Minister
Zdrowia

EZZC.050.10.2025.AD
Warszawa, 30 kwietnia 2025

Pan
Szymon Hołownia
Marszałek
Sejmu Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,
w odpowiedzi na interpelację nr K10INT8866 Pana Janusza Cieszyńskiego – Posła na Sejm Rzeczypospolitej Polskiej, w sprawie zabezpieczenia placówek ochrony zdrowia przed cyberatakami wobec postępującej cyfryzacji i zagrożeń dla ciągłości świadczenia usług medycznych, proszę o przyjęcie poniższych informacji.

Ad. 1. Jakie konkretne działania planują Ministerstwo Zdrowia oraz Ministerstwo Spraw Wewnętrznych i Administracji w celu zwiększenia poziomu cyberbezpieczeństwa w placówkach ochrony zdrowia w Polsce, w szczególności w kontekście niedawnego ataku na Szpital MSWiA w Krakowie?

Ministerstwo Zdrowia wraz z Centrum e-Zdrowia prowadzi liczne działania na rzecz podnoszenia poziomu cyberbezpieczeństwa, a także doskonali techniki i procedury w zespołach cyberbezpieczeństwa.

Od uruchomienia sektorowego zespołu cyberbezpieczeństwa w sektorze ochrony zdrowia (CSIRT CeZ) zwiększana jest systematycznie obsada kadrowa oraz rozszerzane są obszary kompetencji i odpowiedzialności zespołu.
W bieżącym roku realizowane są liczne działania edukacyjne skierowane do kadry kierowniczej oraz specjalistów IT w podmiotach szpitalnych. CSIRT CeZ prowadzi cykl szkoleń dedykowanych dla Zarządów szpitali. Ponadto, w odpowiedzi na ostatni atak CSIRT CeZ rozpoczął nowy cykl szkoleń dotyczących przeciwdziałania oraz radzenia sobie z atakami ransomware. Pierwsze trzy warsztaty zrealizowano w dniach 2, 8 i 10 kwietnia 2025 roku i wzięła w nich udział większość kluczowych podmiotów sektora ochrony zdrowia w Polsce.
W najbliższych miesiącach planowane jest też uruchomienie kolejnego cyklu szkoleń skierowanego do informatyków w szpitalach. Ponadto, w ramach środków z KPO planowane jest znaczne zwiększenie możliwości prowadzenia szkoleń dla całej kadry w szpitalach w kraju.

CSIRT CeZ opracował wytyczne w zakresie ochrony przed cyberatakami w odpowiedzi na ostatni atak oraz krótki poradnik „Jak reagować na ataki ransomware". Wkrótce opublikowany zostanie też podręcznik z zakresu tzw. security awareness, który podmioty wykonujące działalność leczniczą będą mogły udostępnić wszystkim pracownikom. Systematycznie są publikowane materiały, takie jak aktualne ostrzeżenia oraz celowane zalecenia, np. dla usług zdalnego dostępu, VPN-ów czy polityki haseł.
Ze środków z KPO są planowane liczne inwestycje, które umożliwią:

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

ul. Miodowa 15
00-952 Warszawa

• cykliczne monitorowanie wybranych aspektów cyberbezpieczeństwa w szpitalnych podmiotach medycznych,
• zwiększenie możliwości reagowania na realne zagrożenia,
• rozwój kompetencji własnego zespołu.

W ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" wchodzącej w skład komponentu D Krajowego Planu Odbudowy i Zwiększania Odporności, uruchomiono nabór w trybie konkurencyjnym kierowany do 325 szpitali z tzw. sieci szpitali (szpitali zakwalifikowanych do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej). Nabór będzie obejmował m.in. zakup sprzętu i usług IT, w tym na potrzeby zwiększenia poziomu cyberbezpieczeństwa w szpitalach, co ma służyć bezpiecznemu przetwarzaniu dokumentacji medycznej.

Dodatkowo, także ze środków KPO, w ramach naboru niekonkurencyjnego kierowanego do Centrum e-Zdrowia, ma zostać wzmocnione i doposażone Centrum Operacji Bezpieczeństwa. CSIRT CeZ - który będzie sektorowym CSIRT-em na mocy nowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa, rozwinie kompetencje w zakresie wsparcia placówek ochrony zdrowia w Polsce, zarówno w zakresie standaryzacji cyberbezpieczeństwa jak również aktywnego wsparcia na wypadek cyber ataku.

Ad. 2. Czy planowane jest stworzenie kompleksowej strategii cyberbezpieczeństwa dla sektora ochrony zdrowia, uwzględniającej zarówno aspekty technologiczne, jak i kadrowe?

W celu utrzymania pozytywnego trendu w rozwoju e-zdrowia w Polsce, jak również w oparciu o cele wyznaczone przez Ministerstwo Zdrowia, Centrum e-Zdrowia - jako jednostka podległa MZ odpowiedzialna za realizację zadań z zakresu budowy społeczeństwa informacyjnego, obejmujących organizację i ochronę zdrowia oraz wspomaganie decyzji zarządczych ministra właściwego do spraw zdrowia - opracowało strategię rozwoju na lata 2023–2027. Strategia definiuje m.in. misję i wizję, opisuje wartości oraz cele, do których instytucja będzie dążyć. Najistotniejszym jest zapewnienie pacjentom i innym uczestnikom systemu ochrony zdrowia wysokiej jakości e-usług. Ponadto, strategia określa długofalowe cele i pokazuje sposób ich realizacji. W efekcie dokument przekłada się na tworzenie specjalistycznych e-usług, odpowiadających potrzebom wszystkich interesariuszy: pacjentów, podmiotów leczniczych i farmaceutycznych, dostawców oprogramowania medycznego oraz organów administracji publicznej.

Ad. 3. W jaki sposób Ministerstwa zamierzają rozwiązać problem niedoboru specjalistów IT w sektorze publicznej ochrony zdrowia, biorąc pod uwagę znaczną różnicę w wynagrodzeniach pomiędzy sektorem publicznym, a prywatnym?

Od kilku lat działa fundusz celowy na rzecz wsparcia finansowego rządowych specjalistów ds. cyberbezpieczeństwa, znany jako Fundusz Cyberbezpieczeństwa. Jednocześnie, dla zapewnienia adekwatnej do realizowanych zadań obsługi IT, jednostki organizacyjne w ramach swojego budżetu zabezpieczają odpowiednie zasoby kadrowe.

W celu podnoszenia świadomości kadry kierowniczej w zakresie obowiązków i odpowiedzialności działów IT oraz konsekwencji wynikających z ataków na infrastrukturę teleinformatyczną, w ramach działań sektorowego zespołu cyberbezpieczeństwa CSiRT CeZ prowadzone są działania edukacyjne. Kluczem do skutecznych działań jest świadomość organizacji a w szczególności głównego kierownictwa, jak ważna w obecnej dobie cyfryzacji, jest rola pracowników IT oraz działów cyberbezpieczeństwa.

Ad. 4. Czy planowane jest zwiększenie nakładów finansowych na cyberbezpieczeństwo w placówkach medycznych, w tym na modernizację infrastruktury informatycznej oraz szkolenia personelu?

Prowadzone są liczne działania na rzecz podnoszenia poziomu cyberbezpieczeństwa, a także trwa doskonalenie technik i procedur w zespołach cyberbezpieczeństwa.

W bieżącym roku realizowane są liczne działania edukacyjne skierowane do kadry kierowniczej oraz specjalistów IT w podmiotach szpitalnych (szczegółowe informacje zawarto w odpowiedzi na pyt. 1).

Ad. 5. Jakie procedury są obecnie stosowane w przypadku cyberataków na placówki medyczne i czy planowana jest ich standaryzacja oraz udoskonalenie w świetle niedawnych doświadczeń?

Szczegóły procedur nie mogą zostać ujawnione. Przewidują one szybką, bezpośrednią wymianę informacji pomiędzy krajowymi CSIRT-ami, służbami oraz CSIRT-ami sektorowymi w ramach wymaganego zakresu. Wybrane informacje zawarte są w dokumencie SOP (Standard Operation Procedures). Możliwość szybkiej komunikacji pozwala na sprawny podział zadań oraz uzupełnianie działań zespołów w zależności od sytuacji.

Procedury te są rozwijane tak samo jak kompetencje zespołów oraz ich zasoby.
Ponadto Centrum e-Zdrowia podpisało szereg porozumień, które upraszczają współpracę pomiędzy wybranymi zespołami cyberbezpieczeństwa, m.in. z Policją (CBZC), Wojskiem (DK WOC) oraz Państwowym Instytutem Badawczym NASK.

Ad. 6. W jaki sposób Ministerstwa planują zabezpieczyć ciągłość świadczenia usług medycznych w przypadku cyberataków, tak aby zminimalizować ich wpływ na pacjentów?

W przypadku wystąpienia skutecznego cyberataku, w wyniku którego nie ma możliwości skorzystania z infrastruktury IT, CSiRT CeZ w ramach posiadanych zasobów kadrowych i innych uwarunkowań formalnych pomaga jednostce w odbudowie infrastruktury IT. Dysponuje również sprzętem, który do czasu przeprowadzenia niezbędnych czynności w zakresie urządzeń dotkniętych cyberatakiem przez odpowiednie służby, jest wypożyczany zaatakowanej jednostce w celu uruchomienia niezbędnych usług.

Ad. 7. Czy planowana jest modernizacja wytycznych dotyczących minimalnych standardów cyberbezpieczeństwa, które powinny spełniać placówki medyczne w Polsce?

Tak, prace w tym zakresie są planowane na 2025 rok. Ponadto wymienione wymagania będą cyklicznie aktualizowane w celu dostosowania ich do bieżących realiów.

Ad. 8. Jakie są plany w zakresie edukacji i podnoszenia świadomości personelu medycznego na temat zagrożeń związanych z cyberbezpieczeństwem?

Jak już wskazano w ramach odpowiedzi na poprzednie pytania, w bieżącym roku planowane są liczne działania edukacyjne skierowane do kadry kierowniczej oraz specjalistów IT w podmiotach szpitalnych. CSIRT CeZ prowadzi cykl szkoleń dla Zarządów szpitali. W odpowiedzi na ostatni atak CSIRT CeZ rozpoczął nowy cykl szkoleń dotyczących przeciwdziałania oraz radzenia sobie z atakami typu ransomware.
W najbliższych miesiącach planowane jest uruchomienie kolejnego cyklu szkoleń dla informatyków w szpitalach. Ponadto w ramach środków z KPO planowane jest znaczne zwiększenie możliwości prowadzenia szkoleń dla całej kadry w szpitalach w kraju.

CSIRT CeZ opracował nowe wytyczne w zakresie ochrony przed cyberatakami w odpowiedzi na ostatni atak oraz krótki poradnik „Jak reagować na ataki ransomware". Wkrótce opublikowany zostanie podręcznik z zakresu tzw. security awareness. Jest on opracowywany, aby podmioty wykonujące działalność leczniczą mogły go udostępnić wszystkim swoim pracownikom.
CSIRT CeZ publikuje także materiały, takie jak ostrzeżenia oraz inne, celowane zalecenia, np. dla usług zdalnego dostępu, VPN-ów czy polityki haseł.

Ad. 9. Czy ministerstwa planują współpracę międzynarodową w zakresie wymiany doświadczeń i dobrych praktyk dotyczących cyberbezpieczeństwa w ochronie zdrowia?

Zgodnie z obowiązującą ustawą o Krajowym Systemie Cyberbezpieczeństwa Ministerstwo Zdrowia jest zaangażowane w różne działania operacyjne i projektowe na poziomie międzynarodowym, w tym m.in. współpracę z przedstawicielami Komisji Europejskiej w ramach grupy roboczej ds. zdrowia publicznego. Przedstawiciele CSIRT CeZ również są obecnie zaangażowani w aktywności międzynarodowe. Wraz z rozwojem zespołu CSIRT CeZ zaangażowanie w takie działania będzie rosło.

Z wyrazami szacunku
z upoważnienia Ministra Zdrowia
Jerzy Szafranowicz
Podsekretarz Stanu
/dokument podpisany elektronicznie/