MARSZAŁEK
WOJEWÓDZTWA
ZACHODNIOPOMORSKIEGO

Szczecin, 19.03.2026 r.

Sz. P. Leszek Dobrzyński
Radny Województwa Zachodniopomorskiego

W odpowiedzi na zapytanie nr 83/2026 z dnia 13 marca 2026 r. dotyczące ataku hakerskiego na infrastrukturę informatyczną Samodzielnego Publicznego Wojewódzkiego Szpitala Zespolonego w Szczecinie, przedstawiam poniższe informacje.

W następstwie ataku, w nocy z 7 na 8 marca 2026 r., Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie (SPWSZ) utracił możliwość wykorzystywania systemów teleinformatycznych. Mimo tego utrzymał ciągłość udzielania świadczeń - przeszedł w tryb pracy awaryjnej opartej o dokumentację papierową. Opieka ambulatoryjna, planowe przyjęcia i oddziały ratunkowe działają, jednak z czasowymi utrudnieniami organizacyjnymi. W dalszym ciągu trwa odzyskiwanie danych, odtwarzanie środowiska i przywracanie usług z udziałem specjalistów i zespołów reagowania. Przywracanie odbywa się stopniowo, z priorytetem usług krytycznych dla bezpieczeństwa pacjentów. Trwają czynności analityczne oraz działania mające na celu uniknięcie ryzyka ponownego zaszyfrowania. Zasoby teleinformatyczne szpitala zarządzane są i nadzorowane przez wewnętrzny dział informatyki, przy wsparciu firm zewnętrznych w wybranych obszarach.
W chwili obecnej Zarząd Województwa Zachodniopomorskiego nie posiada żadnych potwierdzonych informacji o wycieku danych. Natomiast zgodnie z obowiązującymi przepisami Szpital zgłosił naruszenie do Prezesa UODO. Zarekomendowano m.in. zastrzeżenie numeru PESEL, monitorowanie aktywności finansowej i wzmożoną czujność wobec prób oszustw. W chwili obecnej Szpital współpracuje z właściwym CSIRT - zespołem reagowania na incydenty bezpieczeństwa komputerowego, organami ścigania i Prezesem UODO oraz innymi służbami w zakresie przewidzianym przepisami.

Z uwagi na czynności podejmowane przez Prokuraturę Okręgową w Szczecinie, zgodnie z art. 38 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) nie jest możliwe udostępnienie szczegółowych informacji w przedmiotowej sprawie mogących

Urząd Marszałkowski Województwa Zachodniopomorskiego
ul. Korsarzy 34, 70-540 Szczecin, tel. (+48 91) 48 07 243, (+48 91) 48 07 253, fax (+48 91) 48 93 968
www.wzp.pl,, marszalek@wzp.pl

negatywnie wpłynąć na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.

Jednocześnie informuję, iż Zarząd Województwa Zachodniopomorskiego w dniu 9 marca 2026 podjął decyzję o zawarciu porozumienia w zakresie wsparcia Szpitala zasobami kadrowymi oraz sprzętem komputerowym Urzędu Marszałkowskiego Województwa Zachodniopomorskiego. Ponadto w dniu 11 marca 2026 Zarząd Województwa Zachodniopomorskiego uruchomił rezerwę w wysokości 5 mln zł z przeznaczeniem na działania mające na celu zakup niezbędnego sprzętu informatycznego oraz niwelowanie skutków cyberataku na SPWSZ.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (wdrażająca Dyrektywę NIS2) została ogłoszona w Dzienniku Ustaw RP 2 marca 2026 r., poz. 252 i wchodzi w życie z dniem 3 kwietnia 2026 r. Wejście w życie ustawy inicjuje procedury obligujące podległe jednostki (posiadające osobowość prawną) do zwiększenia nadzoru nad cyberbezpieczeństwem oraz dostosowania się do nowych wymogów (m.in. w zakresie zarządzania ryzykiem, zgłaszania incydentów i audytów).
Jeszcze przed atakiem, pismem z dnia 2 marca 2026 r. zainicjowane zostały przeglądy bezpieczeństwa w podległych jednostkach oraz wdrożono działania oceniające gotowość jednostek do spełnienie wymogów oraz zakres prac przygotowawczych w związku z wejściem w życie nowych przepisów.

z up. MARSZAŁKA WOJEWÓDZTWA
Anna Bańkowska
WICEMARSZAŁEK

Urząd Marszałkowski Województwa Zachodniopomorskiego
ul. Korsarzy 34, 70-540 Szczecin, tel. (+48 91) 48 07 243, (+48 91) 48 07 253, fax (+48 91) 48 93 968
www.wzp.pl,, marszalek@wzp.pl