



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.175.2026
Warszawa, 04 października 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 1 września br. Posłów na Sejm RP, Państwa Dariusza Mateckiego, Małgorzaty Golińskiej, Marka Subocza, Zbigniewa Ziobro w sprawie działań krajowego systemu cyberbezpieczeństwa po cyberataku na Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie (interpelacja nr 19356)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Działania w sprawie incydentu cyberbezpieczeństwa w Samodzielnym Publicznym Wojewódzkim Szpitalu Zespolonym w Szczecinie realizował zespół reagowania na incydenty bezpieczeństwa komputerowego CSIRT NASK oraz CSIRT CeZ, zgodnie ze swoimi ustawowymi kompetencjami.

Koordinacja działań w tej sprawie realizowana była w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), które działa w trybie niejawnym.

Podkreślić należy, że zespoły CSIRT (poziomu krajowego i sektorowe) utrzymują ciągły kontakt z właściwymi podmiotami KSC, w tym z sektora ochrony zdrowia, m.in. dystrybuują informacje o zagrożeniach, podatnościach, wskaźnikach kompromitacji (IoC), jak również wspierają je w obsłudze incydentów, gdy te mają miejsce.

W marcu 2026 r. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa wydał komunikat zaleceniami dla sektora ochrony zdrowia i innych podmiotów KSC, opracowany we współpracy Ministerstwa Cyfryzacji, CSIRT CeZ oraz CSIRT NASK i CSIRT GOV¹.

Jednocześnie należy zauważyć, że po wejściu w życie 3 kwietnia 2026 r. nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa², wiele podmiotów z sektora ochrony zdrowia zostało objętych podwyższonymi wymogami cyberbezpieczeństwa jako podmioty kluczowe lub podmioty ważne. Nakłada to na te placówki medyczne obowiązek m.in. wdrożenia systemu zarządzania bezpieczeństwem informacji, prowadzenia szacowania ryzyka, stosowania uwierzytelniania wieloskładnikowego (MFA), zapewnienia ciągłości działania oraz dbałości o bezpieczeństwo łańcucha dostaw. Szczegółowe wymogi w zakresie cyberbezpieczeństwa określa art. 8 ustawy o KSC.

Ponadto Ministerstwo Cyfryzacji wspiera rozwój CSIRT CeZ oraz cyberbezpieczeństwo w sektorze ochrony zdrowia m.in. w ramach inwestycji z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) kwotą 13,1 mln zł. Równolegle prowadzone są stałe programy szkoleniowe i edukacyjne (m.in. PWCyber, KSCedu) oraz ćwiczenia krajowe (KSC-EXE) podnoszące praktyczne kompetencje podmiotów KSC, w tym z sektora ochrony zdrowia.

¹ <https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa--zalecenia-dla-sektora-ochrony-zdrowia-i-innych-podmiotow-ksc>

² Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm) (dalej: ustawa o KSC)

Zwracam jednocześnie uwagę, że zgodnie z art. 41 ustawy o KSC, zarówno w ówczynie obowiązującym stanem prawnym, jak i obecnie, organem właściwym ds. cyberbezpieczeństwa dla sektora ochrony zdrowia jest Minister Zdrowia.

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

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych