Minister Zdrowia

EZDW.050.6.2025.MM
Warszawa, 05 sierpnia 2025

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na Interpelację nr 10455 z dnia 25 czerwca 2025 r. Pana Posła Piotra Górnikiewicza w sprawie zagrożeń wynikających z niedostatecznego poziomu cyberbezpieczeństwa w podmiotach wykonujących działalność leczniczą oraz działań podejmowanych przez Ministerstwo Zdrowia w celu jego poprawy, proszę przyjąć poniższe wyjaśnienia:

1. **Jakie działania podejmuje Ministerstwo Zdrowia w celu zwiększenia poziomu cyberbezpieczeństwa w placówkach ochrony zdrowia?**

Kluczowym działaniem w celu zwiększenia poziomu cyberbezpieczeństwa była decyzja Ministra Zdrowia z dn. 1 grudnia 2023 r. na podstawie której w Centrum e-Zdrowia został powołany Zespół Reagowania na Incydenty Bezpieczeństwa (Cyber Security Incident Response Team), w celu realizacji zadań Sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego w sektorze ochrony zdrowia (CSiRT CeZ). Podstawą funkcjonowania ww. Zespołu jest ustawa z dn. 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, z późn. zm.). Zakres zadań Sektorowych CSIRT reguluje przede wszystkim art. 44 ww. Ustawy, zgodnie z którym są to w szczególności:

1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 ww. ustawy;
3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu;
4) współpraca z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

W celu analizy stanu cyberbezpieczeństwa w sektorze ochrony zdrowia Centrum e-Zdrowia prowadzi m.in. dobrowolne badania ankietowe. Wyniki ostatniego badania pt.:

telefon: +48 22 250 01 46
adres email: kancelaria@mz.gov.pl
www.gov.pl/zdrowie

ul. Miodowa 15
00-952 Warszawa

„Badanie Informatyzacji Placówek Medycznych", które było już VIII edycją, opublikowane zostały pod adresem: https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2025-03/8.%20Edycja%20Badania%20stopnia%20informatyzacji%20podmiot%C3%B3w%20wykonuj%C4%85cych%20dzia%C5%82alno%C5%9B%C4%87%20lecznicz%C4%85_11.03.2025%20%282%29_0.pdf. Aspektom cyberbezpieczeństwa poświęcony został Rozdział 12 wskazanej publikacji.

Zespół CSIRT CeZ prowadzi również inne analizy poziomu cyberbezpieczeństwa w sektorze ochrony zdrowia. Ostatnie tego typu badanie przeprowadzone w postaci ankiety w sieci szpitali pozwoliło zebrać dane o stanie cyberbezpieczeństwa w 415 podmiotach.

Dodatkowo, CSIRT CeZ realizuje działania o charakterze rozwojowym. W ramach naboru ze środków KPO nr KPOD.05.10-IW.06-003/24 pozyskał dofinansowanie w wysokości ponad 13 mln zł na rozwój CSIRT CeZ. Obecnie trwa procedura podpisania Porozumienia o dofinansowanie projektu z Centrum Projektów Polska Cyfrowa. Zakłada on kompleksowe działania, uwzględniające m.in.: znaczne zwiększenie możliwości monitorowania zagrożeń oraz reagowania na nie, zwiększenie możliwości propagowania dobrych praktyk, podnoszenie poziomu dojrzałości zespołu CSIRT CeZ, inwestycje w infrastrukturę informatyczną oraz podnoszenie kompetencji kadry CSIRT CeZ, jak również działania promocyjne i edukacyjne skierowane do sektora ochrony zdrowia.

Ponadto Ministerstwo Zdrowia w kwietniu 2025 r. ogłosiło nabór do konkursu „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), gdzie na cyfrową transformację ochrony zdrowia przeznaczone zostanie ponad 3 mld zł i jest on skierowany do podmiotów leczniczych zakwalifikowanych do tzw. sieci szpitali. Jednym z kierunków dofinansowania jest zwiększenie poziomu cyberbezpieczeństwa w szpitalach co w efekcie zapewni wyższy poziom ochrony danych pacjentów, co jest kluczowe w dobie rosnących zagrożeń w cyberprzestrzeni.

2. **Czy Ministerstwo planuje uruchomienie programów centralnego wsparcia merytorycznego, technicznego i finansowego w zakresie cyberbezpieczeństwa?**

Pragnę poinformować, że Zespół CSIRT CeZ prowadzi bieżące działania związane z zapewnieniem wsparcia merytorycznego oraz technicznego podmiotom sektora ochrony zdrowia. Oprócz kanałów komunikacji związanych ze zgłaszaniem incydentów, CSIRT CeZ udostępnia również kanał komunikacji mailowej - info@csirt.cez.gov.pl, na który mogą zgłaszać się placówki sektora ochrony zdrowia w celu uzyskania wsparcia merytorycznego, jak również uzyskać wzory dokumentów do wykorzystania np. dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). W 2025 r. zespół CSIRT CeZ zamieścił na swojej stronie internetowej 31 komunikatów oraz 7 publikacji, w tym Fundamentalne wytyczne w zakresie ochrony przed cyberatakami, zalecenia pt.: „Ransomware – czym jest i jak działa?" czy też opublikowany w dniu 18 czerwca 2025 r. podręcznik dotyczący zakresu tzw. security awareness.

W zakresie wsparcia finansowego, tak jak zostało to wskazane w odpowiedzi na pytanie nr 1, Ministerstwo Zdrowia w kwietniu 2025 r. ogłosiło nabór do konkursu „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" ze środków KPO, gdzie na cyfrową transformację ochrony zdrowia przeznaczone zostanie ponad 3 mld zł i jest on skierowany do podmiotów leczniczych zakwalifikowanych do tzw. sieci szpitali.

3. **Czy w ocenie Ministerstwa istnieje zagrożenie, że obecny poziom zabezpieczeń informatycznych w jednostkach medycznych może doprowadzić do incydentów zagrażających zdrowiu lub życiu pacjentów?**

Obecnie występująca w podmiotach architektura usług w placówkach sektora ochrony zdrowia powoduje, że prawdopodobieństwo wystąpienia zdarzenia związanego z cyberbezpieczeństwem, mającego bezpośredni wpływ na stan zdrowia i życia pacjentów jest bardzo niskie. CSIRT CeZ monitoruje i analizuje wszelkie przypadki, które mogą mieć wpływ na bezpieczeństwo zdrowia i życia pacjentów. Należy zauważyć, że zapewnienie odpowiedniego poziomu cyberbezpieczeństwa może mieć pośredni wpływ np. poprzez brak dostępu do dokumentacji medycznej lub dostępności urządzeń analizy medycznej, skutkujący opóźnieniem zaplanowanych zabiegów. Z doświadczenia CSIRT CeZ wynika, że w sytuacji poważnych ataków, podmioty najczęściej przechodzą na tryb pracy opierający się o dokumentację papierową co pozwala na dalsze świadczenie usług.

4. **Czy przewidziane są działania edukacyjne i szkoleniowe dla kadry medycznej i administracyjnej w zakresie cyberbezpieczeństwa?**

Pragnę poinformować, że Zespół CSIRT CeZ przygotował cykl webinarów dotyczący obrony przed atakami ransomware. Dotychczas zorganizowano 7 webinarów, w których wzięło udział 411 osób ze szpitali. Zaplanowane są kolejne spotkania, najbliższe 15 lipca oraz 5 sierpnia br. Ponadto prowadzone są spotkania kierowane do placówek obszaru ochrony zdrowia, dotyczące poprawy świadomości z zakresu cyberbezpieczeństwa . W 2024 r. przeprowadzono 6 spotkań, w których wzięły udział 434 osoby. W 2025 r. zorganizowano 9 spotkań, w których wzięło udział 439 osób. Ww. cykle spotkań będą dalej kontynuowane przez CSiRT CeZ. Planowane jest uruchomienie kolejnego, stricte technicznego szkolenia związanego z zagadnieniami ransomware. W związku z pozyskaniem środków z KPO CSiRT CeZ planuje znaczące poszerzenie oferty szkoleniowej skierowanej do podmiotów. Działania szkoleniowe będą adresowane zarówno do personelu medycznego, jak i niemedycznego, w tym kadry zarządzającej jednostkami oraz pracowników IT. Pracownicy CSiRT CeZ uczestniczą w konferencjach dedykowanych kadrze zarządzającej w podmiotach ochrony zdrowia, organizowanych m. in. przez Mazowieckie Centrum Biznesowe Sp. z o.o. i Polski Instytut Rozwoju Biznesu Sp. z o.o. Prelekcje poświęcane są cyberbezpieczeństwu w kontekście nadchodzących zmian wynikających z nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa oraz promowaniu CSIRT CeZ jako wsparcia dla podmiotów w sektorze ochrony zdrowia.

5. **Czy Ministerstwo monitoruje dane na temat ataków lub incydentów w zakresie cyberbezpieczeństwa placówek ochrony zdrowia, jeśli tak — jak kształtują się te dane w ostatnich latach?**

W ramach działalności Zespołu CSIRT CeZ na bieżąco monitorowany jest obszar cyberbezpieczeństwa w sektorze ochrony zdrowia. W 2024 ww. Zespół monitorując zagrożenia oraz doniesienia branżowe pozyskał i przeanalizował informacje o 910 podatnościach, z czego 18 było podatnościami krytycznymi. W 2025 r. było to 160 podatności, z czego 48 krytycznych, obejmujących infrastrukturę IT w podmiotach sektora ochrony zdrowia. Aby ostrzec o nich CSIRT CeZ w 2024 r. opublikował 6 komunikatów, a w 2025 r. jest to już 31 komunikatów. O najpoważniejszych z nich podmioty informowane były drogą mailową – 17 razy w bieżącym roku. Głównie dominowały podatności umożliwiające zdalne wykonanie kodu, eskalację uprawnień oraz nieautoryzowany dostęp, często występujące w oprogramowaniu sieciowym, służącym do wykonywania kopii zapasowych oraz w środowisku chmurowym.

telefon: +48 22 250 01 46
adres email: kancelaria@mz.gov.pl
www.gov.pl/zdrowie

ul. Miodowa 15
00-952 Warszawa

W 2025 r. w okresie od stycznia do czerwca CSIRT CeZ zarejestrował 792 incydenty a w analogicznym okresie w 2024 r. 470 incydentów, co potwierdza niestety rosnącą tendencję liczby zagrożeń w cyberprzestrzeni. Poniższa tabela przedstawia klasyfikację zarejestrowanych w 2025 r. incydentów.

Kategoria incydentu	**Liczba**
Obraźliwe i nielegalne treści	44
Szkodliwe oprogramowanie	90
Gromadzenie informacji	11
Próby włamań	11
Włamania	22
Dostępność zasobów	17
Atak na bezpieczeństwo informacji	6
Oszustwa komputerowe	311
Podatne usługi	238
Wycieki poświadczeń	29
Inne	13
Złośliwa domena	0
RAZEM	**792**

Z wyrazami szacunku
z upoważnienia Ministra Zdrowia
Marek Kos
Podsekretarz Stanu
/dokument podpisany elektronicznie/