Dane pacjentów w województwie warmińsko-mazurskim słabo chronione przed cyberatakami

Kategoria: Polityka Zdrowotna
Opublikowano: piątek, 16, sierpień 2024 14:14
Małgorzata Orłowska

NiK skontrolowała szpitale w województwie warmińsko-mazurskim pod kątem ochrony danych pacjentów przed cyberatakami oraz ich rzetelnego przetwarzania. Kontrola wykazała, że dostęp do danych medycznych pacjentów w systemach informatycznych miała część personelu niemedycznego, a także byli pracownicy placówek. Odnotowano również poświadczanie nieprawdy podczas wytwarzania dokumentów.

Kontrola przeprowadzona przez Delegaturę NIK w Olsztynie objęła sześć szpitali i jeden ośrodek zdrowia. Były to: Miejski Szpital Zespolony w Olsztynie, Samodzielny Publiczny Zakład Opieki Zdrowotnej w Działdowie, Szpital Miejski św. Jana Pawła II w Elblągu, Szpital Mrągowski im. Michała Kajki Sp. z o.o., Szpital Powiatowy Sp. z o.o. w Pasłęku, Giżycka Ochrona Zdrowia Sp. z o.o. oraz Samodzielny Gminny Zakład Opieki Zdrowotnej w Dywitach. Celem kontroli było ustalenie, czy rozwiązania funkcjonujące w tych podmiotach zapewniły prawidłową ochronę danych pacjentów przed cyberatakami oraz rzetelne ich przetwarzanie.

W okresie objętym kontrolą, tj. w latach 2020-2023 (I półrocze) wszystkie badane jednostki prowadziły działania mające na celu zapewnienie bezpieczeństwa informacji, w tym danych pacjentów. Jednakże w większości z nich (sześć podmiotów) odbywało się to w sposób nierzetelny i/lub nieadekwatny do rodzaju i skali przetwarzanych danych. Nie przestrzegano bowiem w tym zakresie części wewnętrznych regulacji oraz obowiązujących przepisów prawa dotyczących bezpieczeństwa informacji, w tym ochrony danych pacjentów.

Minister Zdrowia uznał w lipcu 2022 r. trzy z siedmiu skontrolowanych podmiotów za operatorów świadczących usługi kluczowe (OUK), mające najważniejsze znaczenie dla krytycznej działalności społecznej lub gospodarczej państwa. Tym samym samodzielny Publiczny Zakład Opieki Zdrowotnej w Działdowie, Szpital Mrągowski oraz Giżycka Ochrona Zdrowia zostały zobligowane do realizacji określonych obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa. Dwie spośród tych trzech jednostek wykonały te obowiązki, przy czym stwierdzono nieprawidłowości, które nie miały istotnego wpływu na realizację zadań w zakresie bezpieczeństwa informacji. Polegały one m.in. na opóźnieniu przekazania danych osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Przychodnie i szpitale mają ustawowy obowiązek wprowadzenia systemu zarządzania bezpieczeństwem informacji opracowanego na podstawie Polskiej Normy (PN-ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania). Co prawa spośród siedmiu skontrolowanych publicznych zakładów opieki zdrowotnej w pięciu opracowano i wdrożono SZBI (Olsztyn, Działdowo, Elbląg, Mrągowo oraz Dywity), jednak w Olsztynie i w Mrągowie tylko niektóre elementy systemu zostały opracowane na podstawie Polskiej Normy, a w Dywitach SZBI zaczął obowiązywać dopiero od 2023 r.

W każdej skontrolowanej jednostce wyznaczono inspektora ochrony danych osobowych (IODO), przy czym w dwóch z nich (Olsztyn oraz Dywity) stwierdzono w tym zakresie istotne nieprawidłowości. W pierwszym przypadku nie zapewniono wsparcia lub zastępstwa IODO, który nie świadczył pracy przez wiele miesięcy. Z kolei w Dywitach IODO został wyznaczony dopiero pod koniec 2022 r.

W okresie objętym kontrolą sześć z siedmiu badanych podmiotów (oprócz SGZOZ w Dywitach)

Kategoria: Polityka Zdrowotna
Opublikowano: piątek, 16, sierpień 2024 14:14
Małgorzata Orłowska
Odsłony: 524

uzyskało dofinansowanie NFZ na inwestycje poprawiające bezpieczeństwo infrastruktury teleinformatycznej w łącznej kwocie blisko 3 mln zł (od 365 tys. zł do 796 tys. zł). W ramach tego dofinansowania zakupiono nowe systemy ochrony sieci wewnętrznej, aplikacji Web i poczty elektronicznej, rozbudowano posiadane systemy, zakupiono system monitorowania infrastruktury, system bezpieczeństwa sieci, system ochrony poczty, zakupiono zapory sieciowe, oprogramowanie antywirusowe, sprzęt komputerowy oraz usługi wdrożeniowe i audytowe.

Kontrolerzy NIK dokonali oględzin sprzętu i programów, służących bezpieczeństwu informacji oraz ochronie danych pacjentów. Łącznie poddano analizie 80 stanowisk komputerowych obsługiwanych przez lekarzy, pielęgniarki i pracowników niemedycznych. Celem było sprawdzenie realizacji postanowień obowiązujących przepisów wewnętrznych (w szczególności SZBI) przez pracowników skontrolowanych placówek medycznych. Podczas oględzin sprawdzono m.in. aktualność systemu operacyjnego i oprogramowania antywirusowego, sposób logowania się użytkowników, w tym liczbę znaków haseł, zawartość pulpitu i folderów systemowych pod kątem danych pacjentów, dostęp do portów usb, a także otoczenie stanowisk pod kątem zapisanych haseł w miejscach ogólnie widocznych.

Tylko w jednej ze skontrolowanych jednostek miał miejsce incydent zagrażający bezpieczeństwu systemu informacyjnego. W Giżyckiej Ochronie Zdrowia Sp. z o.o. w lipcu 2022 r. wystąpił tzw. atak hakerski, mający na celu zaszyfrowanie danych, w wyniku którego utracono czasowo dane dotyczące części komórek administracyjnych Szpitala. W ocenie Spółki nie wystąpiły przesłanki do zgłoszenia naruszenia organowi nadzorczemu, ponieważ nie stwierdzono naruszenia poufności i integralności chronionych danych osobowych, ani ryzyka naruszenia praw lub wolności osób fizycznych. Zaszyfrowane w wyniku ataku dane zostały odzyskane i sprawdzone. W związku z wystąpieniem powyższego zdarzenia Spółka postąpiła zgodnie z procedurą.

Źródło: NIK