Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.18.2026
Warszawa, 16 lutego 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 21 stycznia br. Posła na Sejm RP Pana Macieja Małeckiego w sprawie cyberataków na infrastrukturę energetyczną (interpelacja nr 14677)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie działania podjęto niezwłocznie po grudniowym cyberataku na infrastrukturę energetyczną? Proszę o informację, czy zidentyfikowano sprawców oraz zastosowane narzędzia ataku, a także jakie kroki podjęto w celu zabezpieczenia zaatakowanych elektrociepłowni i systemów OZE przed kolejnymi próbami włamania.

Działania w tej sprawie realizowały zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK i CSRIT GOV, zgodnie z zadaniami tych zespołów i ich zakresem odpowiedzialności określonym odpowiednio w art. 26 ust. 3 i art. 26 ust. 6-7 ustawy o krajowym systemie cyberbezpieczeństwa[1]. W działania włączone były też inne instytucje odpowiedzialne za bezpieczeństwo państwa. Ponadto koordynacja działań była realizowana w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) pod auspicjami Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

Działania zwiększające poziom cyberbezpieczeństwa w sektorze energii realizuje także Ministerstwo Energii, które wykonujące zadania organu właściwego do spraw cyberbezpieczeństwa dla sektora energia (art. 41 i 42 ustawy o KSC).

Ad 2) Czy istnieją szczegółowe plany awaryjne na wypadek częściowo skutecznego ataku (np. scenariusze zapewnienia ciągłości dostaw energii elektrycznej i ciepła dla ludności w przypadku zakłóceń lokalnych)? Proszę również o informację, czy przeprowadzano symulacje lub ćwiczenia reagowania na cyberatak w sektorze energetycznym oraz jakie wnioski z nich wynikły.

Sektor energii jest jednym z sektorów w ramach Krajowego Systemu Cyberbezpieczeństwa (KSC) określonym w ustawie o KSC. W przypadku, gdy podmiot w danym sektorze wyznaczony został przez organ właściwy do spraw cyberbezpieczeństwa jako operator usługi kluczowej (OUK), zobowiązany jest realizować obowiązki OUK określone w art. 8-16a ustawy o KSC w tym m.in. - zgodnie z art. 8 - OUK wdrożyć system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, co obejmuje m.in. wymogi w zakresie zapewnienia ciągłości działania.

Nowelizacji ustawy o KSC, uchwalona przez Parlament na początku bieżącego roku i skierowana do podpisu przez Prezydenta RP, pozwoli systemowo zwiększyć cyberbezpieczeństwo Polski, jak również podnieść poziom odporności na cyberzagrożenia w poszczególnych sektorach, w tym w sektorze energii. W ramach rozwiązań przewidzianych w nowelizacji przewiduje się m.in zastąpienie OUK przez podmioty kluczowe i podmioty ważne, których liczba w skali kraju będzie znacznie większa niż obecnie OUK, jak również

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm.) (dalej: ustawa o KSC)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

będą one obowiązane spełniać bardziej restrykcyjne i lepiej zdefiniowane wymogi w zakresie cyberbezpieczeństwa (nowe art. 8 - 16), co spowoduje obowiązek zapewniania odpowiedniego poziomu cyberbezpieczeństwa przez większą liczbę podmiotów, które są istotne z punktu widzenia bezpieczeństwa państwa, gospodarki i społeczeństwa.

Jednocześnie w ramach systemu ochrony infrastruktury krytycznej, będącego elementem systemu zarządzania kryzysowego, określonego ustawą o zarządzaniu kryzysowym[2]. Wyznaczeni operatorzy infrastruktury krytycznej (IK) muszą realizować obowiązki wynikające z ustawy o zk (m.in. art. 6 oraz opracowywany na podstawie art. 5b Narodowy Program Ochrony Infrastruktury Krytycznej). Obecnie w ramach rządu procedowany jest projekt nowelizacji ustawy o zk, który wdroży w Polsce unijną dyrektywę CER[3], co znacząco wzmocni system ochrony infrastruktury krytycznej, w tym poprzez postawienie szeregu wymogów, które będą musieli spełniać operatorzy IK, zarówno w wymierzę fizycznym jak i cyberbezpieczeństwa (projektowane nowe art. 6ze - 6zj). Zarówno obecne jak i planowane wymogi dla operatorów IK obejmują kwestie związane z zapewnianiem ciągłości działania. Ponadto na poziomie ogólnokrajowym kwestie ciągłości działania obejmuje Krajowy Plan Zarządzania Kryzysowego opracowywane na podstawie ustawy o zk.

Odnosząc się do kwestii ćwiczeń, Ministerstwo Cyfryzacji realizując zadania ministra właściwego do sprawi informatyzacji (art. 45 ustawy o KSC), Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (art. 62 ustawy o KSC) oraz organu właściwego do spraw cyberbezpieczeństwa we właściwych sobie sektorach (art. 42 ustawy o KSC), organizuje krajowe ćwiczenia w zakresie cyberbezpieczeństwa. Informacja o ćwiczeniach KSC-EXE zorganizowanych pod koniec 2025 r. dostępna jest na stronie Ministerstwa Cyfryzacji. Ministerstwo Cyfryzacji prowadzi także wiele różnych typów szkoleń, zarówno specjalistycznych, jak i dotyczących podstaw cyberbezpieczeństwa i higieny cyfrowej, z których bezpłatnie mogą korzystać podmioty KSC, w tym z sektora energii. Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej Bazy Wiedzy cyberbezpieczeństwa na portalu gov.pl.

Ad 3) Na jakim etapie znajduje się realizacja zapowiadanych zmian legislacyjnych, w szczególności prac nad ustawą o Krajowym Systemie Cyberbezpieczeństwa?

Nowelizacji ustawy o KSC została uchwalona przez Parlament na początku bieżącego roku i została skierowana do podpisu przez Prezydenta RP. Ustawa ta zawiera kluczowe rozwiązania prawne, które pozwolą skuteczniej zapewniać cyberbezpieczeństwo Polski, takie jak np. zwiększenie odpowiednich uprawnień poszczególnych instytucji (zapewniających cyberbezpieczeństwo na poziomie krajowym oraz organów właściwych do spraw cyberbezpieczeństwa w poszczególnych sektorach), utworzenie sektorowych zespołów CSIRT, czy instrumenty takie jak polecenie zabezpieczające, czy możliwość wykluczenia dostawców wysokiego ryzyka. Dlatego tak ważne dla bezpieczeństwa państwa, polskiej gospodarki i naszych obywateli jest, aby nowelizacja tej ustawy jak najszybciej weszła w życie w wersji zawierającej te rozwiązania.

Ad 4) Jakie wnioski wyciągnięto z dotychczasowych incydentów, zarówno z grudniowego ataku, jak i wcześniejszych prób cyberataków na wodociągi, szpitale oraz sieci ciepłownicze w 2025 r.?

Pojawiające się incydenty cyberbezpieczeństwa są na bieżąco analizowane, a właściwe wnioski są wdrażane w bieżącym funkcjonowaniu, w tym m.in. za pośrednictwem PCOC (np. wydawanie rekomendacji i komunikatów Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa). W tym kontekście należy wskazać w szczególności na opublikowany

[2] ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122 z późn. zm.) (dalej: ustawa o zk)
[3] Numer z wykazu prac legislacyjnych Rady Ministrów: UC47.

w styczniu 2026 r. Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczący cyberbezpieczeństwa OZE zawierający zalecenia dla podmiotów z sektora energii. Ponadto, aby przekazać wiedzę o przebiegu zdarzeń oraz o technikach zastosowanych przez atakującego, CERT Polska, wchodzący w skład CSIRT NASK, opublikował szczegółowy raport techniczny w tej sprawie: „Raport z incydentu w sektorze energii 29.12".

Należy jednocześnie zauważyć, że kluczowe rozwiązania prawne, które pozwolą skuteczniej zapewniać cyberbezpieczeństwo Polski są przewidziane we wspomnianej w odpowiedzi na wcześniejsze pytania nowelizacji ustawy o KSC.

W kontekście cyberbezpieczeństwa wodociągów należy wskazać na realizowany program Cyberbezpieczne Wodociągi obejmujący kwotę ok. 300 mln zł.

Inne planowane działania zwiększające cyberbezpieczeństwo Polski przedstawione są w projekcie nowej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, która obecnie rozpatrywana jest przez Stały Komitet Rady Ministrów w ramach rządowego procesu legislacyjnego[4].

Ad 5) W jaki sposób doświadczenia te przekładają się na zmiany w procedurach bezpieczeństwa oraz organizacji służb odpowiedzialnych za cyberbezpieczeństwo? W jaki sposób Rząd zamierza zrealizować zapowiadaną „autonomizację i polonizację systemów bezpieczeństwa" w sektorze energetycznym? Proszę o informację, czy planowane są inwestycje w krajowe rozwiązania technologiczne służące cyberochronie sieci energetycznych oraz ograniczenie stosowania urządzeń zagranicznych mogących stwarzać ryzyko dla bezpieczeństwa (np. niecertyfikowanych elementów systemów sterowania). Jakie konkretne kryteria bezpieczeństwa technologicznego będą stosowane wobec dostawców technologii dla sektora energii?

Pojawiające się incydenty cyberbezpieczeństwa są na bieżąco analizowane, a właściwe wnioski są wdrażane w bieżącym funkcjonowaniu poszczególnych instytucji, jak również przekładają się na projektowane zmiany przepisów prawa. Bezpieczeństwo łańcuchów dostaw jest wzmacniane przez ustawę o krajowym systemie certyfikacji cyberbezpieczeństwa[5]. Dalsze wzmocnienie bezpieczeństwa łańcuchów dostaw przewidziane jest ww. nowelizacji ustawy o KSC, w tym poprzez procedurę umożliwiającą wykluczenie dostawców wysokiego ryzyka, czy poprzez obowiązki przewidziane dla podmiotów kluczowych i podmiotów ważnych.

Jednocześnie należy wskazać, że zgodnie z art. 226 ustawy Prawo Zamówień Publicznych[6], zamawiający jest zobowiązany odrzucić ofertę, jeżeli obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa[7]. Ponadto, ww. art. 226 PZP przewiduje też, że zamawiający musi odrzucić ofertę jeśli jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób.

W kontekście polonizacji należy wskazać na działania dotyczące zwiększenia udziału polskich firm w łańcuchach dostaw dla strategicznych inwestycji z wiodącą rolą

[4] Numer z wykazu prac legislacyjnych Rady Ministrów: ID131.
[5] ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. z 2025 r. poz. 1017.)
[6] ustawa z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz.U. z 2024 r. poz. 1320 z późn zm.) (dalej jako: PZP)
[7] Wykaz obowiązujących rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa dostępny jest na portalu dane.gov.pl.

Ministerstwa Aktywów Państwowych i Zespołu do spraw Udziału Komponentu Krajowego w Kluczowych Procesach Inwestycyjnych.

Dodatkowo należy podkreślić, że ww. projekt nowej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, przewiduje także działania w zakresie podniesienia poziomu odporności systemów informacyjnych; zwiększania potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienia suwerenności technologicznej RP w obszarze cyberbezpieczeństwa; wzmocnienia bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym; stymulowania badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa. Warto w tym aspekcie wskazać choćby na taką wytyczną wskazaną w projektowanej Strategii, jak: *„Instytucje publiczne i spółki Skarbu Państwa, w ramach dopuszczonych prawem formach, w tym przy poszanowaniu reguł rynku wewnętrznego UE, będą ukierunkowywać swoje działania, aby korzystać przede wszystkim z rozwiązań cyberbezpieczeństwa rodzimych polskich firm, w przypadku, gdy są one konkurencyjne i spełniają wymagania zamawiającego. Pozwoli to zbudować w RP silne marki i sektor cyberbezpieczeństwa oraz będzie wspierać ekspansję zagraniczną polskich przedsiębiorstw z branży cyberbezpieczeństwa, a także przełoży się na wzmocnienie suwerenności państwa w zakresie technologii oraz strategicznej autonomii decyzyjnej. Przyczyni się to także do uniezależnienia od wielkich zagranicznych korporacji technologicznych. Jednocześnie będą podejmowane działania, aby przyciągać do RP zagraniczne inwestycje związane z cyberbezpieczeństwem."*

Ad 6) Czy Polska wystąpiła o wsparcie lub wymianę informacji w ramach UE/NATO po grudniowym cyberataku?

Polska nie wystąpiła w tej sprawie o wsparcie w ramach Unii Europejskiej i NATO. Jednocześnie współpraca w zakresie cyberbezpieczeństwa z państwami sojuszniczymi realizowana jest na bieżąco, w tym na szczeblu ministerstw, zespołów CSIRT, służb specjalnych.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa