Cyberatak to nie jest wirtualny problem

Do ataków hakerskich na szpitale i placówki zdrowia dochodzi na całym świecie. Część z nich wiąże się z wyciekiem danych wrażliwych, inne – z żądaniem okupu. Wszystkie zagrażają bezpieczeństwu pacjentów.

Justyna Kowalewska

Jak pisze „Polityka Zdrowotna”: „Z raportu Data Protection Trends Report 2022 wynika, że na skutek ataków *ransomware*, w uproszczeniu polegających na zablokowaniu komputerów i żądaniu okupu za ich odblokowanie, placówki medyczne na całym świecie w 2021 r. bezpowrotnie straciły prawie 40 proc. danych. Autorzy raportu wskazują również, że najwięcej przerw w działalności szpitali oraz podobnych ośrodków spowodowanych jest właśnie cyberatakami”.

Mający miejsce w grudniu cyberatak na szpital we francuskim Wersalu zmusił placówkę do odwołania operacji oraz ewakuacji kilkunastu pacjentów. Hakerzy, m.in. udostępniający dane pacjentów w sieci, zażądali okupu.

Pod koniec października ofiarą cyberataku padł Instytut Centrum Zdrowia Matki Polki w Łodzi. Atak hakerów stwarzał duże zagrożenie dla infrastruktury szpitalnej. Istniało niebezpieczeństwo wycieku danych pacjentów oraz pracowników. Wyłączono sieć. Dopiero w połowie listopada placówka poinformowała, że powoli wraca do swojej pełnej działalności.

– Instytut Centrum Zdrowia Matki Polki padł ofiarą cyberataku. Aby zminimalizować jego skutki, zdecydowaliśmy się na czasowe wyłączenie systemów informatycznych. Prowadzimy intensywne działania, które mają doprowadzić do jak najszybszego, pełnego ich uruchomienia – mówił rzecznik ICZMP Adam Czerwiński w materiale Wirtualnej Polski z 3 listopada 2022 r. Dalej w tym tekście czytamy: „Wszystkie formalności, które do tej pory wykonywano zdalnie – od przyjęcia do szpitala, poprzez wystawianie skierowań na badania – muszą od kilku dni odbywać się w sposób tradycyjny, na papierze. Utrudnione są także czynności diagnostyczne – co prawda badania obrazowe są wykonywane, jednak lekarz na oddziale nie może już zapoznać się z nimi w swoim komputerze. Badanie trzeba zapisać na nośniku i dostarczyć do kliniki”.

ICZMP to nie jedyny cel hackerów w Łodzi. W lutym do ataku doszło w Centralnym

Szpitalu Klinicznym. CyberDefence24.pl pisze: mgr Agnieszka Wielgus, asystentka zastępcy dyrektora ds. medyczno-organizacyjnych CKD Centralnego Szpitala Klinicznego Uniwersytetu Medycznego w Łodzi przesłała nam oficjalne pismo, podpisane przez dyrekcję szpitala. Jak czytamy, 6 lutego br. około godziny 5.00 rano rzeczywiście doszło do cyberataku na system informatyczny Centralnego Szpitala Klinicznego w Łodzi. Dyrekcja zapewnia, że „natychmiast udało się zlokalizować problem i profilaktycznie wyłączono systemy informatyczne szpitala". Dalej czytamy, że „nie doszło do wycieku danych pacjentów ani innych informacji wrażliwych". „Dzięki tworzonej codziennie kopii danych, wszystkie dane szpitala są bezpieczne. Aktualnie w CSK trwa przywracanie wszystkich funkcjonalności systemowych. Rozpoczęto przyjmowanie chorych planowych oraz wykonywanie zabiegów. Cały proces był monitorowany przez Ministerstwo Zdrowia i Centrum e-Zdrowia w celu najszybszego przywrócenia pracy i wdrożenia zabezpieczeń oraz procedur na przyszłość" – dodano.

W 2020 r. hakerzy włamali się do systemu finansowego szpitala im. Pirogowa i zrabowali blisko pół miliona złotych. A to tylko przykłady z łódzkiego podwórka. Do podobnych ataków dochodzi na całym świecie. W trakcie pisania tego tekstu, szpital Clinic w Barcelonie jest pozbawiony planowych operacji i wizyt ambulatoryjnych w związku z atakiem, do którego doszło 6 marca.

Panaceum 4/2023

Cyber(nie)bezpieczeństwo

Dominik Wcibisz, ekspert firmy Iron Mountain zajmującej się bezpieczeństwem danych

Tylko 16 proc. szpitali w Polsce deklaruje, że w ubiegłym roku przeprowadziło szkolenia dla pracowników w zakresie cyberbezpieczeństwa. Tymczasem w sektorze prywatnym duże firmy i korporacje szkolą pracowników nawet kilka razy w roku. W ostatnim kwartale 2022 r. ochrona zdrowia była atakowana najczęściej poprzez ransomware. Ataki na służbę zdrowia stanowiły 16 proc. ogółu ataków, co było najwyższym wskaźnikiem spośród wszystkich sektorów.

Ataki hakerskie to nie tylko problem naszego kraju, dochodzi do nich na całym świecie. Co więcej, ataki będą się powtarzać i będą dotyczyły szczególnie sektora średnich przedsiębiorstw, które łatwiej zaatakować niż duże korporacje, a jednocześnie można uzyskać od nich więcej niż od pojedynczych konsumentów. Nie jest także zaskoczeniem,

że ataki dotyczą i będą dotyczyć sektora publicznego, który jest znacznie gorzej dofinansowany, a co za tym idzie często gorzej zabezpieczony niż sektor prywatny.

Większość ataków (ok. 40%) to ataki ransomware, czyli takie, podczas których szyfrowane są dane, a przestępcy domagają się okupu. Tutaj jedynym sensownym zabezpieczeniem jest backup danych. W dużych instytucjach kopie zapasowe są zapisywane co kilka minut, więc w razie ataku, straty są minimalne. Z tego, co wiemy, listopadowy atak na szpital w Łodzi miał właśnie taki charakter. Szpital zareagował prawidłowo, natychmiast odcinając komputery od sieci. Niestety, co dla nas jest trudne do zrozumienia, backup danych szpitala był online i również został zniszczony podczas ataku.

Nie ma wątpliwości co do tego, że ataki będą się powtarzać i jest to sprawa bezpieczeństwa publicznego. Wskazane byłoby stworzenie rządowych programów wsparcia dla sektora publicznego w zakresie cyberbezpieczeństwa, chociażby przez organizowanie obowiązkowych audytów.