

Pakiet antyblackoutowy

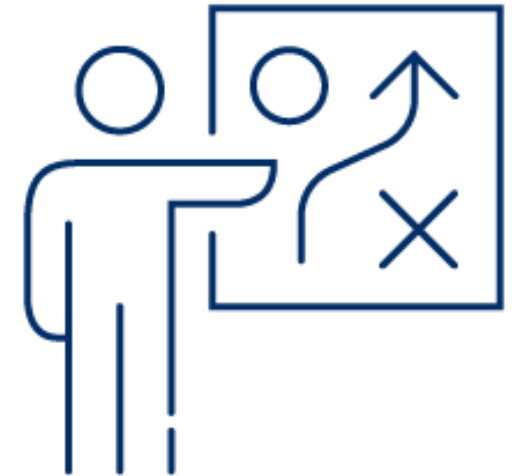
Local content i cyberbezpieczeństwo

Problem

- Rosnący udział urządzeń istotnych dla pracy KSE, których odporność na zagrożenia cyberbezpieczeństwo jest nieznana
- Brak jednolitych standardów certyfikacji tego typu urządzeń
- Rosnące znaczenie energetyki „niezawodowej”, w której przestrzeganie zasad cyberbezpieczeństwo jest głównie dobrą wolą producentów i użytkowników.

Rozwiązania

- Nominowanie PSE S.A. na sektorowy CSIRT w obszarze elektroenergetyki jako naturalne uzupełnienie obowiązków i uprawnień OSP w zapewnianiu bezpiecznej pracy systemu.
- Wprowadzenie wymogów certyfikacyjnych dla urządzeń przyłączanych do KSE celem uzyskania jak najmniejszej podatności na cyberataki.
- Nałożenie na kluczowe podmioty w sektorze obowiązków w zakresie m.in.
 - podstawowych zasad cyberhigieny w mechanizmach kontroli dostępu do kluczowych systemów,
 - zapewnienia bezpieczeństwa funkcjonowania stosowanych systemów sterowania (security by design),
 - zapewnienia zdolności do obsługi incydentów i zarządzania incydentami (dedykowane centra SOC/CERT/CSIRT),
 - corocznego przeprowadzania testów oraz audytów bezpieczeństwa, oraz współpracy z sektorowym CSIRT w tym zakresie
- Nałożenie analogicznych obowiązków także na operatorów mniejszych urządzeń przyłączonych do sieci OSD oraz na podmioty nimi zarządzające, np. agregatorów, itd.



Problem

- Zwiększone ryzyko dla bezpieczeństwa krytycznej infrastruktury energetycznej w warunkach obecnej niepewności geopolitycznej, zwłaszcza zależności od dostaw spoza UE
- Uzależnienie od długich, globalnych łańcuchów dostaw, które są podatne na przerwania i opóźnienia
- Ryzyko ograniczonej dostępności i trudności w zapewnieniu szybkiego serwisu oraz obsługi technicznej krytycznych urządzeń
- Niewystarczające wykorzystanie potencjału krajowych i unijnych producentów urządzeń oraz dostawców usług ICT, co ogranicza rozwój lokalnych zdolności serwisowych i produkcyjnych.

Rozwiązania

- Zmiana prawa zamówień publicznych w taki sposób, aby umożliwić zamawiającemu wskazanie, że część produkcji lub świadczenia usług musi odbywać się na terytorium UE, a w przypadku zamówień o szczególnym znaczeniu (np. infrastruktura krytyczna) także w Polsce.
- Rozszerzenie katalogu kryteriów oceny ofert poprzez wprowadzenie kryteriów „local content” i „eu-content”, czyli przyznawania dodatkowych punktów ofertom z określonym udziałem komponentów wytworzonych w Polsce lub w UE.
- Zastosowanie dla uzasadnionych kategorii zamówień, tzn. dla strategicznych projektów wzmacniających bezpieczeństwo energetyczne) mechanizmów proporcjonalności i obiektywizmu. Kryteria oceny będą punktowe, a nie eliminacyjne, co pozwoli uniknąć naruszeń zasady równego traktowania i przejrzystości wynikającej z prawa unijnego.



Wprowadzenie krajowych wymogów certyfikacyjnych dla urządzeń przyłączanych do sieci

- Obowiązkowa certyfikacja urządzeń przyłączanych do sieci oraz narzędzi wykorzystywanych do zarządzania nimi (np. SCADA).
- Stworzenie krajowego rejestru certyfikowanych dostawców komponentów infrastruktury energetycznej, obejmującego m.in. inwertery, systemy sterowania i moduły komunikacyjne.
- Uwarunkowanie dopuszczenia dostawcy do zamówień publicznych uzyskaniem certyfikacji potwierdzającej zgodność z normami bezpieczeństwa krajowego i europejskiego – model wzorowany na systemie certyfikacji NIS2 i ENISA.
- Wprowadzenie procedury obowiązkowego okresowego audytu bezpieczeństwa już zainstalowanej infrastruktury – z możliwością cofnięcia zgody eksploatacyjnej w przypadku wykrycia zagrożeń.
- Wymogami należy objąć agregatorów i operatorów urządzeń takich jak moduły wytwarzania energii (w tym OZE), magazynów energii czy dużych instalacji odbiorczych. Regulacja powinna dotyczyć także m.in. lokalnego i zdalnego sterowania oraz funkcjonalności zmiany w trybie on-line nastaw parametrów falowników, urządzeń IoT (Internet of Things), systemów monitoringu.
- Wymagania certyfikacyjne powinny iść w kierunku standaryzacji (ograniczenie liczby dopuszczalnych rozwiązań) i dopuszczać do sprzedaży, instalacji i użytkowania na terenie kraju wyłącznie certyfikowanych urządzeń i oprogramowania, zgodnych z wytycznymi, np. CERT-u sektorowego lub zapisów tzw. cyberustawy.



Przegląd i certyfikacja istniejącej infrastruktury w KSE

- Aby uniknąć sytuacji, w której potencjalne zagrożenia są już obecne w funkcjonującej infrastrukturze, rekomendujemy podjąć działania mitygujące ryzyka cyberataków poprzez:
 - audyty i przeglądy infrastruktury KSE pod kątem cyberzagrożeń i zgodności technologicznej – obejmujący szczególnie komponenty OZE importowane w latach 2015–2024;
 - wdrożenie procedury recertyfikacji komponentów wrażliwych – analogicznie do certyfikacji sprzętu telekomunikacyjnego po wykluczeniu niektórych dostawców;
 - utworzenie niezależnej jednostki nadzorującej proces audytów cyber i certyfikacji sprzętu w sektorze energii, działającej we współpracy z PSE, ABW, UKE, NASK.



Obowiązek posiadania centrów SOC/CERT/CSIRT w dużych instalacjach przyłączonych do KSE oraz u wszystkich podmiotów zajmujących się zarządzaniem pracą takich instalacji

- Obowiązek posiadania SOC (Security Operations Center, czyli centrum operacyjne bezpieczeństwa), które w trybie 24/7 monitoruje, analizuje i reaguje na incydenty bezpieczeństwa.
- Obowiązek posiadania CSIRT (Computer Security Incident Response Team) lub CERT (Computer Emergency Response Team), czyli zespołów reagowania na incydenty komputerowe. CSIRT zajmuje się m.in. analizą incydentów, koordynacją odpowiedzi, raportowaniem i profilaktyką.
- Obowiązek posiadania SIEM (Security Information and Event Management), czyli systemu informatycznego do zbierania, korelowania, analizowania i raportowania danych związanych z bezpieczeństwem IT w czasie rzeczywistym.
- Alternatywnie pozyskanie analogicznych zdolności na zasadzie usługi rynkowej.



Preferencje dla local content i dostawców unijnych

- Nowelizacja Prawa zamówień publicznych w duchu projektowanych zmian (UC88), wprowadzająca jednoznaczną możliwość wykluczania dostawców z państw trzecich (spoza UE i porozumienia GPA), co jest zgodne z wyrokiem TSUE z 22.10.2024 r. (C-652/22).
- Zobowiązanie zamawiających do uwzględniania tzw. wskaźnika local content w Specyfikacji Warunków Zamówienia (SWZ), np. poprzez premiowanie udziału europejskich komponentów, lokalnych podwykonawców i produkcji na terenie Polski.
- Zastosowanie obowiązkowych kryteriów zgodnych z wytycznymi KE dotyczącymi udziału oferentów z państw trzecich – m.in. konstrukcja opisu przedmiotu zamówienia promująca towary europejskie, certyfikaty zgodności z europejskimi normami oraz lokalizację serwisu i wsparcia technicznego na terenie UE.
- Wprowadzenie mechanizmu „zielonego bezpieczeństwa”, czyli połączenia kryteriów zrównoważonego rozwoju z certyfikacją bezpieczeństwa dla każdego dostarczanego komponentu technologicznego.



Zaostrzenie wymagań w zakresie minimalizacji podatności na cyberataki urządzeń przyłączanych do KSE

- Obowiązek fizycznej i logicznej segmentacji sieci związanej z zarządzaniem operacyjnym (OT) w dużych instalacjach OZE, w tym wydzielenie warstw dostępowych dla zarządzania lokalnego OSD/OSP. Segmentacja sieci i ochrona stref OT powinna być dostosowana do stopnia wpływu, jaki dostawca może wyrzucić na KSE;
- Obowiązek stosowania podstawowych narzędzi „cyberhigieny” dla systemów zdalnego dostępu
- Pełna ewidencja użytkowników posiadających dostęp do infrastruktury sterującej, w tym monitoring bądź potwierdzanie operacji sterowania itd.
- Zaostrzenie wymagań dotyczących możliwości zdalnego serwisowania instalacji i zdalnych systemów zarządzania;
- Wymóg przeprowadzania regularnych testów bezpieczeństwa i penetracyjnych podczas przyłączania instalacji do sieci oraz regularnie w czasie okresu eksploatacji instalacji. Co najmniej raz w roku powinien być przeprowadzany audyt i test penetracyjny.



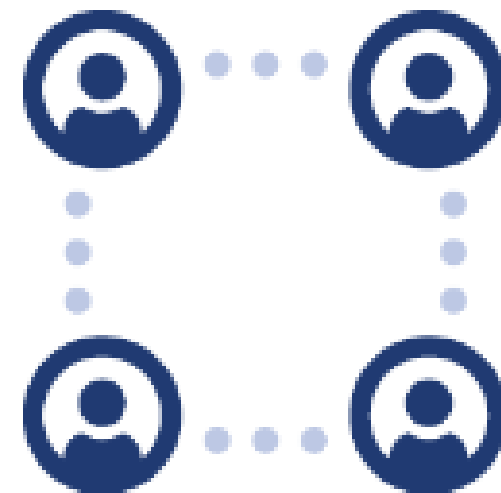
Monitoring, detekcja i szybka reakcja na incydenty cyfrowe

- Utworzenie hierarchicznego ośrodka i mechanizmów monitorowania procesów wymiany informacji w czasie rzeczywistym między podmiotami sektora elektroenergetycznego, w tym zwłaszcza pomiędzy operatorami OSP-OSP, OSP-OSD, OSD-OSD oraz operatorami i pozostałymi podmiotami sektora elektroenergetycznego.
- Wprowadzenie obowiązku zgłaszania incydentów do OSD/OSP i CERT-u sektorowego (od określonego progu, np. zakłócenia wpływające na jakość energii, napięcie, synchronizację).
- Wprowadzenie dla instalacji OZE o określonej mocy obowiązku posiadania wewnętrznych procedur reakcji na incydenty (możliwe jest świadczenie tych usług przez podmioty trzecie), systemów detekcji incydentów (system wykrywania włamań – Intrusion Detection System IDS, system zapobiegania włamaniom – Intrusion Prevention System PIS), ustalonych kanałów zgłoszeniowych do CSIRT/CERT sektorowego.



Ćwiczenia i testy odporności systemowej

- Cykl regularnych ćwiczeń (np. raz na rok), w których uczestniczą operatorzy dużych farm wiatrowych i PV, agregatorzy, OSP/OSD, CERT/CSIRT (NASK, ABW, MON), administracja lokalna.
- Symulacje krajowe i regionalne z udziałem sektora OZE, uwzględniające różne scenariusze, np. masowy atak na farmę PV lub jednego z producentów falowników, skutkujący celowym przeciążeniem sieci przez zdalne wysterowanie falowników lub innym rodzajem destabilizacji racy sieci, awaria synchronizacji farmy z siecią krajową, utrata możliwości zdalnego sterowania instalacją podczas sytuacji zagrożenia pracy KSE, itd.



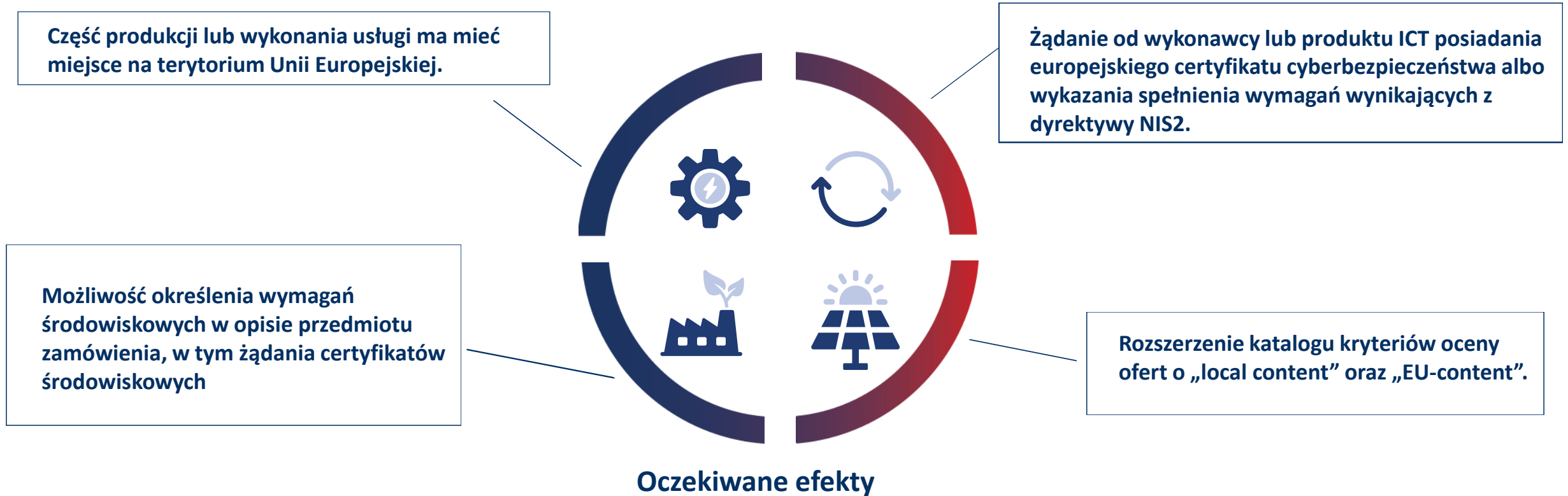
Postulowane zmiany prawne w zakresie ustawy Prawo zamówień publicznych (Pzp)

- Obecne przepisy Pzp dopuszczają już uwzględnianie aspektów środowiskowych (m.in. rachunek kosztów cyklu życia uwzględnia koszty emisji CO₂), jednak brakuje w nich szczegółowych wymogów dotyczących „znaku węglowego”, certyfikatów środowiskowych czy cyberbezpieczeństwa. Nowelizacja zapełnia te luki, realizując cele polityki krajowej i unijnej: wsparcia gospodarki, bezpieczeństwa narodowego oraz zrównoważonego rozwoju.
- Projekt wprowadza zestaw instrumentów, które umożliwiają zamawiającym równoważenie celów bezpieczeństwa dostaw, polityki klimatycznej oraz jakości i konkurencyjności ofert, przy zachowaniu zasad proporcjonalności oraz równego traktowania wykonawców – mając jednocześnie na uwadze umożliwienie maksymalizacji udziału podmiotów polskich oraz unijnych w organizowanych zamówieniach publicznych.



Wyzwania dla Krajowego Systemu Elektroenergetycznego

Plan Rozwoju Sieci Przesyłowej



- Zwiększenie odporności łańcuchów dostaw oraz bezpieczeństwa dostaw w zamówieniach wrażliwych
- Podniesienie poziomu cyberbezpieczeństwa w sektorze publicznym
- Systemowe włączenie wymogów środowiskowych w cały cykl życia zamawianych towarów i usług.