Minister Energii

Rekomendacje Ministra Energii
dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa - uwzględniania wymagań cyberbezpieczeństwa przy realizacji usług podmiotów przyłączonych do Krajowego Systemu Elektroenergetycznego

wydane na podstawie art. 42 ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r.
o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r. poz. 20, z późn. zm.)[1]

Wstęp

Rozwój odnawialnych źródeł energii oznacza nie tylko zmianę sposobu wytwarzania energii, lecz także coraz większe uzależnienie infrastruktury energetycznej od systemów teleinformatycznych, automatyki przemysłowej i zdalnej komunikacji. Farmy fotowoltaiczne i wiatrowe, magazyny energii oraz stacje elektroenergetyczne są dziś elementami złożonego, wzajemnie połączonego systemu, w którym bezpieczeństwo cyfrowe staje się integralną częścią bezpieczeństwa energetycznego. Wraz ze wzrostem cyfryzacji, rośnie również znaczenie właściwego zabezpieczenia nie tylko środowisk IT, ale także OT, urządzeń sterujących, systemów zdalnego dostępu i komunikacji farm z operatorami sieci elektroenergetycznych. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wskazuje, że sektor energii należy do obszarów szczególnie zależnych od technologii ICT, a rosnąca konwergencja systemów IT i OT zwiększa potencjalne skutki incydentów cyberbezpieczeństwa, co zostało także uwzględnione w nowelizacji UKSC, która weszła w życie 3 kwietnia 2026 roku.

W związku z powyższym, w celu zmniejszenia ryzyka związanego z zagrożeniami dla bezpieczeństwa dostaw energii elektrycznej, Minister Energii jako organ właściwy ds. cyberbezpieczeństwa, przygotował niniejsze rekomendacje we współpracy z zespołami CSIRT NASK i CSIRT GOV, RCB, Polskim Towarzystwem Przesyłu i Rozdziału Energii Elektrycznej (PTPiREE), głównymi operatorami systemu dystrybucyjnego oraz operatorem systemu przesyłowego.

[1] Dalej jako: „UKSC”.

Rekomendacje kierowane są do OSD oraz OSP[2] energii elektrycznej, jako podmiotów mających rzeczywisty wpływ na kształtowanie wymagań technicznych i organizacyjnych wobec uczestników przyłączonych do sieci.

Rekomendacje powinny stanowić kluczowy materiał do opracowania lub ujednolicenia wymagań technicznych ujmowanych przez operatorów systemów dystrybucyjnych oraz operatora systemu przesyłowego w odpowiednich dokumentach, w szczególności w instrukcjach ruchu i eksploatacji sieci elektroenergetycznych oraz dokumentach umownych regulujących współpracę z podmiotami przyłączonymi do sieci elektroenergetycznych, w tym w szczególności w umowach przyłączeniowych i dystrybucyjnych.

Niniejszych rekomendacji nie należy traktować jako zbioru technicznych zaleceń wyłącznie dla bezpośrednich adresatów tego dokumentu, czyli operatorów systemów dystrybucyjnych oraz operatora systemu przesyłowego, lecz jako rekomendacje w zakresie wdrażania rozwiązań technicznych dla większości podmiotów związanych ze świadczeniem usługi przesyłu, wytwarzania i dystrybucji energii w Krajowym Systemie Elektroenergetycznym. Celem tych rekomendacji jest zmniejszenie prawdopodobieństwa realizacji skutecznego ataku, skrócenie czasu wykrycia i reakcji na incydent oraz zapewnienie możliwości bezpiecznego funkcjonowania instalacji również
w sytuacji naruszenia jej środowiska cyfrowego.

Równocześnie, te rekomendacje wskazują kierunek zmian, które są nieuniknione, w drodze wzmacniania bezpieczeństwa systemu elektroenergetycznego w Polsce i wyrównywania poziomu dojrzałości, w zakresie cyberbezpieczeństwa, w podmiotach realizujących zadania w sektorze energii.

[2] Podmioty kluczowe w myśl UKSC, świadczące usługi przesyłu i dystrybucji energii elektrycznej, jako przedsiębiorstwa energetyczne o których mowa w art. 3 pkt 24) oraz pkt 25) ustawy z dnia 10 kwietnia 1997 r. - Prawo energetyczne (t.j. Dz.U. z 2026 r. poz. 43, z późn. zm., dalej jako: „Prawo energetyczne”), posiadające koncesję na wykonywanie działalności gospodarczej.

Rekomendacje

Rekomenduje się, aby Operatorzy Systemu Dystrybucyjnego (OSD) oraz Operator Systemu Przesyłowego (OSP) uwzględniali poniższe zagadnienia przy opracowywaniu lub aktualizacji instrukcji ruchu i eksploatacji sieci dystrybucyjnych lub sieci przesyłowej (IRiESD[3], IRiESP[4]) oraz odpowiednich dokumentów umownych z podmiotami przyłączonymi do tych sieci, w szczególności świadczącymi usługi w zakresie wytwarzania energii z OZE lub magazynowania energii elektrycznej.

Rekomenduje się, w celu wzmocnienia cyberbezpieczeństwa Krajowego Systemu Elektroenergetycznego, aby operator systemu dystrybucyjnego oraz operator systemu przesyłowego:

- w treści instrukcji ruchu i eksploatacji sieci elektroenergetycznych właściwych[5] dla danego operatora oraz w odpowiednich dokumentach umownych,
- a także, w odpowiednim zakresie, w dokumentach umownych dotyczących przyłączania i współpracy z podmiotami przyłączonymi do sieci elektroenergetycznych, w szczególności z wytwórcami energii w instalacjach OZE[6], a także podmiotami realizującymi zadania z zakresu magazynowania energii elektrycznej,

uwzględnili podstawowe wymagania techniczne i organizacyjne, w zakresie dotyczącym cyberbezpieczeństwa, obejmującym co najmniej poniższe zagadnienia:

1. Bezpieczeństwo urządzeń komunikacyjnych/brzegowych

Rekomenduje się, aby operatorzy systemów uwzględniali w IRiESD, IRiESP oraz odpowiednich dokumentach umownych podstawowe wymagania dotyczące zabezpieczenia urządzeń zapewniających komunikację instalacji OZE z infrastrukturą operatorów systemów takich, jak routery, zapory sieciowe, urządzenia VPN lub inne urządzenia komunikacyjne.

W szczególności rekomenduje się uwzględnienie wymagań dotyczących:

a) stosowania oprogramowania aktualnego i wspieranego przez producenta, z uwzględnieniem możliwości technicznych rozwiązań oraz analizy ryzyka,

[3] IRiESD - Instrukcja Ruchu i Eksploatacji Sieci Dystrybucyjnej.
[4] IRiESP - Instrukcja Ruchu i Eksploatacji Sieci Przesyłowej.
[5] Instrukcja ruchu i eksploatacji sieci właściwych dla danego operatora, o którym mowa w art. 9g ust. 1 ustawy z 10 kwietnia 1997 r. Prawo energetyczne.
[6] Wytwórca energii w instalacji odnawialnego źródła energii – zgodnie z art. 2 pkt 39) ustawy z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (t.j. Dz.U. z 2026 r. poz. 68, z późn. zm.).

b) stosowania urządzeń objętych wsparciem producenta w zakresie poprawek bezpieczeństwa,
c) zarządzania podatnościami oraz planowania działań ograniczających ryzyko związane z ujawnionymi podatnościami,
d) stosowania bezpiecznej konfiguracji urządzeń, z uwzględnieniem uznanych dobrych praktyk właściwych dla środowisk OT i ICS, a także normy IEC 62443[7],
e) ograniczania dostępu z zewnętrznych sieci bezprzewodowych, z wykorzystaniem dedykowanych lub odpowiednio odseparowanych kanałów komunikacyjnych (np. prywatny APN[8], medium fizyczne).

Ponadto tam, gdzie to jest możliwe, działania powinny obejmować:

- jeżeli zdalny przesył danych telemetrycznych z użyciem sieci komórkowej jest niezbędny – wykorzystanie prywatnych APN lub innych rozwiązań zapewniających logiczną separację ruchu, równocześnie uwzględniając: traktowanie prywatnego APN jako sieci niezaufanej względem sieci OT, ograniczenie komunikacji pomiędzy siecią OT a urządzeniem pełniącym funkcję bramy do prywatnego APN, monitorowanie ruchu pomiędzy siecią OT a prywatnym APN; ograniczenie do niezbędnego minimum liczby otwartych portów dostępnych na interfejsie osiągalnym z prywatnego APN[9], czy też realizacja gdy urządzenie wspiera taką konfigurację: centralne logowanie i monitorowanie zdarzeń z urządzeń będących bramą do prywatnego APN;
- śledzenie komunikatów bezpieczeństwa dotyczących wykorzystywanych urządzeń i uwzględnianie ich w planowaniu działań serwisowych;
- aktualizowanie urządzeń zgodnie z harmonogramem prac serwisowych oraz z uwzględnieniem ryzyka operacyjnego;
- stosowanie segmentacji sieci komunikacyjnej co najmniej na styku sieci obiektowej[10] z innymi sieciami; w większych lub bardziej złożonych instalacjach zasadne jest stosowanie segmentacji również wewnątrz sieci obiektowej;

[7] ISA/IEC 62443 – międzynarodowy zestaw standardów definiujących wymagania i procesy dla cyberbezpieczeństwa systemów automatyki przemysłowej i sterowania (*Industrial Automation and Control Systems*, IACS) oraz infrastruktury OT. Standard ten został opracowany przez *International Society of Automation* (ISA) i przyjęty przez *International Electrotechnical Commission* (IEC).

[8] Prywatny APN – prywatny *Access Point Name* (APN - nazwa bądź adres bramy pomiędzy siecią komórkową operatora a zewnętrzną siecią komputerową, umożliwiającą m.in. routowanie pakietów między tymi sieciami).

[9] Rekomendacje wskazane przez CERT Polska po analizie incydentu z 29 grudnia 2025 r. „Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025", CERT Polska: https://cert.pl/posts/2026/08/uzupelnienie-raportu-incydent-sektor-energii-2025/

[10] Sieć obiektowa (ang. fieldbus) - rodzina przemysłowych, cyfrowych sieci komunikacyjnych przeznaczonych do rozproszonego sterowania w czasie rzeczywistym (IEC 61158 *Industrial communication networks – Fieldbus specifications*).

- dążenie do tego, aby urządzenia krytyczne dla pracy instalacji, takie jak RTU czy sterowniki zabezpieczeń polowych, nie były osiągalne bezpośrednio z urządzeń brzegowych;
- ograniczanie dostępu zdalnego do obiektu wyłącznie do przypadków uzasadnionych operacyjnie. Rekomendowane jest realizowane takiego dostępu z wykorzystaniem tunelu VPN *site-to-site* do zaufanych połączeń wymaganych na stałe lub wykorzystanie dostęp serwisowy z wykorzystaniem wieloskładnikowego uwierzytelniania;
- unikanie bezpośredniego dostępu z Internetu do urządzeń OT oraz do interfejsów administracyjnych urządzeń komunikacyjnych;
- włączanie dostępnych mechanizmów bezpieczeństwa, takich jak weryfikacja integralności firmware, jeżeli są one dostępne i uzasadnione technicznie;
- wykonywanie kopii zapasowych konfiguracji po zmianach oraz ich bezpieczne przechowywanie;
- prowadzenie podstawowej inwentaryzacji wykorzystywanego sprzętu i oprogramowania, obejmującej co najmniej typ urządzenia, wersję oprogramowania, sposób komunikacji oraz informacje niezbędne do zarządzania bezpieczeństwem. W tym rekomendowane jest przechowywanie informacji o dostępnych interfejsach administracyjnych, użytkownikach i ich uprawnieniach, adresacją IP, numerami seryjnymi oraz wersją oprogramowania;
- przeprowadzenie audytu konfiguracji elementów np. prywatnego APN[11], wraz z analizą ryzyka umożliwiającą przejęcie podłączonych urządzeń.

2. Zarządzanie dostępem i bezpieczeństwo uwierzytelniania

Rekomenduje się, aby operatorzy systemów uwzględniali wymagania dotyczące bezpiecznego zarządzania dostępem do urządzeń i systemów wykorzystywanych do komunikacji z OSD lub OSP.

W szczególności rekomenduje się:

a) zakaz stosowania domyślnych danych dostępowych,

b) stosowanie autoryzacji co najmniej wieloskładnikowej dla dostępu zdalnego, tam, gdzie jest to technicznie możliwe i uzasadnione charakterem rozwiązania,

c) stosowanie zasad tworzenia haseł zgodnie z dobrymi praktykami bezpieczeństwa (https://cert.pl/hasla/),

d) zmianę domyślnych danych uwierzytelniających do systemów i urządzeń obiektowych, w szczególności do interfejsów administracyjnych oraz tam, gdzie

[11] Rekomendacje wskazane przez CERT Polska w analizie incydentu z 29 grudnia 2025 r. „Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025", CERT Polska: https://cert.pl/posts/2026/08/uzupelnienie-raportu-incydent-sektor-energii-2025/

to jest możliwe wykorzystanie unikalnych danych uwierzytelniających dla każdego obiektu,

e) wprowadzenie zasad nadawania, zatwierdzania i cofania dostępu zdalnego,

f) ograniczenie dostępu administracyjnego wyłącznie do upoważnionego personelu,

g) prowadzenie aktualnego wykazu osób uprawnionych do administracyjnego i zdalnego dostępu oraz cykliczny przegląd uprawnień (nie rzadziej niż raz na kwartał),

h) rejestrowanie sesji podłączeń,

i) przydzielanie wykonawcom zewnętrznym identyfikatorów o ograniczonym czasie ważności lub ograniczonym zakresie dostępu,

j) wyłączanie nieużywanych kont, usług, protokołów i interfejsów administracyjnych lub diagnostycznych, jeżeli nie są wymagane operacyjnie.

W przypadku stosowania rozwiązań odmiennych od rekomendowanych, warto w procedurach wskazać odpowiednie uzasadnienie takiego rozwiązania, w szczególności z punktu widzenia ograniczeń technicznych danego środowiska lub zastosowanych środków kompensujących.

3. Utrzymanie dostępności i ciągłości łączności

Rekomenduje się, aby operatorzy systemów uwzględniali w dokumentach technicznych i umownych wymagania dotyczące utrzymania sprawnej i bezpiecznej komunikacji pomiędzy instalacjami OZE a OSD lub OSP, w szczególności:

a) zapewnienia dostępności dedykowanych i bezpiecznych (zapewniających separację od sieci komunikacyjnych publicznych) kanałów komunikacji wykorzystywanych do nadzoru i sterowania,

b) stosowania rozwiązań redundantnych w przypadku instalacji uznanych przez operatora za istotne z punktu widzenia pracy sieci elektroenergetycznych lub bezpieczeństwa dostaw,

c) niezwłocznego informowania operatora systemu dystrybucyjnego lub systemu przesyłowego o utracie lub istotnym ograniczeniu łączności,

d) podejmowania działań zmierzających do przywrócenia łączności w możliwie najkrótszym czasie, adekwatnie do charakteru instalacji i znaczenia zakłócenia (zalecany czas nie dłuższy niż 24 godziny).

4. Monitorowanie i wykrywanie incydentów

Rekomenduje się, aby operatorzy systemów uwzględniali wymagania dotyczące monitorowania pracy urządzeń i systemów w zakresie adekwatnym do skali i charakteru instalacji oraz ryzyka związanego z jej przyłączeniem i eksploatacją.

Zalecane jest, aby umowy zawierały wymagania dotyczące monitorowania pracy urządzeń i systemów, jeśli to jest możliwe technicznie, w zakresie:

a) prowadzenia w trybie ciągłym monitoringu ich działania,

b) wykrywania incydentów oraz nietypowych zdarzeń mogących świadczyć o incydencie cyberbezpieczeństwa,

a w szczególności:

i) prowadzenie monitorowania działania urządzeń i systemów istotnych dla komunikacji oraz sterowania,
ii) wykrywanie incydentów oraz nietypowych zdarzeń mogących świadczyć o naruszeniu cyberbezpieczeństwa,
iii) rejestrowanie istotnych zdarzeń technicznych, takich jak próby logowania, zmiany konfiguracji, alarmy oraz komunikaty o stanie urządzeń,
iv) odnotowywanie zdalnych sesji administracyjnych i serwisowych w zakresie adekwatnym do możliwości wykorzystywanego technicznych rozwiązania,
v) rozważenie korzystania z mechanizmów powiadamiania o ekspozycji usług lub urządzeń udostępnianych przez właściwe podmioty krajowego systemu cyberbezpieczeństwa:
   - rejestrowanie zdarzeń sieciowych w obrębie sieci obiektu oraz wykrywanie anomalii w ruchu sieciowym, w szczególności odbiegających od połączeń realizowanych podczas normalnego trybu pracy instalacji;
   - gromadzenie logów technicznych urządzeń OT i IT w centralnym i chronionym przed modyfikacją systemie, z mechanizmami korelacji zdarzeń, automatycznego powiadamiania oraz okresem przechowywania ustalonym na podstawie analizy ryzyka. Natomiast, jeśli to nie jest technicznie możliwe - wówczas co najmniej rejestrowanie logów technicznych urządzeń OT w dziennikach zdarzeń i przechowywania lokalnie przez okres minimum 30 dni;
   - rejestrowanie lub odnotowywanie każdej sesji zdalnego dostępu i czynności na systemach lub urządzeniach OT w formie logów lub nagrań sesyjnych, obejmując co najmniej czas połączenia oraz identyfikator użytkownika;
   - zarejestrowanie się w systemie moje.cert.pl przez podanie wykorzystywanej w instalacji adresacji IP i domen, co pozwoli

na automatyczne powiadamianie o ekspozycji urządzeń lub anomaliach wykrytych przez CERT Polska.

5. Współpraca w przypadku incydentu cyberbezpieczeństwa

Rekomenduje się, aby operatorzy systemów określali zasady współpracy pomiędzy operatorem systemu a podmiotem przyłączonym do sieci elektroenergetycznej w przypadku incydentów cyberbezpieczeństwa, w szczególności w zakresie:

a) możliwie szybkiego przekazywania informacji o incydentach mogących wpływać na łączność, nadzór lub możliwość sterowania instalacją. Rekomendowany jest czas nie dłuższy niż 4 godziny od zdarzenia zidentyfikowanego jako incydent,
b) ustanowienia kanału łączności do osób odpowiedzialnych po stronie zarządcy instalacji na potrzeby pilnego kontaktu,
c) uzgadniania działań ograniczających skutki zakłóceń oraz wspierających przywrócenie bezpiecznej pracy instalacji.

6. Świadomość i kompetencje personelu

Rekomenduje się, aby operatorzy systemów uwzględniali wymagania dotyczące podnoszenia świadomości i kompetencji personelu technicznego odpowiedzialnego za konfigurację, utrzymanie i eksploatację urządzeń oraz systemów wykorzystywanych do komunikacji z siecią elektroenergetyczną.

W szczególności rekomenduje się uwzględnienie:

a) szkoleń z aktualnych zagrożeń cyberbezpieczeństwa w sektorze energii,

b) dobrych praktyk w zakresie bezpiecznej konfiguracji urządzeń i zarządzania dostępem,

c) podstawowych zasad rozpoznawania i zgłaszania incydentów cyberbezpieczeństwa.

Rekomenduje się, aby operatorzy systemów dystrybucyjnych oraz operator systemu przesyłowego uwzględniali niniejszy dokument przy opracowywaniu propozycji zmian w instrukcjach ruchu i eksploatacji sieci elektroenergetycznych oraz przy kształtowaniu odpowiednich wymagań technicznych w relacjach z podmiotami przyłączonymi do sieci elektroenergetycznej.

Zalecane jest, by szczegółowe wymagania wynikające z rekomendacji były równocześnie określone w IRiES i rekomendowane jest, aby OSD oraz OSP

przygotowali propozycje zmian, a także, by aktualizacja IRiES była jednolita dla wszystkich operatorów.

Zalecane jest, by OSD i OSP wdrożyli rekomendacje z uwzględnieniem czasu niezbędnego na przygotowanie i procedowanie dokumentów służących ich realizacji.

Rekomendowane jest również, w celu wzmocnienia bezpieczeństwa dostaw energii, by w przypadku rażącego braku spełnienia wymagań cyberbezpieczeństwa przez wytwórcę OZE, OSD lub OSP rozważył możliwość odmowy przyłączenia danego obiektu lub też, w przypadku już podpisanej rozmowy, rozwiązywał umowę z danym wytwórcą OZE, po dokonaniu analiz możliwości prawnych.

Wdrażając wymagania, wynikające z niniejszych rekomendacji, operatorzy systemów elektroenergetycznych mogą przyjmować podejście polegające na wskazywaniu oczekiwanego poziomu zabezpieczeń oraz wymaganiu uzasadnienia w przypadku zastosowania rozwiązań odmiennych, o ile zapewniają one porównywalny poziom bezpieczeństwa albo są uzasadnione uwarunkowaniami technicznymi lub analizą ryzyka. Zaleca się także uwzględnienie procesu dostosowania do wymagań, np. poprzez rozważenie planu naprawczego, okresu dostosowawczego czy też stopniowania poziomu zgodności zależnie od sukcesywnego wdrażania wymagań. Rekomenduje się także wskazanie mechanizmów weryfikacji spełnienia wymagań obejmujących konieczność cyklicznych audytów cyberbezpieczeństwa, możliwości prowadzenia kontroli ad hoc, jak również obowiązku raportowania poziomu zgodności.

Warto szczególnie uwzględnić, że ten dokument, w formie rekomendacji, jest równocześnie jednym z wielu sygnałów wskazujących kierunek zmian dotyczących wymagań w zakresie wzmocnienia poziomu cyberbezpieczeństwa, które w nadchodzącym czasie będą obowiązywać uczestników rynku energetycznego.

Miłosz Motyka
Minister Energii