Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.14.2026
Warszawa, 25 stycznia 2026 r.

Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 20 stycznia 2026 r. Posłów na Sejm RP Pani Magdaleny Małgorzaty Kołodziejczak, Pana Henryka Szopińskiego, Pań Renaty Rak, Alicji Łuczak oraz Pana Stanisława Gorczycy w sprawie wzmocnienia odporności infrastruktury energetycznej na zagrożenia cybernetyczne (interpelacja nr 14691)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Ad 1) Jakie działania o charakterze systemowym są obecnie podejmowane w celu dalszego zwiększania odporności infrastruktury energetycznej na zagrożenia cybernetyczne?

Ministerstwo Cyfryzacji, w tym jako urząd obsługujący Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, realizuje przede wszystkim zadania związane z bezpieczeństwem cyberprzestrzeni w wymiarze cywilnym[1] oraz zadania Pełnomocnika w dotyczące koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa[2]. W związku z tym realizowane przez Ministerstwo Cyfryzacji działania dotyczą pośrednio zwiększenia cyberbezpieczeństwa sektora energii lub jest to element szerszych działań. Ministerstwo Cyfryzacji we współpracy z innymi instytucjami KSC podejmuje w szczególności następujące działania zwiększające cyberbezpieczeństwo Polski, które uwzględniają też cyberbezpieczeństwo sektora energii:

- regulacyjno-systemowe, np.:
    - skierowany do Sejmu RP projekt nowelizacje ustawy o KSC (druk 1955), który wdroży w Polsce dyrektywę NIS 2 (ustawa ta znacząco wzmocni też sektor energii, m.in. poprzez wzmocnienie kompetencji organów właściwych do spraw cyberbezpieczeństwa oraz utworzenie w poszczególnych sektorach sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego – w tym sektorze energii);
    - przygotowywana nowa Strategia Cyberbezpieczeństwa RP, w której przewidziano przedsięwzięcia podnosząca poziom cyberbezpieczeństwa zarówno w wymiarze krajowym jak i sektorowym;
- szkoleniowo-kompetencyjne i kadrowe, np.:
    - liczne inicjatywy szkoleniowe, dla ogółu społeczeństwa, dla różnych grup społecznych, dla specjalistów – z których mogą korzystać także podmioty z sektora energii;
    - Fundusz Cyberbezpieczeństwa zapewniający w sektorze publicznym konkurencyjne wynagrodzenia dla specjalistów ds. cyberbezpieczeństwa w stosunku do sektora prywatnego;

[1] Art. 12a ust. 1 pkt 10 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. z 2025 r. poz. 1275)
[2] art. 62 ust. 1 ustawy 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

- programy wsparcia dla poszczególnych sektorów, np.:
    - rozwój CSIRT-ów sektorowych (66 mln zł);
    - Cyberbezpieczny Samorząd (1,5 mld zł), Cyberbezpieczny Rząd (271 mln zł);
- organizacyjno-koordynacyjne, np.:
    - działania Kolegium do Spraw Cyberbezpieczeństwa na poziomie strategiczno-politycznym;
    - Połączone Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) na poziomie operacyjnym (pozwala na szybką koordynację działań i wymianę informacji, w tym z udziałem Ministerstwa Energii oraz w odniesieniu do incydentów w sektorze energii);
    - rekomendacje i komunikaty dla podmiotów KSC wydawane przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (co oddziałuje także na sektor energii);
- techniczne, np.:
    - system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) zapewniany przez Ministerstwo Cyfryzacji na potrzeby własne i 9 innych instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym (co pośrednio oddziałuje także na cyberbezpieczeństwo w sektorze energii);
    - środki bezpiecznej łączności Komunikator i SKR-Z zapewniane przez Ministerstwo Cyfryzacji – w tym wykorzystywane przez Ministerstwo Energii);
    - system AntyDDoS, którym Ministerstwo Cyfryzacji zapewnia osłonę przed atakami DDoS dla kilkudziesięciu instytucji publicznych;
    - system zarządzania cyberbezpieczeństwem S46 zapewniany przez Ministerstwo Cyfryzacji (z którego korzystają m.in. organy właściwe do spraw cyberbezpieczeństwa oraz OUK – w tym z sektora energii);
    - Portal Cyber.gov.pl – z którego mogą korzystać także podmioty z sektora energii.

Jednocześnie należy podkreślić, że organem właściwym do spraw cyberbezpieczeństwa dla sektora energii, zgodnie z art. 41 ustawy o KSC, jest minister właściwy do spraw energii (obecnie Minister Energii). W związku z tym w zakresie realizacji zadań organu właściwego do spraw cyberbezpieczeństwa, o których mowa w art. 42 ustawy o KSC, właściwy jest Minister Energii i Ministerstwo Energii, które realizuje te zadania, np. związane z wyznaczaniem operatorów usług kluczowych (OUK) w sektorze energii oraz prowadzi kontrole OUK.

Ad 2) W jaki sposób Ministerstwo Cyfryzacji współpracuje w tym zakresie z innymi resortami, w szczególności z Ministerstwem Klimatu i Środowiska oraz z operatorami infrastruktury krytycznej?

Ministerstwo Cyfryzacji współpracuje w zakresie cyberbezpieczeństwa z resortem realizującym zadania organu właściwym do spraw cyberbezpieczeństwa w sektorze energii (Ministerstwo Energii), resortem wcześniej realizującym te zadania (Ministerstwo Klimatu i Środowiska) oraz innymi podmiotami KSC, w szczególności instytucjami zapewniającymi cyberbezpieczeństwo na poziomie krajowym.

Incydenty w sektorze energii są przedmiotem prac Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) z udziałem m.in. zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSRIT) poziomu krajowego, służb specjalnych, Policji, Rządowego Centrum Bezpieczeństwa, ale także Ministerstwa Energii.

W odniesieniu do cyberbezpieczeństwa sektora energii należy wskazać, że Pełnomocnik Rządu do Spraw Cyberbezpieczeńtwa wydał w styczniu 2026 r. komunikat[3] w tej sprawie, opracowany dzięki współpracy Ministerstwa Cyfryzacji z zespołami CSIRT poziomu krajowego: CSIRT NASK i CSIRT GOV.

Ministerstwo Cyfryzacji bierze także udział w spotkania poświęconych cyberbezpieczeństwu sektora energii z udziałem właściwych w tej sprawie podmiotów.

Ad 3) Czy planowane jest wzmocnienie kompetencji i zasobów instytucji odpowiedzialnych za reagowanie na incydenty cybernetyczne w obszarze energetyki?

Rozpatrywany obecnie przez Parlament projekt nowelizacji ustawy o KSC pozwoli systemowo zwiększyć cyberbezpieczeństwo Polski, jak również podnieść poziom odporności na cyberzagrożeń w poszczególnych sektorach.

Nowelizacja zakłada m.in. powołanie sektorowych CSIRT (w tym w sektorze energii), które zastąpią powoływane obecnie fakultatywnie sektorowe zespoły cyberbezpieczeństwa, mające bardziej ograniczoną rolę w KSC. Ministerstwo Cyfryzacji realizuje projekt, w ramach którego planuje się przeznaczyć ze środków KPO 66 mln zł na rozwój CSIRT-ów sektorowych, w tym dla CSIRT Energia.

Ponadto, nowelizacja zakładania włącznie do Kolegium do Spraw Cyberbezpieczeństwa (organ odpowiedzialny za zarządzanie cyberbezpieczeństwem Polski na poziomie strategiczno-politycznym) organów właściwych do spraw cyberbezpieczeństwa w poszczególnych sektorach, w tym dla sektora energii. Pozwoli to m.in. lepiej synchronizować działania podejmowane w poszczególnych sektorach.

Należy również zwrócić uwagę, że nowelizacja przewiduje także wprowadzenie instrumentów, które dadzą prawne możliwości odpowiedniego reagowania na cyberzagrożenia (przy zachowania proporcjonalności i transparentności), takie jak polecenie zabezpieczające, czy możliwość wykluczenia dostawców wysokiego ryzyka.

Ad 4) Czy doświadczenia wynikające z ostatnich zagrożeń zostaną wykorzystane przy aktualizacji krajowych strategii i planów dotyczących cyberbezpieczeństwa?

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).

Należy jednocześnie wskazać, że kluczowe rozwiązanie prawne, które pozwolą skuteczniej zapewniać cyberbezpieczeństwo Polski są przewidziane w rozpatrywany obecnie przez Parlament projekcie nowelizacji ustawy o KSC, takie jak np. zwiększenie odpowiednich uprawnień poszczególnych instytucji (zapewniających cyberbezpieczeństwo na poziomie krajowych oraz organów właściwych do spraw cyberbezpieczeństwa w poszczególnych sektorach), 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 5) Czy rozważane są dodatkowe działania edukacyjne lub szkoleniowe skierowane do podmiotów zarządzających infrastrukturą energetyczną, w celu podniesienia standardów bezpieczeństwa cyfrowego?

[3] https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-dotyczacy-cyberbezpieczenstwa-oze

Ministerstwo Cyfryzacji prowadzi 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[4].

Należy również wskazać na wspomniany w odpowiedzi na pytanie nr 2 Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczący cyberbezpieczeństwa OZE zawierający zalecenia dla podmiotów z sektora energii.

Ad 6) W jaki sposób Sejm Rzeczypospolitej Polskiej może być na bieżąco informowany o kierunkach działań rządu w tym obszarze, z poszanowaniem zasad bezpieczeństwa państwa?

Ministerstwo Cyfryzacji niezmiennie pozostaje w gotowości, aby przedstawiać informacje na posiedzeniach właściwych komisji sejmowych, w tym na posiedzeniach organizowanych w trybie niejawnym.

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

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[4] https://www.gov.pl/web/baza-wiedzy/szkolenia

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

ul. Królewska 27
00-060 Warszawa