Bezpieczne dane pacjentów. Są pieniądze z NFZ dla szpitali na cyberbezpieczeństwo.

Podpisaliśmy już blisko 600 umów ze szpitalami, które chcą zabezpieczyć się przed cyberatakami. Do końca listopada oddziały wojewódzkie NFZ przyjmują wnioski o wsparcie kolejnych inwestycji poprawiających bezpieczeństwo infrastruktury teleinformatycznej. W puli jest jeszcze ponad 200 mln zł. O dofinansowanie mogą starać się szpitale i, od niedawna, także placówki prowadzące pilotaż centrów zdrowia psychicznego. Incydenty, które bezpośrednio zagrażają cyberbezpieczeństwu placówek medycznych, nasiliły się po napaści Rosji na Ukrainę. Szczególnie niebezpieczne i groźne w skutkach mogą być cyberataki na szpitale. Sparaliżowanie infrastruktury informatycznej szpitala może zagrażać zdrowiu, a nawet życiu pacjentów, dlatego tak ważne jest maksymalne zabezpieczenie tych systemów m.in. przed próbami włamań. Atak, który może kosztować życie – Wyciek danych, w tym danych osobowych pacjentów, blokowanie systemu informatycznego, czy szyfrowanie plików przez cyberprzestępców mogą prowadzić do paraliżu i ogromnych strat w podmiotach leczniczych. Mogą także uniemożliwić przeprowadzanie planowanych operacji, co zagraża bezpośrednio życiu i zdrowiu pacjentów – zaznacza Jarosław Olejnik , dyrektor w Centrali NFZ, który od lat zajmuje się sprawami bezpieczeństwa, w tym bezpieczeństwa informatycznego. Gdzie są największe potrzeby szpitali? – Z naszych obserwacji wynika, że dyrektorzy szpitali muszą przede wszystkim inwestować w systemy SIEM, EDR, IPS/IDS, które są podstawowym filarem w zakresie ochrony przed atakami. Pozwalają m.in. skutecznie monitorować systemy teleinformatyczne, serwery i pojedyncze komputery pod kątem wystąpienia incydentów, które są poważnym zagrożeniem dla bezpieczeństwa teleinformatycznego szpitali – wskazuje dyrektor Olejnik. – Ponadto warto rozważyć wprowadzenie podwójnego uwierzytelniania. Braki w tym zakresie znacznie zwiększają ryzyko wycieku danych – dodaje. Ekspert od bezpieczeństwa w NFZ wskazuje też na inne obszary, m.in.: kopie zapasowe (tworzenie, odmiejscowienie i weryfikacja danych) monitorowanie incydentów oraz reagowania na nie ochronę poczty elektronicznej. Kluczowe są też szkolenia kadry zarządzającej. – Efektem tych szkoleń może być zmiana priorytetów zarządczych i w znaczne podniesienie rangi, i poziomu bezpieczeństwa danych medycznych przy relatywnie niskich nakładach. Z przeprowadzonego badania wynika, że niewiele ponad 13% dyrektorów szpitali odbyło szkolenia w zakresie cyberbezpieczeństwa – podsumowuje dyrektor Olejnik. Szpitale wykazują też brak dokumentacji SZBI, czyli nie mają opisanych procedur w zakresie kopii zapasowych, ciągłości działania. – Należy koniecznie stworzyć pakiet dokumentów wzorcowych – szablonów pozwalających na uzupełnienie niedostatków w tym zakresie – precyzuje szef Biura Bezpieczeństwa Informacji i Ciągłości Działania. Już blisko 600 umów na prawie 250 mln zł Dotychczas podpisaliśmy niemal 600 umów na podniesienie poziomu cyberbezpieczeństwa. Ich wartość to prawie 250 mln zł. Nadal do wykorzystania pozostaje ponad 200 mln zł. Wnioski o wsparcie można składać do końca listopada . – Planujemy podpisywanie umów, aż do wyczerpania pełnej puli środków. Aby maksymalnie wykorzystać dostępne środki i ułatwić sięgnięcie po dotacje przez jak najszerszą grupę placówek szpitalnych, Ministerstwo Zdrowia umożliwiło składanie wniosków przez świadczeniodawców prowadzących szpital albo szpitale i posiadającym

umowę lub umowy o udzielanie świadczeń opieki zdrowotnej zawarte z NFZ, co daje możliwość uzyskania dofinansowania na każdy prowadzony szpital – podkreśla dyrektor Olejnik. Kto może otrzymać środki? Wsparcie jest przeznaczone dla szpitali, które wykonują świadczenia w zakresach: leczenie szpitalne rehabilitacja lecznicza lecznictwo uzdrowiskowe opieka psychiatryczna i leczenie uzależnień oraz świadczeniodawcy, którzy: mają umowę albo umowy na opiekę psychiatryczną i leczenie uzależnień, ale nie są podmiotami wykonującymi działalność leczniczą lub posiadają umowę albo umowy na realizację pilotażu w centrach zdrowia psychicznego. Wysokość środków zależy od wartości kontraktu placówki z NFZ. Wsparcie wynosi od ponad 20 tys. zł (w przypadku placówek AOS), dla szpitali minimum to 240 tys. zł, do nawet 900 tys. zł. Co finansujemy? Zakup i wdrożenie systemów teleinformatycznych oraz związanych z nimi usług musi dotyczyć podniesienia poziomu bezpieczeństwa w placówkach leczniczych, nie samej informatyzacji. Za otrzymane środki można kupić i uruchomić: urządzenia, oprogramowanie i usługi teleinformatyczne, które zapobiegają, wykrywają lub zwalczają cyberataki, np. systemy do tworzenia kopii danych, systemy antywirusowe, systemy kontroli dostępu administracyjnego i zarządzania uprawnieniami, urządzenia i oprogramowanie zabezpieczające sieć (firewall), systemy zapewniające bezpieczeństwo poczty elektronicznej. urządzenia i oprogramowanie oraz wsparcie eksperckie dotyczące cyberbezpieczeństwa, technologie, które ułatwiają precyzyjne monitorowanie bezpieczeństwa infrastruktury IT, skany podatności, które pozwalają identyfikować zagrożenia we własnym środowisku IT, opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji, a także przeprowadzić szkolenia z cyberbezpieczeństwa dla kadry zarządzającej i pracowników. Środki na ten cel pochodzą z Funduszu Przeciwdziałania COVID-19. Obejmują wydatki ponoszone od 29 kwietnia do 31 grudnia 2022 roku. Co zrobić, aby otrzymać dofinansowanie? Aby skorzystać z dofinansowania trzeba, do 30 listopada 2022 r., złożyć do Dyrektora właściwego oddziału wojewódzkiego NFZ wniosek o zawarcie umowy. Do wniosku koniecznie należy dołączyć raport z Systemu Statystyki Ochrony Zdrowia, który potwierdza wypełnienie ankiety badającej poziom bezpieczeństwa systemów teleinformatycznych. Warunkiem uzyskania wsparcia przez szpital jest zawarcie umowy i złożenie w siedzibie właściwego oddziału Funduszu, nie później niż do 16 grudnia 2022 r., kilku dokumentów: wniosku o wypłatę finansowania, którego wzór określony jest w załączniku nr 3 do zarządzenia Prezesa NFZ, specyfikacji finansowania, której wzór określony jest w załączniku nr 4 do zarządzenia Prezesa NFZ, kopii dokumentów, które potwierdzają nabycie i sfinansowanie w okresie od 29 kwietnia 2022 roku do 31 grudnia 2022 roku przedmiotu finansowania (kopie dokumentów potwierdzone za zgodność z oryginałem), wyniku audytu bezpieczeństwa. Źródło: Centrala NFZ