc dane osobowe. Dane te w przypadku przejęcia mogą być analizowane i wykorzystywane do wyciągnięcia wniosków na temat działań gospodarstwa domowego, czy nawet rodzaju urządzeń pobierających energię, co z kolei może prowadzić nie tylko do naruszenia prywatności konsumenta, ale także dostarczyć cyberprzestępcom informacji o rozkładzie dnia konsumenta, jego statusie społecznym i innych aspektach jego życia (profilowanie).

Wyciek danych osobowych nie jest jedynym negatywnym skutkiem cyberzagrożeń dla systemu energetycznego. Inteligentne liczniki energii elektrycznej wyposażone są w styczniki umożliwiające zdalne odłączenie konsumenta od dostaw energii elektrycznej. Tego typu rozwiązanie ma praktyczne zastosowanie dla operatorów sieci

14 https://www.ure.gov.pl/pl/urzad/informacje-ogolne/aktualnosci/10630,Rynek-energii-elektrycznej-historyczne-porozumienie-sektorowe-regulatora-i-opera.html?search=8507173 - dostęp 21.08.2023 r.

dystrybucyjnej, ale jednocześnie fakt implementacji stycznika i możliwość zdalnej zmiany stanu jego pracy umożliwia atakującemu nie tylko pozbawienie zasilania wybraną grupę ofiar ataku, ale - w przypadku kompromitacji wielu urządzeń - zachwianie równowagi całego systemu dystrybucji energii elektrycznej. Jest to tzw. atak wykorzystujący oscylacje obciążenia. Bazuje on na masowym odłączeniu odbiorców energii elektrycznej w momencie, gdy jest wysoki popyt na energię elektryczną (duży pobór energii elektrycznej).

**W wyniku zaniku dużej liczby odbiorców energii, obciążenie jest przenoszone automatycznie na inne segmenty sieci energetycznej, w efekcie wymuszając zadziałanie zabezpieczeń przed nadmiarem energii w całym systemie – powstaje efekt domina, który może doprowadzić do całkowitego odłączenia od zasilania znacznych obszarów kraju**[15].

W swoim stanowisku z 10 lipca 2013 r. w sprawie AMI[16], w rozdziale analiza ryzyk, Prezes URE wskazuje na ryzyka rynkowe oraz operatorskie. Wśród ryzyk rynkowych zostało zidentyfikowane m.in. „ryzyko potencjalnej petryfikacji rynku odbiorców (użytkowników) infrastruktury AMI (odbiorców końcowych oraz OSD E), poprzez podział tego rynku pomiędzy dominujących dostawców elementów infrastruktury", co może prowadzić do „uzależnienia od jednego dostawcy technologii na obszarze działania danego OSD E". Natomiast wśród ryzyk operatorskich: „otwarcie infrastruktury komunikacyjnej AMI na możliwość „oddolnego" (przez odbiorcę końcowego lub osobę trzecią) wprowadzenia sygnału destabilizującego pracę całego systemu, w szczególności poprzez zablokowanie możliwości transmisji sygnałów użytecznych lub poprzez wprowadzenie sygnałów/komend fałszywych; w tym miejscu należy odnotować, że ryzyko „włamania" z wykorzystaniem dostępu fizycznego ma w tym przypadku taki sam charakter jak ryzyko wykorzystania sygnału transmitowanego („włamania się" poprzez eter)". Jak widać już 10 lat temu uświadamiano sobie potencjalne ryzyko związane z ingerencją osób trzecich w inteligentne systemy monitorowania i zarządzania.

Jak dotąd nie odnotowano kampanii lub cyberataku bazującego wyłącznie na inteligentnych urządzeniach pomiarowych lub innym elemencie rozwiązania Smart Grid, który miałby na celu zakłócenie dostaw lub destabilizację całego systemu dystrybucji energii elektrycznej. Jedyny, upubliczniony do tej pory atak wykorzystujący bezpośrednio urządzenia pomiarowe miał inny charakter. Incydent miał miejsce w Puerto Rico[17], gdzie atakujący wykorzystał optozłącze i oprogramowanie do odczytania pamięci liczników inteligentnych, a następnie z pomocą uzyskanych w ten sposób poświadczeń uwierzytelniających fałszował odczyty zużycia energii elektrycznej, zaniżając tym samym rachunki. Straty zostały wycenione na kilkaset milionów dolarów. Nie oznacza to, że zagrożenie nie istnieje. Wektor ten jest przedmiotem analiz i badań naukowych[18], a także stanowi realne zagrożenie. Atak mający na celu destabilizację energetyczną jakiegoś państwa, np. Polski, może być elementem nacisku politycznego lub służyć innym celom wrogiego mocarstwa.

**Wyposażenie liczników inteligentnych w styczniki, w przypadku przejęcia nad nimi kontroli (backdoor) lub dodaniem do liczników bomb logicznych, daje potencjalną możliwość zdalnego, jednoczesnego wyłączenia (lub włączenia) dużej liczby odbiorców. Z tego względu kluczowe jest opracowanie właściwych wymagań względem inteligentnych urządzeń pomiarowych oraz opracowanie procedur weryfikacji spełnienia tych wymagań przez urządzenia**.

15 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10098782&tag=1 – dostęp 17.08.2023 r.

16 Stanowisko Prezesa URE w sprawie niezbędnych wymagań dotyczących jakości usług świadczonych z wykorzystaniem infrastruktury AMI oraz ram wymienności i interoperacyjności współpracujących ze sobą elementów sieci Smart Grid oraz elementów sieci domowych współpracujących z siecią Smart Grid - https://ise.ure.gov.pl/ise/stanowiska-regulatora/5357,Stanowisko-Prezesa-URE-w-sprawie-interoperacyjnosci-sieci-Smart-Grid.html – dostęp 17.08.2023 r.

17 https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ - dostęp 07.08.2023 r.

18 Np. analiza bezpieczeństwa w protokole/licznikach OSGP przedstawiona przez Philippa Jovanovica and Samuela Nevesa – https://www.iacr.org/archive/fse2015/85400109/85400109.pdf (dostęp 16.08.2023) - w efekcie doprowadziła do zmiany algorytmów szyfrujących z RC4 na AES128

Analizując możliwe wektory ataku na system dystrybucji energii elektrycznej, w których wykorzystane mogą zostać inteligentne urządzenia, można wyodrębnić trzy z nich:

**1. Atak fizyczny**

| Opis | Zagrożenia | Zabezpieczenia |
|---|---|---|
| Włamanie poprzez fizyczną manipulację komponentami sprzętowymi urządzenia i jego oprogramowaniem układowym. | Nieuprawniony dostęp do danych pomiarowych, manipulacja danymi pojedynczego licznika, nieuprawnione odłączenie odbioru, uszkodzenie urządzenia. | Detekcja otwarcia obudowy i rejestrowanie zdarzenia sabotażu, sygnalizacja nieautoryzowanego dostępu do centrum nadzoru AMI lub pracownikowi zakładu energetycznego. |

**2. Atak na kanał komunikacyjny**

| Opis | Zagrożenia | Zabezpieczenia |
|---|---|---|
| Atak poprzez wykorzystanie luk oraz podatności w protokołach komunikacyjnych lub w oprogramowaniu układowym. | Przechwycenie lub manipulacja danymi przesyłanymi do i od licznika, w tym nieuprawnione odłączenie odbiorcy, potencjalny dostęp do innych systemów w sieci. | Szyfrowanie komunikacji lub danych przesyłanych przez kanał komunikacyjny, stosowanie mechanizmów silnego uwierzytelnia dla czynności zarządzających, regularne aktualizacje oprogramowania układowego w celu łatania znanych luk bezpieczeństwa. |

**3. Atak na łańcuch dostaw**

| Opis | Zagrożenia | Zabezpieczenia |
|---|---|---|
| Wykorzystanie backdoorów lub bomb logicznych zaimplementowanych w oprogramowaniu układowym licznika podczas procesu produkcyjnego. | Nieuprawniony dostęp do danych przesyłanych do i od licznika lub jego funkcji, nieuprawnione odłączenie odbiorców, potencjalne uszkodzenie lub dezaktywacja licznika, możliwość ataku na inne elementy systemu. | Rygorystyczna weryfikacja dostawców urządzeń i stosowanych w procesie produkcji praktyk bezpieczeństwa, regularne audyty bezpieczeństwa oprogramowania układowego i testy bezpieczeństwa urządzeń, wdrożenie mechanizmów ochrony oprogramowania układowego oraz wykrywania i reagowania na nieautoryzowane modyfikacje oprogramowania układowego. |

## 5.1. Atak fizyczny

Powszechnie uważa się, że inteligentne liczniki energii elektrycznej są zabezpieczone przed pierwszym wektorem ataku – większość liczników w przypadku otwarcia obudowy licznika w nieautoryzowany sposób rejestruje zdarzenie sabotażu i przekazuje je do centrum nadzoru AMI lub zasygnalizuje pracownikowi zakładu energetycznego ten fakt podczas wizyty serwisowej. Ponadto, tego typu ingerencja wymaga fizycznego dostępu do urządzenia, co ogranicza skalę potencjalnego ataku.

Liczniki energii elektrycznej, nawet te inteligentne, zbudowane są zazwyczaj w oparciu o specjalnie w tym celu opracowane mikroprocesory i dedykowane oprogramowanie układowe. Oznacza to, że nie występują w nim instrukcje czy polecenia umożliwiające wykonywanie skomplikowanych operacji np. odczytu i udostępnienia atakującemu zawartości pamięci procesora czy układów pamięci nieulotnej. Standardowo licznik udostępnia dane związane z odczytem zużycia i jakości energii elektrycznej, które są przesyłane w trybie pull, po wcześniejszym

nawiązaniu połączenia z licznikiem przez system monitoringu dostawcy energii elektrycznej – w ramach zestawienia sesji komunikacyjnej przeprowadzana jest autoryzacja, negocjowane są parametry kanału komunikacyjnego, a sam kanał jest szyfrowany. Fakt powyższy nie powstrzymuje cyberprzestępców i osób pasjonujących się hackowaniem urządzeń. W sieci Internet udostępniono wiele materiałów[19] i wyników prac związanych z próbami modyfikacji oprogramowania układowego inteligentnych liczników energii elektrycznej, np. poprzez wprowadzenie mikroprocesora w stan nieustalony tak, by w wyniku krótkotrwałych zaników zasilania doprowadzić do jego wadliwego funkcjonowania. Intencją atakującego jest uzyskanie, w wyniku utraty zasilania, zawartości całej pamięci procesora licznika. Kiedy atakujący pozyska już dane, będzie mógł przeprowadzić ich analizę pod kątem luk i podatności, które z kolei mogą ułatwić atak poprzez kanał komunikacyjny, np. poprzez przejęcie kluczy kryptograficznych zapisanych w pamięci urządzenia. Tego rodzaju atak wymaga pozyskania urządzenia. Zazwyczaj atakujący nabywa licznik poprzez różne portale aukcyjne, rzadziej na drodze kradzieży.

Ten rodzaj ataku wymaga specjalistycznej wiedzy, sprzętu oraz jest czasochłonny, ze względu na jego metodologię oraz konieczność zebrania informacji na temat atakowanego modelu licznika w zakresie podzespołów elektronicznych wykorzystanych do budowy urządzenia. Atakujący może je uzyskać poddając analizie dokumentację licznika opublikowaną lub udostępnianą przez producenta, dokumentację certyfikacyjną oraz dokumentację układów elektronicznych, z których składa się licznik. Fizyczny wektor ataku na inteligentny licznik wydaje się mało prawdopodobny nie tylko ze względu na przywołane powyżej trudności, które musi pokonać atakujący. Dodatkowym czynnikiem jest tutaj efekt skali, wymaga on bowiem ingerencji fizycznej w urządzenie znajdujące się u użytkownika – nawet uzyskanie kontroli nad pojedynczym lub kilkoma urządzeniami nie stanowi zagrożenia dla całego systemu dystrybucji energii elektrycznej.

W przypadku ataku tego rodzaju należy rozważyć ryzyko pozyskania przez atakującego wiedzy w zakresie ewentualnych podatności występujących w oprogramowaniu układowym licznika, co może prowadzić do skutecznego wykorzystania wektora związanego z warstwą komunikacyjną.

## 5.2. Atak na kanał komunikacyjny

Drugim zidentyfikowanym wektorem ataku na inteligentne urządzenia pomiarowe jest wykorzystanie ich warstwy komunikacyjnej do przejęcia przesyłanych danych, modyfikacji tychże lub do przejęcia kontroli nad urządzeniami.
Inteligentne urządzenia pomiarowe komunikują się ze światem zewnętrznym na kilka sposobów. Pierwszą płaszczyzną komunikacji są zazwyczaj sieci komórkowe 3G i 4G, które zapewniają szeroką przepustowość i dostępność. O wiele rzadziej wykorzystuje się usługę pakietowej transmisji danych (GPRS) oraz rozwiązanie 2G. Co warte uwagi, samo połączenie zestawiane pomiędzy urządzeniem pomiarowym a centrum zarządzania nie wykorzystuje do realizacji transmisji sieci Internet lub innej ogólnodostępnej sieci. Wszystkie karty SIM wykorzystywane do zestawienia kanału komunikacji z centrum zarządzania umożliwiają nawiązanie połączenia jedynie z dedykowaną siecią dostawcy energii elektrycznej. Ograniczenia te są gwarantowane przez operatora sieci komórkowej, który konfiguruje parametry zestawiania połączeń (APN) na etapie konfiguracji swoich urządzeń i programowania kart SIM.

Wydaje się, że powyżej opisane ograniczenia mogą być prawdopodobnie przełamane jedynie z wykorzystaniem potencjalnych podatności lub błędów w oprogramowaniu układowym licznika lub z wykorzystaniem intencjonalnych backdoorów umieszczonych w oprogramowaniu układowym przez producenta. Efektem wykorzystania backdoora i ewentualnych podatności może być zestawienie połączenia do zdefiniowanego przez atakującego serwera command & control poprzez modyfikację konfiguracji w zakresie parametrów zestawiania połączeń. Atakujący może także przeprowadzić atak typu Denial-of-Service (DoS) na moduł komunikacyjny bazujący na łączności bezprzewodowej, zakłócając tym samym komunikację z centrum zarządczym. Ten typ ataku wymaga jednak znacznych zasobów ze strony atakującego i tym samym jest mniej prawdopodobny.

19 https://www.youtube.com/watch?v=O-J9H2XrZgE

Kolejnym ryzykiem może być fakt, iż poszczególne urządzenia wykorzystując połączenie komórkowe łączą się w odrębną sieć, która może nie być w żaden sposób segmentowana. W takiej sytuacji kompromitacja jednego urządzenia wystawia na potencjalne zagrożenie pozostałe urządzenia funkcjonujące w tej samej sieci, w tym system zarządzający. Może się tak stać w przypadku zaimplementowania przestarzałych protokołów komunikacji, braku szyfrowania transmisji lub szyfrowanie jej przy pomocy identycznych kluczy szyfrujących na każdym urządzeniu. Jeśli urządzenia pomiarowe mają zaimplementowane w całej populacji ten sam zestaw kluczy szyfrujących – transmisja danych jest najczęściej szyfrowana w sposób symetryczny – tym samym przejęcie jednego klucza umożliwia atakującemu wgląd w dane transmitowane w sieci pomiarowej. To z kolei może prowadzić do przejęcia danych lub do zafałszowania ich w efekcie ataku typu Man-in-the-Middle[20], którego celem może być destabilizacja systemu dystrybucji energii elektrycznej, wykonana przez centrum zarządzania (na podstawie fałszywych danych).

Drugą płaszczyzną komunikacyjną dla inteligentnych liczników jest komunikacja z wykorzystaniem technologii komunikacji elektroenergetyczną siecią dystrybucyjną (ang. power line communication lub ang. power line carrier – PLC). Technologia ta oparta jest na przesyłaniu równolegle z napięciem zasilającym o częstotliwości 50 Hz sygnału o wiele wyższej częstotliwości, który przenosi dane[21]. Ze względu na fakt, iż dane przesyłane są siecią elektroenergetyczną, atakujący może uzyskać do nich dostęp poprzez wykorzystanie przejętego urządzenia pomiarowego. Odbyć może się to, jak w poprzednim przypadku, poprzez np. backdoor zaimplementowany w procesie produkcyjnym licznika.

Trzecią warstwą komunikacyjną inteligentnego licznika jest komunikacja bliskiego zasięgu. Liczniki inteligentne w Polsce powinny być wyposażone w moduł radiowy, pracujący w standardzie wireless M-bus[22], optozłącze i dodatkowy port szeregowy. W przypadku modułu radiowego wMbus, w zdefiniowanych przez dostawcę energii lub producenta licznika interwałach czasowych, licznik rozgłasza datagram zużycia energii elektrycznej w paśmie ISM. Komunikacja jest jednostronna i w przypadku prawidłowej konfiguracji nie jest możliwe zestawienie kanału dwukierunkowego z systemem operacyjnym licznika.
Dodatkowo, liczniki wyposażone są w lokalne porty komunikacyjne, takie jak optozłącze czy port szeregowy RS-485. W porównaniu do wMBus porty te mają typowo znacznie większą funkcjonalność – to kanał z możliwościami analogicznymi do kanału zdalnego (LTE, PLC), umożliwiający także konfigurację urządzenia i wymianę firmware. Zestawienie komunikacji wymaga fizycznej obecności operatora i odbiornika. Porty szeregowe mogą znaleźć wykorzystanie w przypadku modernizacji liczników nieposiadających wbudowanych modułów komunikacyjnych. Komunikacja bliskiego zasięgu może zostać wykorzystana do przeprowadzenia cyberataku na system pomiarowy pod warunkiem wykorzystania przez atakującego backdoora w oprogramowaniu układowym licznika lub podatności i błędów w tym oprogramowaniu.

## 5.3. Atak na łańcuch dostaw

Trzecim wektorem ataku jest atak na łańcuch dostaw, związany z procesem produkcyjnym urządzenia, jakim jest inteligentny licznik. **Jest to bardzo złożony problem. Jednocześnie jest on niezwykle istotny, zwłaszcza z perspektywy cyberataku realizowanego przez jednoczesną kompromitację wielu inteligentnych urządzeń pomiarowych**.

Atak na/poprzez zewnętrzny łańcuch dostaw (z ang. supply chain attack) oznacza atak, w którym nie jest atakowany bezpośrednio podmiot lub infrastruktura podmiotu stanowiącego zasadniczy cel ataku, lecz jego

20 Atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy
21 OSD w Europie mogą korzystać z pasma Cenelec A, od 3 do 95 kHz, ale w praktyce wykorzystuje się częstotliwości od 40 do 95 kHz. Częstotliwości 95-150 kHz są zarezerwowane do innych celów (OSD nie mogą z nich korzystać), natomiast wykorzystanie częstotliwości wyższych niż 150 kHz przez OSD jest, ze względu na możliwe interferencje z radiolatarniami, radiem AM itp., sprawą dyskusyjną
22 Komunikacja między systemem nadrzędnym (master) a licznikami (slave) odbywa się bezprzewodowo w pasmach 169MHz, 433MHz i 868MHz. Szczegółowy opis protokołu i warstwy fizycznej znajduje się w normie europejskiej PN-EN 13757-4 "Systemy komunikacji dla przyrządów pomiarowych" (Communication system for meters and remote reading of meters)

dostawcy. Założeniem atakujących jest, że tacy dostawcy mogą być mniej dojrzali w zakresie cyberbezpieczeństwa oraz mają wdrożone słabsze mechanizmy monitorowania i zarządzania bezpieczeństwem. Przedmiotem ataku na łańcuch dostaw może być zarówno oprogramowanie (software), jak i fizyczne komponenty urządzeń (hardware). Łańcuchy takie są bardzo podatne na ataki, ponieważ w nowoczesnych organizacjach oprogramowanie nie jest tworzone całkowicie samodzielnie i od podstaw, a firmy wykorzystują wiele gotowych komponentów nabytych na rynku, przy czym przy wyborze rozwiązania firma najczęściej kieruje się jedynie kryterium najniższej ceny jako determinanty wybranego rozwiązania. W rozpatrywanym przez nas przypadku elementem takiego rodzaju ataku mogą być dostarczone przez dostawców zewnętrznych liczniki zdalnego odczytu.

Oto kilka popularnych ataków na łańcuch dostaw z ostatnich lat:

1. 3CX Phone System – atakujący skompromitowali oprogramowanie 3CX (centrala VoIP) dodając do niego backdoor i dołączając go do legalnej aktualizacji podpisanej prawidłowymi certyfikatami twórcy oprogramowania. Backdoor umożliwiał dostęp do sieci ofiar. W momencie wykrycia incydentu, zgodnie ze skanem przeprowadzonym w bazie danych Shodan, skompromitowanych zostało ponad 244 tysiące instancji 3CX Software. Co ciekawe, do początkowej kompromitacji doszło również z wykorzystaniem łańcucha dostaw – wektorem wejścia było skompromitowane wcześniej niewspierane już oprogramowanie handlowe[23, 24].
2. UAparser.js – atakujący przejął poświadczenia do konta jednego z twórców oprogramowania w portalu NPM, następnie wprowadził do pakietu UAparser.js backdoor, umożliwiający odczyt poświadczeń zapisanych w przeglądarkach ofiar oraz zapisanych odcisków sesji (pliki cookie). Co więcej, atakujący dodał do niego koparkę wydobywającą kryptowaluty. Pakiet UAparser.js jest wykorzystywany przez największe i najpopularniejsze serwisy internetowe, m. in.: Facebook, Amazon, Microsoft, Google, Instagram, Mozilla, Elastic, Intuit, Slack, Reddit[25, 26].
3. Solar Winds – atakujący wstrzyknęli backdoora do aktualizacji oprogramowania SolarWinds (popularnego narzędzia sieciowego używanego przez wiele renomowanych firm i agencji rządowych). Backdoor umożliwił atakującym zdalny dostęp do tysięcy serwerów korporacyjnych i rządowych. Atak w efekcie doprowadził do wycieku poufnych danych wielu agend rządowych i innych incydentów bezpieczeństwa[27].
4. NotPetya - atak złośliwego oprogramowania, który był wymierzony w rząd i infrastrukturę krytyczną Ukrainy i rozprzestrzenił się na inne kraje poprzez atak łańcucha dostaw na firmę programistyczną MeDoc. Rozpowszechniał się poprzez aktualizację MeDoc, programu do rozliczania podatków powszechnie używanego przez ukraińskie firmy.
5. CCleaner - popularne narzędzie konserwacji/optymalizacji systemu operacyjnego – CCleaner - zostało zhakowane i wykorzystane do dystrybucji złośliwego oprogramowania. .

W kontekście ataku na łańcuch dostaw liczników inteligentnych istotnym ryzykiem jest umieszczenie w ich komponentach elektronicznych tzw. "backdoorów". **Backdoory to celowo wprowadzone luki w oprogramowaniu lub urządzeniach, które umożliwiają nieuprawniony dostęp lub kontrolę nad całym systemem lub wybranym jego elementem czy elementami.** Dostawcy (lub atakujący) mogą celowo wprowadzać backdoory do dostarczanych produktów w celu późniejszego wykorzystania ich w celach szpiegowskich, sabotażowych lub hakerskich. W ten sposób atakujący mogą manipulować dostawą energii, powodować awarie lub całkowicie wyłączyć dostawy.

Kolejnym istotnym ryzykiem jest tzw. "bomba logiczna". **Bomba logiczna może być umieszczona w oprogramowaniu lub systemie operacyjnym i aktywuje się samoistnie w określonych warunkach** (np. w określonym dniu lub godzinie, po zdefiniowanej liczbie uruchomień systemu, po wykonaniu przez użytkownika akcji lub zmiany

23 https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise - dostęp 23.08.2023 r.
24 https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/ - dostęp 23.08.2023 r.
25 https://www.truesec.com/hub/blog/uaparser-js-npm-package-supply-chain-attack-impact-and-response - 23.08.2023 r.
26 https://www.cisa.gov/news-events/alerts/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js - dostęp 23.08.2023 r.
27 https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/ - dostęp 22.08.2023 r.

w systemie). Istotą bomby logicznej jest więc fakt, że nie musi ona posiadać połączenia z serwerami "command & control" ani połączenia z siecią Internet w ogóle. W bombie logicznej zapisane są komendy, które po aktywacji są automatycznie uruchamiane. Mogą wywołać destrukcyjne działania, takie jak usunięcie lub zmiana danych, uszkodzenie systemu operacyjnego lub innych komponentów. Bomby logiczne wykorzystane w sektorze energetycznym mogą mieć na celu osłabienie, dezaktywację a nawet zniszczenie systemów kontroli i zarządzania, które sterują sieciami energetycznymi czy systemami dystrybucji, a w przypadku liczników inteligentnych jednoczesne, masowe wyłączenie odbiorów.

Podsumowanie analizy zagrożeń dla urządzeń i systemów pomiarowych przedstawia poniższa tabela.

| | Obecne środki ochrony | Potencjalne następstwa |
|---|---|---|
| **Atak fizyczny** | średnie | niskie |
| **Atak na kanał komunikacyjny** | wysokie | średnie |
| **Atak na łańcuch dostaw** | niskie | wysokie |

Tabela 1 – Podsumowanie analizy potencjalnych wektorów ataku

Potencjalne następstwa ataku fizycznego i ataku na kanał komunikacyjny, zaprezentowane w tabeli, zostały oszacowane jako relatywnie mniej dotkliwe – niemniej należy pamiętać, że w związku z brakiem standardów w tym obszarze, autorzy niniejszego opracowania nie byli w stanie w pełni ocenić potencjalnych ryzyk w perspektywie średnio- i długookresowej.

# 6. PROPOZYCJE MINIMALIZACJI RYZYKA ZWIĄZANEGO Z ŁAŃCUCHEM DOSTAW

W ocenie autorów niniejszego opracowania najpoważniejsze w swych konsekwencjach dla bezpieczeństwa zaawansowanej infrastruktury pomiarowej są obecnie ryzyka dotyczące łańcucha dostaw. W związku z tym, w kolejnych rozdziałach niniejszego opracowania przedstawione zostaną różne potencjalne środki zmniejszenia tego ryzyka.

W celu uporządkowanego przedstawienia wyników analizy metod minimalizacji ryzyka związanego z łańcuchem dostaw, wykorzystano technikę SWOT (Strengths – mocne strony, Weaknesses – słabe strony, Opportunities – szanse, okazje i Threats – zagrożenia).

Każde z proponowanych rozwiązań może prowadzić do wzrostu cen komponentów AMI, niemniej jest to niezbędny koszt podwyższenia bezpieczeństwa infrastruktury krytycznej.

## 6.1. Wprowadzenie schematów certyfikacyjnych[28] dla komponentów AMI, w tym w szczególności liczników inteligentnych

Wiarygodną metodą oceny zgodności wyrobu z określonymi normami lub standardami jest ich badanie w kompetentnych i uprawnionych (akredytowanych) laboratoriach badawczych oraz certyfikacja w jednostkach certyfikujących. Zawsze w tym przypadku jednostki oceniające zgodność posługują się schematem (programem) certyfikacji tj. zbiorem norm, standardów i procedur badawczych, czyli tymi kryteriami i metodykami, których zastosowanie daje pewność co do obiektywności oceny. Schematy takie powstawały i powstają dla różnych dziedzin techniki, produkcji przemysłowej żywności itp. Przykładem są tu Common Criteria[29] (Wspólne Kryteria) dodatkowo ustanowione jako Międzynarodowa Norma ISO/IEC 15408:2022.

**S Mocne strony:**

- dostępność – każdy producent może certyfikować swój produkt;
- obiektywizm – stosowane kryteria są takie same dla wszystkich produktów, oceny prowadzone zgodnie z tą samą metodyką;
- wielopoziomowość – można zdefiniować wiele poziomów zaufania do produktu (np. w Common Criteria EAL1 – EAL7), producent wybiera, na jaki poziom aspiruje, użytkownik ma (stosownie do ww. poziomu) pewność, co otrzymuje. Również zamawiający może wybrać różny poziom zaufania dla różnej kategorii produktów lub jego komponentów;
- uniwersalność – pozwalają ocenić różne typy produktów, producent deklaruje funkcje bezpieczeństwa specyficzne dla swojego typu produktu;
- zapewnienie zaufania do ocenianych produktów – schematy certyfikacyjne są rozwiązaniem dojrzałym i rozpowszechnionym.

**W Słabe strony:**

- pracochłonność i czasochłonność dla poddającego się ocenie wynikająca z konieczności opracowania wielu dokumentów formalnych i szczegółowej dokumentacji technicznej, stosowania przez laboratorium skomplikowanych procedur badawczych, co wpływa na wysokie koszty oceny;

28 Postulat stworzenia krajowego schematu certyfikacji cyberbezpieczeństwa znalazł się w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa - https://orka.sejm.gov.pl/Druki9ka.nsf/0/C974DE0E6799563DC12589E40030360D/%24File/3457.pdf

29 https://commoncriteriaportal.org/cc/ - dostęp 23.08.2023 r.

- czasochłonność opracowania nowych schematów, wynikające z konieczności ich uzgodnienia w komitetach technicznych (lub na innych forach) oraz partykularnych interesów organizacji normalizacyjnych (ISO/IEC, CEN-CELEC, ENISA), narodowych, gospodarczych lub innych delegujących członków do tych ciał.

**Szanse:**

- uproszczenie istniejących schematów certyfikacyjnych np. Common Criteria poprzez zredukowanie kryteriów do takiego minimum, które zapewni przeprowadzenia badań i certyfikacji w ustalonym czasie (fixed-time), tzw. lekkie schematy certyfikacji – jest już w tym zakresie propozycja w postaci Normy Europejskiej EN 17640;
- liczniki energii elektrycznej muszą spełniać wymagania Rozporządzenia Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. w sprawie systemu pomiarowego[30], a ponadto muszą być okresowo legalizowane przez akredytowane laboratoria badawcze;
- jeżeli koszty certyfikacji według lekkich schematów nie będą zbyt wysokie a czas badań ograniczony, to certyfikacje liczników można będzie wprowadzić w nowej ustawie o krajowym systemie cyberbezpieczeństwa, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa;
- stworzenie przewagi konkurencyjnej certyfikowanych produktów europejskich i polskich w krajach, które obawiają się braku weryfikacji aspektów bezpieczeństwa w produktach dostarczanych nawet przez liczących się dostawców zagranicznych;
- rosnąca świadomość zagrożeń łańcucha dostaw liczników inteligentnych i systemu elektroenergetycznego.

**Zagrożenia:**

- wysokie koszty oceny będą musiały być uwzględnione w cenie licznika, co może przełożyć się na wzrost kosztów wdrożenia liczników zdalnego odczytu i wzrost ogólnych kosztów transformacji;
- możliwość wycofania się z rynku części dostawców;
- zmniejszenie atrakcyjności Polski zarówno dla europejskich dostawców, jak i podmiotów spoza UE;
- wprowadzenie przepisów z odpowiednim vacatio legis, co w praktyce oznacza wdrożenie schematu w długim okresie czasu, w praktyce na koniec planowanego wdrożenia liczników zdalnego odczytu lub po nim;
- w przypadku każdej zmiany w oprogramowaniu lub urządzeniu konieczne jest powtórzenie procedury certyfikacji.

## 6.2. Wprowadzenie przepisów regulujących lub wykluczających dostawców wysokiego ryzyka z rynku liczników inteligentnych

Dostawcy wysokiego ryzyka (DWR) to podmioty, których produkty, usługi lub procesy stosowane w krytycznych gałęziach gospodarki mogą stanowić zagrożenie dla bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym. W Polsce taką kategorię dostawców przewidują przepisy projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[31]. Podmioty dostarczające produkty, usługi lub procesy ICT mogą być uznane za dostawcę wysokiego ryzyka, jeżeli te produkty, usługi lub procesy ICT są wykorzystywane m.in. przez: operatorów usług kluczowych oraz operatorów infrastruktury krytycznej. Przed identyfikacją podmiotu jako dostawcy wysokiego ryzyka dokonuje się wielokryterialnej oceny uwzględniającej m.in.:

- prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
- liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

30 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000788 – dostęp 24.08.2023 r.
31 https://orka.sejm.gov.pl/Druki9ka.nsf/0/C974DE0E6799563DC12589E40030360D/%24File/3457.pdf

- trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania.

Uznanie za dostawcę wysokiego ryzyka skutkuje tym, że nie może on wprowadzić do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją. Ponadto, użytkownicy mają obowiązek wycofać z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją.
Podobne, choć nie tak restrykcyjne, przepisy są stosowane również w innych krajach UE oraz USA i Wielkiej Brytanii.

**S** **Mocne strony:**

- pomoc w zwiększeniu bezpieczeństwa narodowego i bezpieczeństwa konsumentów – państwo eliminuje potencjalnie niebezpieczne lub wadliwe produkty z rynku (rezygnacja DWR z ekspansji na polskim rynku);
- element nacisku politycznego na inne kraje, co może prowadzić do poprawy standardów i praktyk w ich działaniach;
- legislacyjny charakter – silne umocowanie w prawie i możliwość relatywnie szybkiego wprowadzenia.

**W** **Słabe strony:**

- relatywnie wyższe koszty wytworzenia produktów w Europie w porównaniu do produkcji dostawców DWR, co może prowadzić do wzrostu cen dla OSD i odbiorców indywidualnych;
- potencjalny problem z egzekwowaniem przepisów – mogą wystąpić długoletnie batalie sądowe, zawieszające de facto stosowanie przepisów;
- konieczność powołania odrębnego organu do oceny wpływu DWR na bezpieczeństwo oraz konieczność nabycia niezbędnych kompetencji przez personel takiego urzędu lub duże obciążenie pracą istniejących organów;
- możliwe działania odwetowe ze strony państw-gospodarzy wykluczonych DWR w stosunku do polskich podmiotów, wykluczenie dostawców wysokiego ryzyka może spowodować napięcia dyplomatyczne lub prowadzić do utraty potencjalnych partnerów handlowych;
- ryzyko podjęcia działań prawnych przez dostawców DWR, co może prowadzić do paraliżu procesów zakupowych OSD i problemów w całym sektorze.

**O** **Szanse:**

- zwiększenie popytu na produkty europejskie, co może pomóc w pobudzaniu europejskiej gospodarki, a w efekcie może przyczynić się do wzrostu zatrudnienia, powstawania nowych miejsc pracy i wzmocnienia europejskich firm (zarówno producentów, jak i licznych ich lokalnych dostawców i kooperantów);
- rozwijanie lokalnych przedsiębiorstw opierających swoje działania jako źródło dostaw i produkcji, co może wspierać gospodarkę krajową i zwiększyć niezależność kraju (suwerenność technologiczna);
- zwiększenie skali działania i dochodów lokalnych producentów przekładające się na wyższy poziom podatków odprowadzanych do budżetu państwa;
- rozwój badań w zakresie opracowania i wdrożenia krajowych rozwiązań (urządzeń) AMI;
- rozwój kompetencji technicznych i wzrost poziomu innowacyjności w europejskich i krajowych centrach B+R prowadzonych przez lokalnych producentów.

**T** **Zagrożenia:**

- ograniczenie dostępu do dostawców DWR może prowadzić do czasowych niedoborów produktów na rynku krajowym i wzrostu ich cen, a nawet powstania szarej strefy zajmującej się ponowną legalizacją produktów;
- ryzyko konfliktów dyplomatycznych (politycznych i handlowych) z krajami dostawców DWR, co może wpłynąć na inne obszary współpracy;
- zmniejszenie portfolio produktów na rynku spełniających wymagania OSD;
- ograniczenie konkurencji mogące skutkować zmniejszeniem innowacyjności na rynku liczników inteligentnych;

- powstanie szarej strefy przedsiębiorstw obchodzącej zakaz – formalnie spełniających wymagania a faktycznie pozostających pod kontrolą DWR;
- przejściowe problemy z dostępnością urządzeń i komponentów do nich, do czasu zwiększenia mocy produkcyjnych krajowych dostawców lub znalezienia alternatywnych źródeł dostaw spełniających wymagania.

## 6.3. Wspólne porozumienia OSD w zakresie bezpieczeństwa komponentów AMI

Założeniem jest, że OSD oceniają wzajemny wpływ zakłócenia infrastruktury w wyniku ataku na łańcuch dostaw jako wysoki i wspólnie decydują się to ryzyko zmniejszyć w drodze wzajemnych uzgodnień OSD w konkretnej sprawie – bezpieczeństwa komponentów AMI.

**S Mocne strony:**

- porozumienie umożliwi OSD wymianę doświadczeń, wiedzy i najlepszych praktyk związanych z bezpieczeństwem komponentów, czyniąc je funkcjonalnymi i bezpiecznymi poprzez umożliwienie operatorom skupienia większych zasobów na analizie zagrożeń i wdrażaniu środków zabezpieczających;
- możliwość opracowania wspólnych standardów bezpieczeństwa lub zasad pozyskiwania komponentów zaawansowanej infrastruktury pomiarowej;
- nieregulacyjny charakter – brak regulacji prawnych może zachęcić do podejmowania wspólnych inicjatyw;
- mniejsza liczba podmiotów wymagających konsultacji, co sprzyja podjęciu wspólnych decyzji/wniosków.

**W Słabe strony:**

- różne wymagania i różne potrzeby mogą doprowadzić do kompromisu, który obniży bezpieczeństwo redukując je do najniżej wymaganych wspólnych potrzeb;
- konflikt interesów pomiędzy OSD wpływający na treść wypracowanego porozumienia – trudna koordynacja prac;
- brak możliwości weryfikacji realizacji porozumienia;
- bezsankcyjny charakter – dobrowolność stosowania warunków porozumienia może doprowadzić do rezygnacji z ich stosowania pod wpływem decyzji zarządów motywowanych np. czynnikami ekonomicznymi.

**O Szanse:**

- możliwość utrzymywania współfinansowanej współpracy badawczej np. laboratoria, które dzięki zapewnionemu finansowaniu, będą mogły działać na rzecz poprawy bezpieczeństwa narodowego i konsumentów;
- porozumienie sektorowe jako wyraz wspólnoty interesów;
- możliwość łatwiejszego i szybszego powoływania innych struktur np. ISAC (Information Sharing and Analysis Cell), PSIRT (Product Security Incidents Response Team) lub budowy centrum kompetencji.

**T Zagrożenia:**

- długość procesu decyzyjnego i częste zmiany we władzach poszczególnych OSD, które mogą reprezentować różne interesy;
- różny poziom zaangażowania OSD, a czasem jego paraliżujący brak;
- konkurencja pomiędzy OSD może spowodować spadek zaufania oraz brak przepływu kompletnej, autentycznej informacji w zakresie bezpieczeństwa komponentów AMI;
- pozostawienie kwestii bezpieczeństwa komponentów AMI OSD może zniechęcić organy państwa do wzięcia odpowiedzialności za kwestie bezpieczeństwa, licząc wyłącznie na działanie porozumienia OSD;
- koncentracja OSD na aspektach ekonomicznych – brak interesu w zwiększaniu bezpieczeństwa komponentów AMI.

## 6.4. Wprowadzenie zasady obligatoryjnego podziału dostarczanych w ramach przetargu urządzeń

Wprowadzenie zasady (w przepisach lub wiążącym porozumieniu OSD) obligatoryjnego podziału dostarczanych w ramach przetargu urządzeń pomiędzy producentów europejskich oraz pochodzących z innych krajów np. w proporcji 50/50 (50% urządzeń europejskich/50% urządzeń spoza Europy) lub innej.

**S Mocne strony:**

- zmniejszenie udziału DWR w rynku bez narażenia się na zarzut eliminacji konkurencyjności;
- brak ryzyka destabilizacji rynku (nie ma ryzyka niedoborów);
- bardziej akceptowalne przez rynek i DWR;
- zmniejszenie skutków potencjalnego cyberataku na łańcuch dostaw bez względu na dostawcę.

**W Słabe strony:**

- komplikacja postępowań zakupowych poprzez zwiększenie obciążeń administracyjnych po stronie zamawiających;
- konieczność przeprowadzania postępowań zakupowych w zgodzie z parytetem może sprowadzić ryzyko zmniejszenia wagi innych kryteriów jak np. bezpieczeństwo i jakość produktów oraz usług na rzecz kraju-pochodzenia dostawcy;
- trudność w weryfikacji spełniania wymogów (oparcie na oświadczeniach wykonawcy nie jest wystarczającym warunkiem) oraz konieczność wprowadzenia sposobu weryfikacji oświadczenia dostawcy w tym przedmiocie;
- trudność w monitorowaniu i egzekwowaniu wymogu parytetu;
- problem w zdefiniowaniu kraju pochodzenia produktu.

**O Szanse:**

- zmniejszenie zależności od dostawców spoza Europy, co może pomóc w minimalizowaniu ryzyka związanego z zakłóceniami łańcuchów dostaw urządzeń;
- większa odporność kraju w przypadku wystąpienia kryzysu międzynarodowego (politycznego, handlowego) lub innych nieprzewidywalnych sytuacji, jeśli dysponuje własnym zapleczem produkcyjnym;
- pobudzaniu produkcji w Europie oraz w Polsce, co może przyczynić się do wzrostu zatrudnienia i wzmocnienia lokalnych firm;
- impuls rozwojowy i inwestycyjny dla polskich firm, które będą miały większą szansę na sprzedaż swoich produktów i usług;
- „przetarcie szlaków" i pozytywny przykład aktywnego działania na rzecz bezpieczeństwa, który może zostać zaimplementowany również w innych sektorach i branżach, gdzie dominują DWR.

**T Zagrożenia:**

- założenie lub wykupienie przez kraje dostawców wysokiego ryzyka podmiotów spełniających wymogi produktów krajowych a w rzeczywistości będących rozwiązaniami od dostawców wysokiego ryzyka;
- sprowadzanie przez podmioty pochodzenia polskiego lub europejskiego rozwiązań zakupionych od dostawców wysokiego ryzyka, dokonanie rebrandingu i oferowanie tych produktów jako produkty pochodzenia polskiego lub europejskiego;
- zmniejszenie konkurencyjności cenowej lub jakościowej produktów dostępnych dla OSD w Polsce i Europie;
- ograniczenie dostępu do bardziej innowacyjnych lub atrakcyjnych produktów niespełniających kryterium pochodzenia;
- ryzyko podniesienia kosztów produkcji w niektórych przypadkach, co może zwiększyć ceny dla klientów i ograniczyć ich wybór;
- ryzyko sporów politycznych lub handlowych z innymi krajami i ograniczanie potencjału globalnej współpracy.

## 6.5. Opracowanie metodyki i narzędzi testowania wymagań bezpieczeństwa

Branża inteligentnego opomiarowania szybko się rozwija, a zapewnienie bezpieczeństwa i niezawodności inteligentnych urządzeń pomiarowych nabiera coraz większego znaczenia. Świadomość tego faktu znalazła odzwierciedlenie w opracowanych wymaganiach bezpieczeństwa. Wymagania te zostały opracowane przez różne organizacje i w dokumentach o różnym charakterze (w postaci wytycznych, rekomendacji, a nawet rozporządzeń). Brak jest jednakże znormalizowanej metodyki i narzędzi testowania liczników zdalnego odczytu. Nie ma również powszechnie akceptowanego, publicznie dostępnego środowiska testowego.

**S Mocne strony:**

- jednolitość – mają zastosowanie do wszystkich dostawców i oferowanych przez nich produktów;
- obiektywizm – normalizacja testów.

**W Słabe strony:**

- trudne w uzgodnieniu;
- koszty w przypadku wykorzystania w środowisku testowym komercyjnych narzędzi.

**O Szanse:**

- możliwość użycia w schematach certyfikacyjnych – pozwoliłoby to odnosić wyniki do gotowych schematów certyfikacyjnych i umożliwić dokonanie certyfikacji;
- możliwość wykorzystania przez wiele ośrodków, laboratoriów i przez same OSD;
- możliwość wypełnienia ewidentnej luki w zapewnieniu bezpieczeństwa AMI;
- możliwość wykorzystania narzędzi otwartoźródłowych;
- możliwość samodzielnej weryfikacji spełniania przez dostawców kryteriów bezpieczeństwa oferowanych liczników inteligentnych przez OSD.

**T Zagrożenia:**

- trudność w uzgodnieniu oraz niewiadomy charakter wprowadzenia (kto i na jakich zasadach miałby wprowadzić taką metodykę);
- możliwość podważania wyników testów w przypadku samodzielnej oceny przez OSD.

## 6.6. Wprowadzenie ścisłych regulacji prawnych określających odpowiedzialność dostawców za zabezpieczenie łańcucha dostaw

Dostawca wygrywający postępowanie zakupowe wnosi kaucję lub inne zabezpieczenie gwarancyjne, że jego produkt jest wolny od ryzyk związanych z łańcuchem dostaw przez okres trwania umowy. Kaucja jest przechowywana przez instytucję zaufania publicznego lub krajowy bank np. Bank Gospodarstwa Krajowego i zwracana po wygaśnięciu umowy lub wykorzystana do pokrycia kosztów usuwania skutków materializacji ryzyka ataku na łańcuch dostaw.

**S Mocne strony:**

- wprowadzenie ścisłych regulacji zwiększy bezpieczeństwo sieci energetycznych poprzez minimalizację ryzyka potencjalnych cyberataków;
- wymaganie bezpiecznych i niezawodnych inteligentnych liczników pobudzi innowacje w sektorze energetycznym;
- odpowiedzialność dostawcy za produkt - potencjalna utrata kaucji spowoduje, że będzie on dbał o zachowanie najwyższych standardów jakości i bezpieczeństwa;

- prostota - mechanizm kaucyjny jest łatwy w zrozumieniu i implementacji;
- wzrost zaufania publicznego do sektora i państwa.

**W Słabe strony:**

- problem z określeniem wysokości kaucji;
- długi czas życia licznika, powodujący konieczność długiego oczekiwania na zwrot kaucji przez dostawcę,
- utrata wartości kaucji w czasie, przez co może okazać się niewystarczająca, aby pokryć koszty napraw ewentualnych awarii;
- dodatkowe koszty dla dostawców, które mogą być przenoszone na ceny sprzedaży liczników dla OSD, a te z kolei na klientów poprzez wyższe opłaty dystrybucyjne;
- konieczność znacznych zasobów zarówno ze strony dostawców, jak i organów regulacyjnych/państwowych, które będą obsługiwać kwestie administracyjne związane z kaucją.

**O Szanse:**

- rezygnacja części dostawców z udziału w przetargach ze względu na wysokie ryzyko sankcji za niespełnienie wysokich standardów bezpieczeństwa oferowanych produktów;
- rozwój nowych rozwiązań technologicznych zwiększających bezpieczeństwo sieci i urządzeń inteligentnych.

**T Zagrożenia:**

- opór dostawców, zarówno wysokiego ryzyka, jak i pozostałych, którzy mogą sprzeciwiać się takiemu rozwiązaniu;
- negatywny wpływ wysokich kosztów udziału w postępowaniach na płynność finansową podmiotów – zamrożenie na wiele lat dużych kwot może nie być akceptowalne dla uczestników postępowań;
- udział w przetargach dostawców, którzy dysponują dużym kapitałem własnym, a co za tym idzie eliminacja z rynku dostawców niedysponujących zasobami na opłacenie kaucji;
- możliwość udziału w postępowaniach przetargowych podmiotów sponsorowanych przez wrogie państwa, którym nie zależy na zysku, ale na zdobyciu pozycji rynkowej;
- zahamowanie rozwoju mniejszych przedsiębiorstw branży inteligentnego opomiarowania, które nie będą dysponowały zasobami finansowymi na opłacenie kaucji.

## 6.7. Nowelizacja Prawa Zamówień Publicznych

Nowelizacja prawa może dotyczyć również innych przepisów np. ustawy o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590) lub Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 - dalej UKSC).
Zmiana obowiązującego prawa miałby na celu dodanie przepisów o konieczności posiadania przez dostawcę AMI Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI), zgodnego z normą ISO/IEC 27001, obejmującego swym zakresem proces produkcji inteligentnych liczników. Audyt na zgodność SZBI z normą powinien przeprowadzać podmiot akredytowany przez PCA w obszarze OECD lub UE.

**S Mocne strony:**

- zwiększenie zaufania do podmiotów produkujących liczniki, jak również zwiększenie zaufania do samego produktu;
- szybka droga legislacyjna w związku z koniecznością zmian w UKSC, które muszą być wprowadzone w związku z implementacją dyrektywy NIS2, nakładającą na państwa członkowskie obowiązek regulacji kwestii związanych z łańcuchem dostaw, w tym w sektorze energii;
- legislacyjny charakter – silne umocowanie w prawie;
- jednolitość i obiektywizm – przepisy mają zastosowanie do wszystkich dostawców i oferowanych przez nich produktów;
- obchodzenie przepisów lub brak zastosowania do nich jest sankcjonowany mocą ustawy, powodując brak

możliwości uniknięcia kary za niestosowanie wymogów prawa;
- oparcie i wdrożenie przepisów na zasadach prawa wspólnotowego, które ma większy autorytet na arenie krajowej i międzynarodowej.

**W Słabe strony:**

- trudność w określeniu całości procesu produkcyjnego i uwzględnienia zarówno kwestii fizycznych komponentów licznika, jak i oprogramowania;
- brak weryfikacji technicznej produktu – ocena zgodności będzie się opierać w większości o proces analizy ryzyka i zastosowane mechanizmy minimalizujące zidentyfikowane ryzyka;
- brak właściwej identyfikacji faktycznego producenta i miejsca produkcji np. udziału komponentów dostarczanych przez poddostawców dostawcy, a tym samym właściwego podmiotu, który powinien zostać objęty audytem.

**O Szanse:**

- ograniczenie udziału w przetargach podmiotów niezapewniających odpowiednich wymogów bezpieczeństwa w stosunku do wytwarzanych produktów;
- rozpowszechnianie w coraz większej liczbie podmiotów Systemów Zarządzania Bezpieczeństwem Informacji;
- zwiększanie poziomu świadomości i bezpieczeństwa procesu produkcji ogółem, zarówno wśród podmiotów prawnych, jak i obywateli.

**T Zagrożenia:**

- wydłużenie łańcucha dostaw w taki sposób, by utrudnione i wysokokosztowe było dotarcie do prawdziwego producenta i możliwość wykonania audytu;
- trudność w spełnieniu wymogu przez producentów spowodowana tym, że część ich poddostawców nie będzie chciała podlegać takim wymogom (np. dostawcy procesorów);
- brak realnej możliwości oceny skuteczności procesu weryfikacji poddostawców.

## 6.8. Rekomendacje Pełnomocnika ds. Cyberbezpieczeństwa dotyczące dostawców wysokiego ryzyka w obszarze inteligentnych liczników energii

Obowiązująca ustawa o krajowym systemie cyberbezpieczeństwa daje Pełnomocnikowi ds. Cyberbezpieczeństwa możliwość wydania rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Kierując się istotnym interesem bezpieczeństwa państwa Pełnomocnik może wydać rekomendację dla OSD E w postaci ostrzeżenia przed zagrożeniem w dziedzinie cyberbezpieczeństwa polegającym na używaniu środków technicznych lub programowych niepochodzących z państw Unii Europejskiej, Europejskiego Obszaru Gospodarczego, Organizacji Współpracy Gospodarczej i Rozwoju lub Organizacji Traktatu Północnoatlantyckiego w zaawansowanych urządzeniach pomiarowych stosowanych na terenie kraju.

**S Mocne strony:**

- nie wymagają skomplikowanego i długotrwałego procesu legislacyjnego, a jednocześnie mają silne umocowanie w przepisach ustawowych;
- zwiększenie zaufania do podmiotów produkujących liczniki, jak również zwiększenie zaufania do samego produktu;
- wsparcie dla podmiotów produkujących liczniki na terytorium Unii Europejskiej, Europejskiego Obszaru Gospodarczego, Organizacji Współpracy Gospodarczej i Rozwoju lub Organizacji Traktatu Północnoatlantyckiego;
- zmniejszenie/eliminacja udziału DWR w rynku;
- wspieranie krajowych i sojuszniczych rozwiązań technologicznych.

**W Słabe strony:**

- brak wyraźnego mechanizmu sankcyjnego za nieuwzględnienie rekomendacji – w przypadku zagrożenia brakiem dostawców na rynku z powodu wykluczenia ich przez rekomendacje, OSD mogą dążyć do unikania stosowania rekomendacji;
- wymagają uzyskania opinii Kolegium do Spraw Cyberbezpieczeństwa – trudność w uzgodnieniu stanowiska Kolegium;
- brak wskazanego terminu wydania opinii przez Kolegium – wypracowanie opinii może zająć długi okres czasu.

**O Szanse:**

- większa świadomość zagrożeń dla łańcucha dostaw inteligentnych liczników energii;
- wprowadzanie podobnych rekomendacji w innych krajach Unii Europejskiej, Europejskiego Obszaru Gospodarczego, Organizacji Współpracy Gospodarczej i Rozwoju lub Organizacji Traktatu Północnoatlantyckiego (podobne rekomendacje funkcjonują już np. w Republice Czeskiej);
- zmniejszenie zależności od dostawców wysokiego ryzyka;
- pobudzenie rynku krajowego, czego efektem będzie większa suwerenność technologiczna i samowystarczalność;
- poprawa sytuacji ekonomicznej poprzez zwiększenie krajowej produkcji i zapewnienie miejsc pracy.

**T Zagrożenia:**

- wykluczenie dostawców wysokiego ryzyka niesie ryzyko ograniczenia dostępności komponentów AMI i w efekcie - ryzyko problemów z zapewnieniem stabilności dostaw energii;
- proces identyfikacji dostawców wysokiego ryzyka i wdrażania rekomendacji może prowadzić do opóźnień w projektach energetycznych;
- sprowadzanie przez podmioty pochodzenia polskiego lub europejskiego rozwiązań zakupionych od dostawców wysokiego ryzyka, dokonanie rebrandingu i oferowanie tych produktów jako produkty pochodzenia polskiego lub europejskiego;
- ryzyko sporów politycznych, handlowych z innymi krajami i ograniczenia potencjału globalnej współpracy;
- konieczność aktualizacji rekomendacji w sytuacji dynamicznie zmieniającego się środowiska cyberbezpieczeństwa.

# 7. REKOMENDOWANE DZIAŁANIA W ZAKRESIE MINIMALIZACJI RYZYKA ZWIĄZANEGO Z ŁAŃCUCHEM DOSTAW

Jak wskazano w rozdziale 5 atak na łańcuch dostaw inteligentnych liczników stanowi największe ryzyko dla stabilności KSE. Dla tego wektora ataku obecne środki ochrony są najniższe, a potencjalne następstwa najwyższe. W rozdziale 6 niniejszego dokumentu przedstawiono szereg środków minimalizujących ryzyko niepożądanego wpływu na cyberbezpieczeństwo zaawansowanej infrastruktury pomiarowej poprzez łańcuch dostaw. Jak pokazała analiza SWOT przeprowadzona w ww. rozdziale, nie ma jednak jednego, dominującego środka, którego zalety wskazują wyższość nad pozostałymi i na możliwość jego wyłącznego zastosowania w procesie bezpiecznego użytkowania infrastruktury pomiarowej w systemie energetycznym. Dyrektywa NIS2, która powinna być implementowana przez państwa UE do października 2024 r. (w Polsce najprawdopodobniej poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa[32]), wymaga zapewnienia bezpieczeństwa łańcucha dostaw przez wszystkie podmioty, które będą jej podlegać[33], a takimi podmiotami będą OSD E.

Mając na uwadze zapewnienie stabilności KSE, do czasu implementacji dyrektywy NIS2, rekomenduje się podjęcie następujących działań w celu minimalizacji ryzyka związanego z łańcuchem dostaw zawansowanej infrastruktury pomiarowej.

## 7.1. Bliska perspektywa czasowa

### 7.1.1. Zmiana UKSC

Wykorzystując prowadzony aktualnie proces legislacyjny nowelizacji UKSC należy zgłosić propozycje przepisów dotyczących AMI. Nowa ustawa UKSC, oprócz dotychczasowych rozwiązań (wymaganie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji - SZBI przez operatora usługi kluczowej), powinna zawierać przepisy wymagające:

- posiadania SZBI przez podmioty produkujące urządzenia IT i oprogramowanie, które będą miały zastosowanie w obszarze krytycznej działalności społecznej lub gospodarczej, a więc również elektroenergetyce, w tym wchodzących w skład zaawansowanej struktury pomiarowej;
- realizacji przez ww. podmioty wszystkich wymagań wyszczególnionych w punktach a)–l) poniżej, co zapobiegłoby wyłączeniu ich z zakresu SZBI;
- konieczności przeprowadzania audytów zgodności z UKSC przez akredytowane jednostki certyfikujące lub organizacje będące podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa (o ile nie zachodzi konflikt interesów – np. ww. podmiot dostarcza usługi SOC lub CERT).

Bezpieczeństwo produktu IT jest pochodną bezpieczeństwa organizacyjnego, osobowego, fizycznego i technicznego producenta i jego dostawców (np. oprogramowania lub podzespołów elektronicznych). Oprócz ogólnie znanych aspektów bezpieczeństwa informacji (hardening systemów IT, kontrola dostępu, bezpieczeństwo sieci, szyfrowanie transmisji i in.) niezmiernie ważne są również te, które bezpośrednio wpływają na opracowanie, wykonanie i funkcjonowanie zabezpieczeń w docelowym produkcie IT. Zaliczają się do nich:

32 Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw jest aktualnie w trakcie procesu legislacyjnego - https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=3457

33 Art. 21 ust. 2 lit. d - bezpieczeństwo łańcucha dostaw w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami

a) Opracowanie bezpiecznej architektury systemu i stosowanie zasad inżynierii;
b) Stosowanie bezpiecznego cyklu rozwoju oprogramowania;
c) Uwzględnianie wymagania bezpieczeństwa aplikacji;
d) Bezpieczne tworzenie oprogramowania;
e) Testy bezpieczeństwa w fazie rozwoju i akceptacji;
f) Zlecanie rozwoju oprogramowania na zewnątrz z zachowaniem zasad bezpieczeństwa;
g) Separacja środowisk deweloperskich, testowych i produkcyjnych;
h) Korzystanie z Cyber Threat Intelligence;
i) Uwzględnienie bezpieczeństwa informacji w zarządzaniu projektami;
j) Zapewnienie bezpieczeństwa informacji w relacjach z dostawcami;
k) Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT;
l) Monitorowanie, przegląd i zarządzanie zmianami usług dostawców.

Nowe normy ISO/IEC 27001:2022 (wymagania) oraz ISO/IEC 27002:2022 (zalecenia) zawierają wiele wymagań i zaleceń, które pokrywają wszystkie ww. aspekty. Dlatego tak istotne jest, by każda organizacja uczestnicząca w procesie produkcji inteligentnych liczników wdrożyła SZBI zgodny z ww. normami.

### 7.1.2. Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa

Obowiązująca Ustawa o Krajowym Systemie Cyberbezpieczeństwa daje Pełnomocnikowi ds. Cyberbezpieczeństwa możliwość wydania rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Kierując się istotnym interesem bezpieczeństwa państwa Pełnomocnik może wydać rekomendację następującej treści:

*„Po wyrażeniu w dniu ..... opinii przez Kolegium do Spraw Cyberbezpieczeństwa, rekomenduję podmiotom Krajowego Systemu Cyberbezpieczeństwa niestosowanie w systemach energetyki urządzeń lub oprogramowania niepochodzących z państw Unii Europejskiej, Europejskiego Obszaru Gospodarczego, Organizacji Współpracy Gospodarczej i Rozwoju lub Sojuszu Północnoatlantyckiego, w celu wdrożenia technologii umożliwiających osiągnięcie wymaganego poziomu pomiaru bezpośredniego kategorii B1, C1 zgodnie z Rozporządzeniem Rozporządzenie Ministra Klimatu i Środowiska z 22.03.2022 r. w sprawie systemu pomiarowego (Dz. U. z 2022 Poz. 788) ze względu na możliwe podatności na zagrożenia w obszarze cyberbezpieczeństwa w ww. urządzeniach lub oprogramowaniu."*

Propozycja bazuje na rozwiązaniu zastosowanym w Republice Czeskiej a dotyczącym ograniczenia ekspansji DWR na rynku. Polegało ono na wydaniu Ostrzeżenia przed zagrożeniem w dziedzinie cyberbezpieczeństwa polegającym na użyciu środków technicznych lub programowych niepochodzących z państw Unii Europejskiej, Europejskiego Obszaru Gospodarczego, Organizacji Współpracy Gospodarczej i Rozwoju lub Sojuszu Północnoatlantyckiego, w celu wdrożenia technologii umożliwiających wymagany poziom pomiaru bezpośredniego typu B, C1, C2 lub C3 zgodnie z czeskimi przepisami w sprawie pomiarów energii elektrycznej. Ostrzeżenie to zostało opublikowane przez tamtejsze Krajowe Biuro ds. Cyberbezpieczeństwa i Informacji. Z informacji na stronie https://www.nukib.cz/en/ wynika, że ta instytucja odpowiada za różne aspekty bezpieczeństwa informacji zarówno niejawnych, jak i publicznych w systemach ICT, cyberbezpieczeństwa (prowadzi zespół CERT dla organów państwowych i infrastruktury krytycznej) i nie ma jednego odpowiednika w Polsce, gdzie ww. kompetencje są podzielone pomiędzy DBTI ABW, CERT ABW, Ministerstwo Cyfryzacji i CERT NASK. W związku z tym oraz biorąc pod uwagę silne umocowanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa i jego kompetencji w przepisach ustawowych, wydaje się on być najlepszym podmiotem do wydania takich rekomendacji.

Nie byłby to precedens. Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał już w przeszłości rekomendację dotyczącą niestosowania w systemach informacyjnych oprogramowania, którego producentem jest firma Kaspersky Lab z siedzibą w Moskwie[34]. Podstawą prawną wydawania tego typu rekomendacji jest art. 33 ust. 4 UKSC a merytoryczną – opinia Kolegium do Spraw Cyberbezpieczeństwa o którym mówi art. 64 UKSC. Co jednak najważniejsze w kontekście bezpieczeństwa łańcucha dostaw, miałoby to bezpośredni wpływ na procesy zakupowe realizowanych przez OSD E – art. 226 ust.1 pkt 17) PZP stanowi, że Zamawiający odrzuca ofertę, 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. Rekomendacja o treści zaproponowanej w niniejszym rozdziale wypełnia ten warunek.

## 7.2 Długa perspektywa czasowa

Długofalowym (jeszcze praktycznie niedostępnym w Polsce) rozwiązaniem w zakresie zapewnienia cyberbezpieczeństwa inteligentnych liczników może być ich certyfikacja na bazie tzw. „lekkiego" schematu (programu) certyfikacji (certification schemes). Idea wprowadzenia takich schematów jest związana z europejskim rozporządzeniem Cyber Security Act[35] (dalej CSA), które wprowadza trzy poziomy uzasadnienia zaufania (assurance level) do usług, produktów i procesów ICT:

**„Podstawowy" (Basic)**

- przedmiot oceny zapewnia minimalizowanie znanych, podstawowych ryzyk odnoszących się do incydentów bezpieczeństwa i cyberataków;
- poświadczenie przeprowadzenia oceny jest wydane przez akredytowaną jednostkę oceny zgodności (w postaci certyfikatu) albo przez stronę pierwszą, czyli producenta lub dostawcę, w postaci deklaracji zgodności;

**„Istotny" (Substantial)**

- przedmiot oceny zapewnia minimalizowanie znanych ryzyk incydentów bezpieczeństwa, przy założeniu, że cyberataki są przeprowadzane przez atakujących o ograniczonych umiejętnościach i zasobach;
- poświadczenie (certyfikat) przeprowadzenia oceny spełnienia wymagań cyberbezpieczeństwa przez przedmiot oceny jest wydane przez akredytowaną jednostkę oceny zgodności;

**„Wysoki" (High)**

- przedmiot oceny zapewnia minimalizowanie ryzyk najnowocześniejszych cyberataków, przy założeniu, że są one przeprowadzane przez atakujących o znaczących umiejętnościach i zasobach;
- poświadczenie (certyfikat) przeprowadzenia oceny spełnienia wymagań cyberbezpieczeństwa przez przedmiot oceny jest wydane przez akredytowaną jednostkę oceny zgodności, będącą podmiotem publicznym albo podmiotem prywatnym, na którego delegowano realizację zadania: w obu przypadkach podmioty te są dodatkowo autoryzowane przez krajowy organ nadzorujący certyfikację cyberbezpieczeństwa[36].

34 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-oprogramowania-kaspersky - dostęp 23.08.2023 r.

35 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)

36 W ostatnim projekcie nowelizacji UKSC jest nowy Art. 59b. w którym jest propozycja „Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji"

„Lekkie" schematy oceny cyberbezpieczeństwa rozpoczęto wdrażać w kilku krajach Europy, m.in. we Francji, Holandii, Hiszpanii i Niemczech, co dorowadziło do opracowania Europejskiej Normy EN 17640[37] jako ich uogólnienia. Norma ta jest znacznym uproszczeniem kryteriów Common Criteria i metodyki CEM i może być stosowana w programach, w których kluczowymi czynnikami są ograniczone zasoby i limitowany czas wykonania badania.

Rekomendowane lub wymagane zadania w zakresie oceny produktu IT stosownie do deklarowanego przez producenta poziomu zostały przedstawione w Tabeli 2.

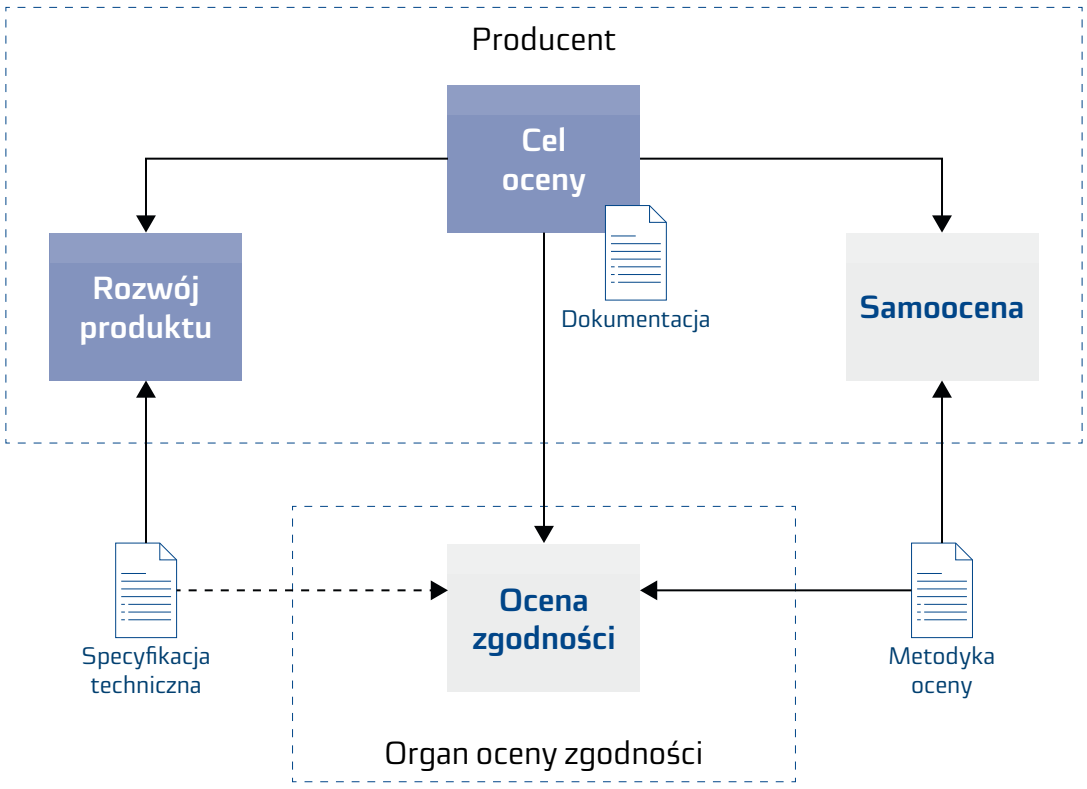
| | | Deklaracja zgodności na poziomie CSA | | |
|---|---|---|---|---|
| **Zadanie oceny** | **Odniesienie** | **Podstawowy** | **Istotny** | **Wysoki** |
| Sprawdzenie kompletności | 6.1 | Wymagana | Wymagana | Wymagana |
| Przegląd funkcjonalności zabezpieczeń | 6.3 | Wymagana | | |
| Ocena dokumentu FIT Security Target | 6.4 | | Wymagana | Wymagana |
| Ocena dokumentacji projektowej | 6.5 | Wymagana | Wymagana | Wymagana |
| Ocena instalacji TOE | 6.6 | Rekomendowana | Wymagana | Wymagana |
| Testy zgodności | 6.7 | Rekomendowana | Wymagana | Wymagana |
| Przegląd podatności w zabezpieczeniach | 6.8 | Rekomendowana | Wymagana (lub wykonywane w 6.9) | |
| Testowanie podatności | 6.9 | | Rekomendowana | |
| Testy penetracyjne | 6.10 | | | Wymagana |
| Kryptoanaliza podstawowa | 6.11 | Rekomendowana | Rekomendowana | |
| Kryptoanaliza rozszerzona | 6.12 | | | Wymagana |

Tabela 2 - Zadania w zakresie oceny vs. deklaracja zgodności na poziomie CSA

37 EN 17640:2022 Fixed-Time Cybersecurity Evaluation Methodology for ICT Products

Podobnie, jak w przypadku badań na zgodność z Common Criteria producent – zgodnie z EN 17640 – ma obowiązek opracowania dokumentu Security Target[38]. Przykładowa struktura i zawartość jest zawarta w aneksie A do Normy.

Należy zauważyć, co Norma EN 17640 wyraźnie podkreśla we Wstępie, że nie można jej używać samodzielnie. Każda domena (program certyfikacji) musi zapewniać specyficzne dla niej wymagania bezpieczeństwa cybernetycznego ujęte formalnie w „specyfikacjach technicznych" (technical specifications) dla produktów, które mają być oceniane i certyfikowane. A więc metodyka opisana w EN 17640 jest przeznaczona do stosowania w połączeniu ze specyfikacjami technicznymi zawierającymi wymogi w zakresie cyberbezpieczeństwa. Obrazuje to Rysunek 1.




Rysunek 1 - Działania w zakresie oceny zgodności produktu w ramach EN 17640

Do rozwiązania w przyszłości (być możne w odpowiednich przepisach) będą następujące zagadnienia:

- Na jakim poziomie szczegółowości powinny być opracowywane specyfikacje techniczne dla różnych typów produktów IT, które będą mogły lub powinny być certyfikowane na bazie EN 17640?
- Czy za taką specyfikację techniczną dla liczników inteligentnych można uważać Załącznik nr 1 do Rozporządzenia Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. w sprawie systemu pomiarowego czy raczej zestaw wymagań opracowany na poziomie europejskim?
- Na jaki poziom CSA (Podstawowy, Istotny, Wysoki) producent liczników smart powinien wnioskować o certyfikat? Im wyższy, tym skuteczniejsze ograniczenie DWR, ale i większe restrykcje w stosunku do producentów kierujących urządzenia do certyfikacji.

38 Określenie to nie ma dobrego tłumaczenia na język polski, propozycja – Specyfikacja zabezpieczeń.

W Polsce nie ma jeszcze akredytowanych laboratoriów realizujących oceny według Normy EN 17649. Można założyć, że istniejące akredytowane laboratoria i jednostka certyfikująca, realizujące oceny na podstawie Common Criteria mogą rozszerzyć swój zakres działalności, ale musi to zrobić również PCA w zakresie ich akredytacji. Mimo że pojawiają się informacje o lekkich programach certyfikacji w Niemczech, Hiszpani Francji i Holandii, to nie natrafiono na informacje o takim akredytowanym laboratorium w UE. Prawdopodobnie sprawę wstrzymują niezakończone prace w ENISA nad odpowiednim europejskim schematem/programem certyfikacji – na stronie https://certification.enisa.europa.eu/ można znaleźć informację o trzech uzgodnionych schematach (dla Common Criteria, usług chmurowych i 5G), ale brak dla EN 17640.

Reasumując, na podstawie rozporządzenia CSA oraz EN 17640 stosowanie Wspólnych Kryteriów nie jest konieczne do badań i certyfikacji takich urządzeń, jak liczniki smart. Można bazować na Europejskiej Normie EN 17640, która definiuje, co ma być dostarczone przez producenta i jakie mają być czynności laboratoriów badawczych. Konieczne jest jednak ustalenie, co będzie dodatkową specyfikacją techniczną i realizacja czynności formalnych – akredytacji laboratoriów i jednostek certyfikujących, co determinuje to rozwiązanie jako możliwe do realizacji w długiej perspektywie czasowej.

# 8. APEL O PODJĘCIE DZIAŁAŃ NA RZECZ POPRAWY CYBERBEZPIECZEŃSTWA W SEKTORZE ENERGETYCZNYM

W obliczu szybkiego rozwoju technologicznego i ciągle zwiększającego się zapotrzebowania na energię elektryczną, sektor energetyczny przechodzi istotne zmiany, które przynoszą ze sobą szereg korzyści, ale także pojawiają się przed nim nowe wyzwania i zagrożenia. Zagrożenia i wyzwania wynikają nie tylko z rozwoju technologii, ale również z sytuacji geopolitycznej, w której się obecnie znajdujemy.

Jednym z osiągnięć rozwoju technologicznego i symbolem zmian zachodzących w gospodarowaniu energią elektryczną są inteligentne liczniki, które oferują niezaprzeczalne korzyści, w postaci efektywniejszego zarządzania, bieżącego monitorowania zużycia oraz zrównoważonego jej wykorzystania. Istnieje jednak zagrożenie w postaci nieodpowiedniego zabezpieczenia tych liczników lub ich części składowych przez ich producentów lub dostawców z krajów wysokiego ryzyka, co niesie ze sobą szereg zagrożeń omówionych wcześniej w niniejszym dokumencie. **Ataki hakerskie, backdoory czy bomby logiczne mogą skompromitować nie tylko prywatność obywateli, ale również zdestabilizować całą sieć energetyczną**.

Wdrożenie technologii 5G zwróciło powszechnie uwagę na zagadnienie technologicznej suwerenności i realne zagrożenia płynące z niedostrzegania jej wagi lub koncentracji wyłącznie na aspekcie ekonomicznym wdrażanych w krajach zachodnich technologiach. W związku z powyższym nie możemy dopuścić do zaniechań w dziedzinie cyberbezpieczeństwa, bo jego poprawa w sektorze energetycznym to nie tylko ochrona interesów naszych obywateli, ale także gwarancja stabilności działania polskiej nfrastruktury krytycznej.

**Nie można zagwarantować cyberbezpieczeństwa bez właściwie i instytucjonalnie zapewnionego bezpieczeństwa łańcucha dostaw. Konieczne jest posiadanie przez państwo stosownych, skutecznych instrumentów prawnych i technicznych i to nie tylko w sektorze energii elektrycznej, ale w całym obszarze gospodarki i życia obywateli, jednak ze szczególnie wzmocnioną odpornością w sektorze publicznym i infrastrukturze krytycznej. Dlatego niniejszą ekspertyzą apelujemy o wprowadzenie nieodzownych a oczekiwanych, odpowiedzialnych i efektywnych działań, aby zapewnić przyszłość, która ma być zarówno nowoczesna, bezpieczna, jak i zrównoważona**.

# SŁOWNIK POJĘĆ

| | |
|---|---|
| AMI | Advanced Metering Infrastructure |
| Backdoor | (pol. „tylne drzwi, furtka") – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania do nieuprawnionego dostępu |
| Bomba logiczna | Złośliwe oprogramowanie uruchamiające się po spełnieniu określonych warunków (np. nadejście określonej daty, zalogowanie się konkretnego użytkownika lub określona liczba uruchomień programu) |
| CERT | Computer Emergency Response Team |
| CSA | Cyber Security Act |
| Common Criteria - ISO/IEC 15408:2022 | Norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych |
| EN 17640 | Dokument opisujący metodykę oceny cyberbezpieczeństwa systemów teleinformatycznych, którą można wdrożyć przy wykorzystaniu wcześniej określonych zasobów czasowych i obciążeniowych |
| ENISA | The European Union Agency for Cybersecurity |
| EOG | Europejski Obszar Gospodarczy |
| Hardening | Proces rekonfiguracji systemów teleinformatycznych, mający na celu zwiększenie bezpieczeństwa rekonfigurowanego systemu |
| ISO/IEC 27001 | Norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji |
| KSE | Krajowy System Elektroenergetyczny |
| LZO | Licznik Zdalnego Odczytu |
| Man in the middle | Atak teleinformatyczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy |
| NIS2 | Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii |
| OECD | Organizacja Współpracy Gospodarczej i Rozwoju |
| OSD | Operatorzy Systemów Dystrybucyjnych |
| PCA | Polskie Centrum Akredytacji |
| SOC | Security Operations Center |
| SZBI | System Zarządzania Bezpieczeństwem Informacji |
| UKSC | Ustawa o Krajowym Systemie Cyberbezpieczeństwa |
| URE | Urząd Regulacji Energetyki |


Materiał przygotowany przez:

ComCERT SA
ul. Adama Branickiego 13
02-972 Warszawa

Apator SA
ul. Gdańska 4a lok. C4
87-100 Toruń
e-mail: rzecznik.prasowy@apator.com
www.apator.com

2023.091.PL