



Minister Zdrowia

EZBT.050.2.2026.KS
Warszawa, 22 września 2026

Pan
Włodzimierz Czarzasty
Marszałek
Sejmu Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w związku ze skierowaną do Ministra Zdrowia Interpelacją nr 19353 z dnia 1 września 2026 r. w sprawie skutków cyberataku na Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie, bezpieczeństwa danych pacjentów, procesu odbudowy infrastruktury informatycznej oraz działań podjętych przez resort zdrowia w celu ochrony placówek medycznych przed kolejnymi atakami, poniżej zamieszczam odpowiedzi na zadane w Interpelacji pytania, przygotowane we współpracy z Centrum e-Zdrowia:

Pytanie nr 1

Czy na dzień udzielania odpowiedzi na niniejszą interpelację wszystkie systemy informatyczne SPWSZ w Szczecinie zostały już w pełni przywrócone do normalnego działania? Proszę o wskazanie daty pełnego odtworzenia infrastruktury oraz przedstawienie harmonogramu przywracania najważniejszych systemów – w szczególności dokumentacji medycznej, rejestracji pacjentów, diagnostyki laboratoryjnej i obrazowej, systemów obsługi oddziałów oraz systemów administracyjnych.

Odpowiedź:

Zgodnie z uzyskanymi z Centrum e-Zdrowia (dalej: CeZ) informacjami systemy informatyczne związane z realizacją usług ochrony zdrowia przez Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie (dalej: SPWSZ w Szczecinie), do których poprawnego funkcjonowania konieczne jest połączenie z systemami centralnymi zostały w pełni odtworzone (np. e-recepta, e-skierowanie). Szczegółowe harmonogramy odtwarzania wszystkich systemów szpitala są w posiadaniu SPWSZ w Szczecinie.

Pytanie nr 2

Jakie były rzeczywiste skutki cyberataku dla udzielania świadczeń zdrowotnych? Ilu pacjentów zostało dotkniętych utrudnieniami, ile wizyt, badań, zabiegów lub hospitalizacji zostało odwołanych, przesuniętych albo wykonanych z opóźnieniem oraz czy stwierdzono przypadki, w których brak dostępu do systemów informatycznych lub dokumentacji medycznej miał wpływ na bezpieczeństwo pacjentów albo przebieg leczenia?

Odpowiedź:

Ministerstwo Zdrowia (dalej: MZ) oraz CeZ informują, że czasowa niedostępność części systemów teleinformatycznych oraz związane z nią utrudnienia w dostępie do dokumentacji medycznej skutkowały jedynie przejściowymi trudnościami w dostępie do usług lub procesów w SPWSZ w Szczecinie. Jednocześnie – co do zasady – ciągłość udzielania świadczeń zdrowotnych została zachowana, a podmiot stosował przewidziane procedury awaryjne umożliwiające prowadzenie procesu leczenia i obsługę pacjentów. Szczegółowe informacje dotyczące ewentualnych braków w dostępie do systemów teleinformatycznych lub dokumentacji medycznej, które skutkowałyby zagrożeniem dla życia lub zdrowia pacjentów bądź wymagały zmiany przyjętego postępowania terapeutycznego są dostępne w SPWSZ w Szczecinie oraz Oddziale Regionalnym NFZ.

Pytanie 3

Jaki jest, według aktualnej wiedzy Ministerstwa Zdrowia, Centrum e-Zdrowia oraz SPWSZ, rzeczywisty zakres naruszenia danych osobowych? Proszę podać liczbę osób, których dane mogły zostać objęte incydem, rodzaje i kategorie danych oraz wskazać czy potwierdzono ich skopiowanie lub wyprowadzenie poza infrastrukturę szpitala, opublikowanie, sprzedaż bądź inne wykorzystanie przez osoby nieuprawnione.

Odpowiedź:

Szczegółowymi informacjami dotyczącymi rzeczywistego zakresu naruszenia powinien dysponować SPWSZ w Szczecinie jako administrator danych odpowiedzialny za analizę incydem i realizację obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej: RODO). Według informacji posiadanych przez CeZ, właściwy podmiot leczniczy zgłosił naruszenie ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.

Zgodnie z art. 4 pkt 7 RODO, administratorem danych pacjentów jest podmiot, który samodzielnie określa cele i sposoby przetwarzania tych danych. W przypadku danych osobowych pacjentów przetwarzanych w związku z udzielaniem świadczeń zdrowotnych funkcję administratora danych pełni właściwy podmiot leczniczy.

Zgodnie z art. 24 ust. 1 oraz art. 33 i 34 RODO obowiązek dokonania oceny ryzyka naruszenia praw lub wolności osób fizycznych, zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz w przypadkach określonych w RODO, zawiadomienia osób, których dane dotyczą, spoczywa na administratorze danych.

Ocena zakresu naruszenia, jego skutków oraz zasadności podejmowania poszczególnych działań wynikających z przepisów o ochronie danych osobowych pozostaje zatem w kompetencji administratora danych (SPWSZ w Szczecinie), odpowiedzialnego za ich przetwarzanie, w ramach prowadzonej działalności leczniczej.

Pytanie nr 4

W jaki sposób zrealizowano obowiązek poinformowania osób, których dane mogły zostać naruszone? Ilu pacjentów lub innych osób poinformowano indywidualnie, kiedy rozpoczęto i zakończono ten proces, jakimi kanałami przekazywano informacje oraz czy na dzień odpowiedzi istnieją osoby objęte naruszeniem, których nie udało się skutecznie powiadomić?

Odpowiedź:

Zgodnie z art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator

danych bez zbędnej zwłoki zawiadania o naruszeniu osobę, której dane dotyczą. W związku z powyższym na SPWSZ w Szczecinie, jako administratorze, spoczywa obowiązek poinformowania pacjentów o wycieku. Szczegółowe dane na temat realizacji obowiązku informacyjnego posiada SPWSZ w Szczecinie.

Pytanie nr 5

Czy ustalono techniczną przyczynę skutecznego włamania do infrastruktury SPWSZ? Bez ujawniania informacji, których publikacja mogłaby zagrozić bezpieczeństwu systemów, proszę wskazać, czy źródłem skutecznego ataku była podatność techniczna, niewłaściwa konfiguracja systemów, przejęcie danych uwierzytelniających, czynnik ludzki lub inne zaniedbanie oraz czy przed 8 marca 2026 r. SPWSZ był poddawany audytom lub testom cyberbezpieczeństwa prowadzonym bądź finansowanym przez podmioty podległe Ministrowi Zdrowia.

Odpowiedź:

Dane, w tym logi procesu uwierzytelniania, które pozwoliłyby na jednoznaczną identyfikację pierwotnego wektora ataku posiada Zarząd Centralnego Biura Zwalczania Cyberprzestępczości w Szczecinie, który zabezpieczał materiał dowodowy. Postępowanie w tej sprawie prowadzi Prokuratura Okręgowa w Krakowie.

Pytanie 6

Jak dokładnie wyglądała pomoc udzielona SPWSZ przez Ministerstwo Zdrowia i CSIRT CeZ? Proszę wskazać daty rozpoczęcia i zakończenia działań, liczbę zaangażowanych specjalistów, zakres wykonanych prac, ich koszt oraz poinformować, czy po zakończeniu działań został sporządzony raport, analiza incydentu lub rekomendacje dla SPWSZ. Jeśli tak, proszę o przedstawienie najważniejszych wniosków i zaleceń.

Odpowiedź:

Sektorowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Ochrony Zdrowia (dalej: CSIRT CeZ) od momentu zgłoszenia incydentu udzielał wsparcia podmiotowi objętemu incydem. Działania te prowadzone były od dnia 8.03.2026 r. do dnia 31.07.2026 r. Do szpitala w dn. 18.03.2026 r. zostało skierowanych 3 specjalistów CSIRT CeZ, celem wsparcia obsługi incydentu na miejscu.

CeZ nie prowadziło wyceny udzielonego wsparcia, ponieważ jego zakres mieści się w obowiązkach wynikających z art. 44 ustawy o krajowym systemie cyberbezpieczeństwa (dalej: ustawa o KSC), określającego zadania Sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego. Szczegółowe rekomendacje dotyczące incydentu były na bieżąco przekazywane do podmiotu.

Zgodnie z art. 37 ustawy o KSC udostępnianie informacji dotyczących podatności, incydentów i cyberzagrożeń podlega ograniczeniu.

Pytanie 7

Jaki był łączny koszt usunięcia skutków cyberataku i odbudowy lub wymiany infrastruktury informatycznej SPWSZ oraz z jakich źródeł wydatki te zostały sfinansowane? Proszę również wskazać, czy Ministerstwo Zdrowia, Centrum e-Zdrowia lub inne jednostki podległe resortowi przekazały szpitalowi dodatkowe środki finansowe, sprzęt lub oprogramowanie.

Odpowiedź:

CSIRT CeZ udzielał SPWSZ w Szczecinie wsparcia merytorycznego i operacyjnego w zakresie obsługi oraz koordynacji działań związanych z reagowaniem na incydent bezpieczeństwa. CeZ nie prowadził wyceny udzielonego wsparcia, ponieważ jego zakres mieścił się w obowiązkach realizowanych przez CSIRT CeZ, wynikających z art. 44 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Wsparcie realizowane przez CeZ miało charakter ekspercki i operacyjny oraz stanowiło wykonanie ustawowych zadań w zakresie reagowania na incydenty bezpieczeństwa teleinformatycznego w sektorze ochrony zdrowia.

Kwestie związane z kosztami usunięcia skutków incydu, odbudowy lub wymiany infrastruktury teleinformatycznej pozostają w zakresie zarządzania i działalności podmiotu leczniczego tj. SPWSZ w Szczecinie.

Pytanie 8

Jakie konkretne działania systemowe Ministerstwo Zdrowia podjęło po cyberataku w Szczecinie w celu zwiększenia bezpieczeństwa pozostałych szpitali w Polsce? Proszę wskazać, czy po 8 marca 2026 r. przeprowadzono lub zlecono audyty, testy podatności albo kontrole w innych placówkach, ilu podmiotów one dotyczyły, w ilu wykryto poważne lub krytyczne podatności oraz czy Ministerstwo posiada informacje o ich usunięciu. Proszę również wskazać, jakie obowiązkowe zalecenia lub standardy bezpieczeństwa wprowadzono w następstwie tego incydu.

Odpowiedź:

Znowelizowana ustawa o KSC, która weszła w życie 3 kwietnia 2026 r. nakłada na szpitale spełniające przesłanki uznania za podmiot kluczowy albo podmiot ważny obowiązki w zakresie zarządzania cyberbezpieczeństwem, zabezpieczenia systemów informacyjnych oraz obsługi i zgłaszania incydentów. Obowiązki te obejmują w szczególności:

- wdrożenie systemu zarządzania bezpieczeństwem informacji, systematyczne szacowanie ryzyka, monitorowanie systemów, zarządzanie podatnościami, aktualizowanie oprogramowania oraz stosowanie odpowiednich zabezpieczeń technicznych i organizacyjnych, zgodnie z art. 8 ustawy;
- opracowanie i aktualizowanie dokumentacji bezpieczeństwa, zgodnie z art. 10 ustawy;
- obsługę i terminowe zgłaszanie incydentów poważnych oraz podejmowanie działań naprawczych, zgodnie z art. 11 i 12 ustawy;
- powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo albo zawarcie umowy z wyspecjalizowanym dostawcą takich usług, zgodnie z art. 14 ustawy;
- w przypadku podmiotu kluczowego, przeprowadzanie na własny koszt, audytu bezpieczeństwa co najmniej raz na trzy lata, zgodnie z art. 15 ustawy.

Zakres i termin realizacji obowiązków wynikających z ustawy o KSC zależą jednak od statusu danego szpitala jako podmiotu kluczowego albo podmiotu ważnego oraz od przewidzianych w ustawie okresów dostosowawczych.

W zakresie prowadzonych działań systemowych, CSIRT CeZ przygotował i opublikował pod adresem <https://csirt.cez.gov.pl/pl/aktualnosci/jak-zwiekszyc-bezpieczenstwo-danych-medycznych-zalecenia-dla-dostawcow-platform-it> dokument pn. Zalecenia bezpieczeństwa dla dostawców platform IT w ochronie zdrowia. Stanowią one praktyczny materiał, który pomaga ocenić poziom zabezpieczeń systemów, zidentyfikować obszary wymagające uwagi i zaplanować dalszy rozwój mechanizmów ochronnych. Zalecenia nie zastępują obowiązków wynikających z przepisów prawa. Służą jako wsparcie przy planowaniu działań związanych z bezpieczeństwem. Dokument jest skierowany do

producentów oprogramowania, dostawców platform IT oraz operatorów systemów wspierających świadczenie usług zdrowotnych, w tym integrujących się z platformą e-zdrowia P1 lub systemami placówek medycznych.

Zasady reagowania na tego rodzaju zdarzenia przedstawiono również uczestnikom wydarzenia „Cyberbezpieczeństwo w szpitalach”, zorganizowanego przez Centrum e-Zdrowia w dniu 11 maja 2026 r. W wydarzeniu uczestniczyli przedstawiciele szpitali oraz instytucji zaangażowanych w reagowanie na incydenty cyberbezpieczeństwa, w tym SPWSZ w Szczecinie, Dowództwa Wojsk Obrony Terytorialnej oraz Centralnego Biura Zwalczenia Cyberprzestępczości. Podczas spotkania przeanalizowano rzeczywisty atak ransomware na szpital w Szczecinie oraz przedstawiono praktyczne zasady działania w pierwszych godzinach po wykryciu incydu, podział ról i odpowiedzialności, zasady współpracy z właściwymi instytucjami, a także zalecenia dotyczące komunikacji i odbudowy systemów.

Ponadto, w związku z ww. incydem CSIRT CeZ, zarówno w trakcie prowadzonych działań, jak i po ich zakończeniu, publikował na stronie <https://csirt.cez.gov.pl/pl> wytyczne, rekomendacje i ostrzeżenia dla podmiotów sektora ochrony zdrowia oraz przekazywał je bezpośrednio zainteresowanym placówkom.

Z wyrazami szacunku
z upoważnienia Ministra Zdrowia
Tomasz Maciejewski
Podsekretarz Stanu
/dokument podpisany elektronicznie/