Minister Energii

BM-WPR.0510.304.2026.MK
Warszawa, 04.11.2026

Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Szanowny Panie Marszałku,

w nawiązaniu do skierowanej przez posłankę Olgę Ewę Semeniuk-Patkowską interpelacji nr 20303 *w sprawie przygotowania sektora energetycznego do zagrożeń sabotażowych i cyberataków oraz zapewnienia ciągłości dostaw energii i ciepła*, poniżej przedstawiam odpowiedzi na zadane pytania.

Zagrożenia sabotażowe w obecnej sytuacji geopolitycznej oraz rozwoju technologii, w tym sztucznej inteligencji nie opierają się już tylko na fizycznych dywersjach czy atakach kinetycznych. Można do nich także zaliczyć dezinformację, podkładanie materiałów wybuchowych pod obiekty o szczególnym znaczeniu dla zachowania ciągłości działania usług, podpalanie obiektów, używanie bezzałogowych statków powietrznych lub pojazdów lądowych czy wodnych do fotografowania oraz niszczenia obiektów, a także odwracania uwagi, wszelkie działania floty cieni, czyli niszczenie podwodnej infrastruktury, a także działania związane z cyberprzestępczością. Za wdrażanie rozwiązań mających na celu ochronę systemów sterowania przemysłowego odpowiada przedsiębiorca - właściciel systemu.

W zakresie cyberbezpieczeństwa sektora energii nastąpiła istotna zmiana prawna, tj. została znowelizowana ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], która zaczęła obowiązywać od dnia 3 kwietnia 2026 r. (dalej: ustawa o KSC). Nowelizacja znacząco rozszerzyła sam system cyberbezpieczeństwa o nowe podmioty zobligowane do stosowania przepisów, ale również zakres obowiązków.

Poza powszechnie obowiązującymi standardami mającymi na celu ochronę systemów sterowania przemysłowego, tj. normy ISA/IEC 62443, PN-EN ISO/IEC 27001, PN-EN ISO 22301, PN-EN ISO 3100, Ministerstwo Cyfryzacji opracowało Rekomendacje dotyczące bezpieczeństwa technologii operacyjnych (OT) (NIST SP 800-82r3_wer. 2.0_PL) z dnia 25 czerwca 2024 r. Znowelizowana ustawa o KSC nałożyła nowe przepisy na podmioty, które działają w strategicznych sektorach gospodarki, w tym obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zwiększających bezpieczeństwo systemów informatycznych. Ustawa ta wprowadziła także odpowiedzialność kierowników za realizację zadań z zakresu cyberbezpieczeństwa.

W 2021 roku ówczesny organ właściwy ds. cyberbezpieczeństwa dla sektora energii, którym był Minister Klimatu i Środowiska, opracował „Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów”[2].

[1] Dz. U. z 2026 r. poz. 20, 252, 815, 1003, 1206

[2] Rekomendacje dostępne na stronie: „Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów” - Ministerstwo Klimatu i Środowiska - Portal Gov.pl

+48 (22) 626 43 30
www.gov.pl/energia
kancelaria@me.gov.pl

Ministerstwo Energii
ul. Przemysłowa 26
00-450 Warszawa

Minister Energii monitoruje realizację obowiązków z zakresu cyberbezpieczeństwa zgodnie z ustawą o KSC, jednak znaczna część podmiotów, które uległy cyberatakom, nie podlega tym przepisom. Zakres czynności wobec poszczególnych podmiotów jest dostosowywany do charakteru dostępnych informacji, zidentyfikowanego ryzyka oraz znaczenia świadczonych usług. W zależności od okoliczności, czynności te mogą obejmować analizę dokumentacji, uzyskiwanie dodatkowych wyjaśnień oraz ocenę sposobu realizacji obowiązków i zaleceń wynikających z audytów. Takie podejście pozwala koncentrować nadzór na zagadnieniach wymagających szczególnej uwagi.

Odpowiedzialność dotycząca wdrażania wystosowanych zaleceń leży po stronie sektora prywatnego, opiera się na decyzjach celowych podejmowanych przez ich kierownictwo.

Ww. ustawa nakłada na podmioty kluczowe i podmioty ważne obowiązek zapewnienia bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym. W tym celu obecnie procedowane są konsultacje publiczne projektu ankiety bezpieczeństwa łańcuchów dostaw[3], który zawiera szereg usystematyzowanych zagadnień, aby podmioty kluczowe i ważne uzyskały istotne informacje do zarządzania bezpieczeństwem łańcuchów dostaw. Z drugiej strony usystematyzowana ankieta ułatwi dostawcom sprzętu i oprogramowania przygotowanie niezbędnych informacji z zakresu łańcuchów dostaw.

W obszarze zależności pomiędzy energetyką, ciepłownictwem, wodociągami i łącznością a ryzykiem równoczesnego ataku na kilka elementów systemu, poza ww. ustawą o KSC, warto również wspomnieć o znowelizowanej ustawie o zarządzaniu kryzysowym i Krajowym Planie Reagowania Kryzysowego (KPRK), który zawiera m.in. określenie zadań i obowiązków podmiotów wymienionych w siatce bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków czy opis zasad współpracy podmiotów, w tym wymiany informacji.

W zakresie bezpieczeństwa kontroli dostępu oraz relacji z dostawcami, podmioty prywatne powinny zapewnić ochronę aktywów organizacji udostępnianym dostawcom tak, aby uwzględniała ona analizę ryzyka oraz zawierała stosowne zapisy umowy SLA (Umowa o Gwarantowanym Poziomie Świadczenia Usług). To, jakie rozwiązanie zastosuje wybrany podmiot, jest zależne od przeprowadzonej przez niego analizy i decyzji podjętych na jej podstawie.

Zasady reagowania na incydenty określono w ustawie o KSC. Podmiot kluczowy lub ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług. Kanałem zgłoszeń jest system S46[4], dostęp do systemu jest nadawany dla podmiotów krajowego systemu cyberbezpieczeństwa w sposób ciągły. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV należy monitorowanie cyberzagrożeń i incydentów na poziomie krajowym.

Praktyczne ćwiczenia z zakresu cyberbezpieczeństwa odbywają się cyklicznie na poziomie krajowym i europejskim oraz w ramach NATO. Wśród zrealizowanych można wyróżnić: Kaskada 2026 (obejmowały scenariusz wystąpienia blackoutu czy ukierunkowanie na

[3] Konsultacje publiczne projektu ankiety bezpieczeństwa łańcuchów dostaw – Ministerstwo Cyfryzacji - Portal Gov.pl

[4] S46 Cyber Hub – platforma operacyjna dla uczestników KSC. Służy do zgłaszania i obsługi incydentów, wymiany informacji o cyberzagrożeniach oraz współpracy między CSIRT, organami właściwymi i podmiotami.

doskonalenie działania administracji publicznej), CMX (ich celem było doskonalenie współpracy państw członkowskich NATO), KSC-EXE (skupiające się na sprawdzeniu działania procedur oraz weryfikacji zdolności operacyjnych podmiotów krajowego systemu cyberbezpieczeństwa w sytuacji kryzysowej spowodowanej cyberatakiem), czy Cyber Europe 2024 (których przedmiotem były cyberataki wymierzone w sektor energetyczny UE). Przećwiczono różne scenariusze, których szczegółowy opis przedstawiono w formie raportów o ograniczonym gronie odbiorców.

Zagrożenia dla ludności są wykrywane za pomocą systemu wykrywania zagrożeń, który funkcjonuje w sposób ciągły. Zgodnie z art. 67 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej obowiązek podjęcia działań w zakresie powiadamiania, ostrzegania i alarmowania ludności spoczywa na tym organie administracji publicznej lub podmiocie ochrony ludności, który pierwszy powziął informację o wystąpieniu zagrożenia. Powiadamianie, ostrzeganie i alarmowanie ludności o zagrożeniach następuje za pomocą systemu powiadamiania, ostrzegania i alarmowania o zagrożeniach, nadzorowanego przez ministra właściwego do spraw wewnętrznych.

Z wyrazami szacunku
z upoważnienia Ministra

Piotr Masłowski
Sekretarz stanu
04.11.2026

Do wiadomości: Kancelaria Prezesa Rady Ministrów