Stanowisko Rady do Spraw Cyfryzacji w sprawie cyberbezpieczeństwa w sektorze medycznym.

W ostatnich dwóch latach istotnie wzrosła liczba cyberataków na placówki opieki medycznej, lekarzy i dane pacjentów. Krajobraz zagrożeń w tym sektorze jest zróżnicowany, a skutki incydentów mogą być bardzo poważne. W sektorze ochrony zdrowia dochodzi zarówno do naruszenia poufności danych (włamania i publikacja danych pacjentów i pracowników), naruszenia dostępności (w postaci ataków ransomware, paraliżujących pracę szpitali), a także integralności i autentyczności (poprzez wystawianie recept przez osoby nieuprawnione podszywające się pod lekarzy). Organy ścigania prowadzą postępowania dotyczące przełamania zabezpieczeń rejestrów medycznych, jak również aplikacji gabinetowych. Celem sprawców jest przede wszystkim pozyskanie i wykorzystanie danych pacjentów (dane osobowe, historia wizyt, przebyte choroby, wystawione recepty), personelu medycznego (dane osobowe, dane dostępowe do usług medycznych) i lekarzy (dane osobowe, dane dostępowe do systemów medycznych, certyfikaty lekarskie). Dzięki pozyskanym informacjom sprawcy wpływają na automatyczne przetwarzanie danych w systemach medycznych generując e-recepty, recepty papierowe, certyfikaty odbytych szczepień (COVID-19, szczepień obowiązkowych dzieci). Aktualnie szczególnie głównym celem jest wygenerowanie recept na leki opioidowe, które są następie oferowane do sprzedaży w DarkWeb. Recepty te realizowane są w polskich aptekach, po czym trafiają na rynek polski, a także do krajów Europy zachodniej i północnej. Proceder ten naraża pacjentów na niedostępność określonych leków, a skarb państwa na wymierne straty finansowe. Do realizacji przestępczego celu sprawcy wykorzystują różne luki i podatności systemu. Część z nich, na podstawie ustaleń podjętych w toku postępowań karnych, została usunięta, jednak sprawcy nadal z sukcesem uzyskują dostęp do danych i możliwości generowania recept wykorzystując luki i podatności, których usunięcie wymaga zmian legislacyjnych lub współdziałania wieku podmiotów sektora medycznego. Aktualnie podstawowe metody kompromitacji danych bazują na przejmowaniu danych dostępowych lekarzy i podszywaniu się pod nich, jak również na wykorzystaniu podatności i luk bezpieczeństwa komercyjnego oprogramowania wspierającego działalność podmiotów leczniczych (tzw. aplikacji gabinetowych) oraz certyfikatów podmiotu i lekarzy pracujących w danej placówce medycznej. Umożliwia to sprawcom łączenie się z systemami NFZ takimi jak eWUŚ oraz P1 za pośrednictwem API.

Na cyberbezpieczeństwo danych lekarzy i pacjentów oraz cyberodporność całego sektora wpływa kilka czynników wymagających zróżnicowanego podejścia. **Najpilniejsze działania objąć powinny jednak zmiany legislacyjne i niezwłoczne określenie minimalnych wymagań dla komercyjnych aplikacji gabinetowych.** Art. 8b ustawy o systemie informacji

w ochronie zdrowia[1] nakłada na usługodawców i podmioty prowadzące rejestry medyczne obowiązek zapewnienia zgodności swoich systemów teleinformatycznych z minimalnymi wymaganiami technicznymi i funkcjonalnymi zamieszczanymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia. W systemach usługodawców nacisk położony był dotychczas tylko na aspekty funkcjonalne. **Rada ds. Cyfryzacji rekomenduje nałożenie prawnego obowiązku zapewnienia również określonych minimalnych wymagań cyberbezpieczeństwa systemów usługodawców i podmiotów prowadzących rejestry medyczne.** Do tego czasu, minimalne wymagania techniczne podnoszące bezpieczeństwo danych powinny zostać określone w minimalnych wymaganiach technicznych i funkcjonalnych zamieszczanych w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

Do niewątpliwych **minimalnych wymagań cyberbezpieczeństwa zaliczone powinny być**: obligatoryjne dwuskładnikowe uwierzytelnienie (2FA), wymuszone używanie silnych haseł, blokowanie kont po kilku nieudanych próbach logowania, automatyczne wylogowanie po okresie bezczynności, przydzielanie uprawnień na podstawie ról przypisanych użytkownikom, polityka zakładania kont oparta o konta indywidulane, szyfrowanie ruchu sieciowego, szyfrowanie danych w spoczynku i w ruchu, mechanizmy kontroli dostępu, gromadzenie i monitorowanie śladu audytowego, zaimplementowane automatyczne alerty w przypadku wykrycia podejrzanej aktywności. **Systemy usługodawców i podmiotów prowadzących rejestry medyczne powinny również mieć zaimplementowane podstawowe mechanizmy ochrony przed atakami**, mechanizmy wykrywania i zapobiegania włamaniom, jak również monitorowania ruchu sieciowego. Systemy i aplikacje powinny podlegać regularnym testom bezpieczeństwa w celu identyfikacji i eliminacji podatności. Dodatkowo w placówkach medycznych powinny być realizowane podstawowe zasady bezpieczeństwa odnoszące się do użytkowych urządzeń i systemów informacyjnych, takie jak m.in. bieżąca aktualizacja systemów operacyjnych i użytkowych wykorzystywanych w pracy. Ponieważ zapewnienie ciągłości działania jest kluczowym elementem cyberbezpieczeństwa w sektorze medycznym, placówki medyczne powinny mieć również wdrożone procedury odnoszące się do planowania ciągłości działania oraz powinny regularnie testować plany awaryjne.

Rekomendowane jest również wprowadzenie określonych ograniczeń przy udzielaniu dostępu do API dla podmiotów medycznych korzystających z komercyjnego oprogramowania gabinetowego niespełniającego minimalnych wymagań, z zapewnieniem określonego okresu przejściowego gwarantującego ciągłość realizacji zadań przez te podmioty w okresie przejściowym. Usługi API oferowane przez NFZ również powinny spełniać minimalne wymagania bezpieczeństwa, w tym zapewniać autoryzację, ochronę przed nieautoryzowanymi zapytaniami z różnych źródeł, gromadzenie informacji audytowej czy wykrywanie anomalii na podstawie historycznej aktywności i generowanie

[1] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2025 poz. 302)

powiadomień o podejrzanych działaniach, takich jak nagłe zwiększenie liczby zapytań lub prób nieautoryzowanego dostępu.

Rada rekomenduje nałożenie wymagań na usługodawców i podmioty prowadzące rejestry medyczne w zakresie korzystania jedynie z systemów zapewniających minimalne wymagania cyberbezpieczeństwa oraz wprowadzenie obowiązków dotyczących cyklicznego prowadzenia audytów bezpieczeństwa tych systemów. Docelowo Rada zaleca objęcie tych systemów procesem certyfikacji cyberbezpieczeństwa.

Ponadto Rada pragnie podkreślić i zwrócić uwagę na fakt, iż certyfikat ZUS, który w swoich pierwotnych założeniach funkcjonalnych oraz technicznych **miał być rozwiązaniem przejściowym**, umożliwiającym wyłącznie lekarzom wystawianie elektronicznych zaświadczeń lekarskich o niezdolności do pracy, stał się rozwiązaniem powszechnie wykorzystywanym do potwierdzania transakcji w zakresie usług medycznych. Zdecydowana większość dokumentacji medycznej podpisywana jest z wykorzystaniem certyfikatu ZUS. Od strony technologicznej, bezpieczeństwa oraz ryzyk wynikających z użycia niezgodnego z przeznaczeniem, wdrożone przez ZUS rozwiązanie odpowiadało wyłącznie wyzwaniom dotyczącym procesu wystawiania e-ZLA, nad którym ZUS miał pełną kontrolę. Sytuacja, w której certyfikat ten zaczął być wykorzystywany do innych celów niż statutowe zadania ZUS oraz poza kontrolą systemów informatycznych Zakładu powoduje brak możliwości realnego i bieżącego reagowania na incydenty związane z wyłudzeniem certyfikatu i wykorzystaniem go np. do wystawiania e-recept na lekarstwa i pobierania danych osobowych pacjentów. **Nadużycia w tym obszarze występują coraz częściej, co potwierdzają liczne prowadzone postępowania karne.**

Z uwagi na coraz większą liczbę nadużyć związanych z wykorzystaniem certyfikatu ZUS w procesie potwierdzania transakcji usług medycznych (e-recepty, e-skierowania, e-ZLA itp.) Rada rekomenduje podjęcie prac legislacyjnych mających na celu zastąpienie certyfikatu ZUS innymi dostępnymi rozwiązaniami autoryzacyjnych (kwalifikowany certyfikat, Profil Zaufany, e-dowód) lub wypracowanie nowego rozwiązania, które będzie gwarantowało odpowiedni poziom bezpieczeństwa i jednocześnie będzie przyjazne w użytkowaniu dla pracowników poszczególnych grup medycznych.

Ponieważ zdecydowana większość naruszeń poufności, dostępności, integralności i autentyczności danych związanych jest z naruszeniem poufności danych uwierzytelniających lekarzy, personelu medycznego lub personelu administracyjnego, Rada rekomenduje **wprowadzenie dwuskładnikowego uwierzytelnienia (2FA) do systemów i aplikacji usługodawców i podmiotów prowadzących rejestry medyczne.** Dwuskładnikowe uwierzytelnienie powinno być również wprowadzone na kontach poczty elektronicznej personelu medycznego, wykorzystywanych do celów służbowych, w tym powiązanych z certyfikatami ZUS. Dane umożliwiające logowania do kont poczty elektronicznej lekarzy i personelu medycznego są przedmiotem obrotu zarówno w DarkWeb, jak również na kanałach wyspecjalizowanych w sprzedaży danych wyciekowych

założonych w komunikatorach internetowych (np. Telegram), a znając schemat kodu świadczeniodawcy, można je łatwo zidentyfikować w danych, które są publicznie dostępne. Zaimplementowanie dwuskładnikowego uwierzytelnienia (2FA) znacznie utrudni wykorzystanie danych z wycieku przez adwersarzy.

Ponadto, Rada rekomenduje prowadzenie regularnych szkoleń personelu medycznego i administracyjnego świadczeniodawców pod kątem zasad cyberbezpieczeństwa i cyberhigieny.

Rada rekomenduje również powołanie grupy roboczej mającej za zadanie identyfikację luk bezpieczeństwa i podatności podmiotów systemu opieki medycznej oraz przygotowanie rozwiązań prawnych, organizacyjnych i technicznych dla podniesienia poziomu bezpieczeństwa danych pacjentów.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/