



Minister Energii

BM-WPR.0510.225.2026.KK

Warszawa, 15.08.2026

Pan

Włodzimierz Czarzasty

Marszałek Sejmu

Kancelaria Sejmu RP

Szanowny Panie Marszałku,

w nawiązaniu do interpelacji posła Kacpra Płażyńskiego oraz grupy posłów o numerze 18513 w sprawie zagrożenia uzależnienia polskiego sektora energetycznego od Chin w związku z realizacją polityki tzw. zielonej transformacji, poniżej przedstawiam odpowiedzi do zadane pytania.

Ministerstwo Energii traktuje bezpieczeństwo bateryjnych magazynów energii jako istotny element bezpieczeństwa krajowego systemu elektroenergetycznego. Zagadnienie to obejmuje nie tylko fizyczne zabezpieczenie instalacji, lecz również ochronę systemów sterowania, kanałów komunikacji, jak i danych diagnostycznych i operacyjnych przetwarzanych podczas eksploatacji tych urządzeń. Poziom bezpieczeństwa konkretnej instalacji nie może być oceniany wyłącznie przez pryzmat kraju pochodzenia jej producenta. Nie oznacza to jednak, że okoliczność ta pozostaje bez znaczenia. Przy ocenie ryzyka należy brać pod uwagę także strukturę własnościową dostawcy rozwiązań oraz otoczenie prawne, w którym prowadzi on działalność. Ważnym elementem, który powinien zostać objęty analizą, jest również możliwość oddziaływania na niego przez władze państwa trzeciego. Istotnym filarem wzmacniającym krajowe ramy bezpieczeństwa m.in. w tym obszarze jest nowelizacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która weszła w życie w dniu 3 kwietnia 2026 r. i zaimplementowała do polskiego porządku prawnego założenia wynikające z unijnej dyrektywy NIS2, dotyczącej środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE. W załączniku nr 1 do ww. ustawy, w ramach sektora „energia”, uwzględniono podmioty świadczące usługi związane z magazynowaniem energii elektrycznej jako „podmioty kluczowe”. W związku z tym, podmiot spełniający ustawowe kryteria identyfikacji jako podmiot kluczowy, musi zrealizować szereg obowiązków na rzecz zapewnienia cyberbezpieczeństwa. Są to środki służące m.in. zarządzaniu ryzykiem, ochronie systemów i danych, ciągłości działania i reagowania na incydenty. Jest również zobowiązany do zgłaszania incydentów właściwemu zespołowi CSIRT i poddawania organizacji okresowym audytom w zakresie cyberbezpieczeństwa.

Aby wymusić na inwestorach skrupulatne badanie pochodzenia technologii i realizację planów ochrony, ww. nowelizacja wprowadziła rygorystyczny mechanizm sankcyjny, który umożliwia nakładanie kar finansowych za uchybienia w procedurach bezpieczeństwa, w tym za niezastosowanie się do wytycznych dotyczących zabezpieczenia infrastruktury przed zagrożeniami technicznymi lub zignorowanie ostrzeżeń dotyczących dostawców wysokiego ryzyka. Ponadto rozporządzenie wymagane na mocy art. 6ze ust. 4 znowelizowanej ustawy o zarządzaniu kryzysowym opracowuje konkretne standardy bezpieczeństwa konieczne do wdrożenia przez operatora infrastruktury krytycznej. Jeżeli z racji używania komponentów pochodzących z ChRL potencjalny operator IK nie przejdzie pomyślnie audytu zgodności z minimalnymi wymaganiami w zakresie cyberbezpieczeństwa i ciągłości działania, inwestor

docelowo nie otrzyma zgody na eksploatację operacyjną magazynu energii w strukturach Krajowego Systemu Elektroenergetycznego (KSE).

Szczególną rolę w zakresie ochrony przed zdalnym wyłączeniem lub modyfikacją działania odgrywa zachowanie przez polskiego operatora magazynu rzeczywistej kontroli nad procesem jego sterowania. Producent, niezależnie od kraju jego pochodzenia, nie powinien posiadać stałego i niekontrolowanego dostępu administracyjnego, który umożliwiałby mu samodzielne zmienianie konfiguracji, aktualizowanie lub wydawanie poleceń dotyczących pracy urządzeń.

Ustawa o krajowym systemie cyberbezpieczeństwa przewiduje ponadto instrument ochronny, który polega na możliwości uznania dostawcy sprzętu lub oprogramowania za tzw. dostawcę wysokiego ryzyka. Kompetencje w tym zakresie posiada minister właściwy ds. informatyzacji, tj. Minister Cyfryzacji. Postępowanie administracyjne w tym zakresie może zostać wszczęte z urzędu lub na wniosek przewodniczącego Kolegium ds. Cyberbezpieczeństwa – Prezesa Rady Ministrów. Wydanie decyzji w tym zakresie wymaga przeprowadzenia indywidualnej oceny i nie może opierać się wyłącznie na państwie pochodzenia danego dostawcy. W ramach tej oceny, analizowane mogą być zarówno czynniki techniczne, jak i okoliczności związane z bezpieczeństwem państwa.

Za ochronę konkretnej instalacji odpowiada w pierwszej kolejności podmiot będący jej właścicielem lub operatorem. Nie może on ograniczyć się wyłącznie do zapewnień producenta dotyczących bezpieczeństwa produktu. Powinien przeprowadzić własną ocenę ryzyka i na jej podstawie wdrożyć środki organizacyjne i techniczne, odpowiadające charakterowi instalacji oraz potencjalnym skutkom zakłócenia jej działania.

Bezpieczeństwo infrastruktury krytycznej nie może zależeć od dobrej woli producenta ani jego gotowości do współpracy w warunkach napięcia międzynarodowego. Przede wszystkim to podmiot eksploatujący dane rozwiązania techniczne, w ramach prowadzonej przez siebie działalności gospodarczej, jest odpowiedzialny za ich bezpieczeństwo, stąd ww. ustawa skupia się na zobowiązaniu w tym zakresie podmiotów kluczowych i ważnych. Z tego względu zakres wsparcia producenta powinien zostać jednoznacznie określony już na etapie postępowania zakupowego i znaleźć odzwierciedlenie w stosownych umowach. W przypadku poważnego incydentu podstawą działania są krajowe mechanizmy reagowania, w tym właściwy CSIRT sektorowy oraz zespoły CSIRT poziomu krajowego. Pomoc producenta może stanowić istotne wsparcie, jednak nie może ona zastępować zdolności własnych podmiotu lub innych uczestników krajowego systemu cyberbezpieczeństwa do ochrony i odtwarzania działania takiej infrastruktury.

Z wyrazami szacunku
z upoważnienia Ministra

Konrad Wojnarowski
Podsekretarz stanu
15.08.2026