Cyberbezpieczeństwo w ochronie zdrowia coraz częściej poddawane próbie

Kategoria: Polityka Zdrowotna
Opublikowano: wtorek, 28, czerwiec 2022 16:53
Katarzyna Sekuła

Hakerstwo dla dużego grona osób brzmi nieco zagadkowo, a znaczenie tego słowa jest mniejsze wśród osób starszych, dla których cyfryzacja nie jest łatwą sprawą. Słowo to budzi filmowe skojarzenia, w których to antybohater nocami włamuje się do serwerów rządowych. W rzeczywistości jednak atak hakerski może spotkać każdego – nie trzeba być liderem politycznym, ani inną osobistością, by paść ofiarą cyberataku.

Cyberprzestępcy coraz częściej atakują sektor ochrony zdrowia – szpitale, przychodnie, laboratoria medyczne, gdyż wiedzą, że w placówkach medycznych poziom ochrony danych jest z reguły niższy niż w innych branżach. Na początku roku zaatakowane zostało także Lotnicze Pogotowie Ratunkowe. W 2021 roku na całym świecie odnotowano łącznie o 71% incydentów więcej niż w 2020 – czytamy w 2022 Cyber Security Report. W efekcie, było to średnio 830 incydentów tygodniowo. Z kolei według ekspertów z Checkpoint Research, w ubiegłym roku hakerzy atakowali przede wszystkim szpitale w Europie Środkowej – liczba przypadków wzrosła o 45% rok do roku.

Przykłady z życia wzięte

Skala działań hakerów nie zna granic, a w skrajnym przypadku cyberprzestępcy doprowadzili do najgorszego.

- Atak na Lotnicze Pogotowie Ratunkowe z żądaniem okupu
  W nocy z 13 na 14 lutego bieżącego roku, w Lotniczym Pogotowiu Ratunkowym przestały działać kluczowe dla ratowników systemy – w tym narzędzie do przesyłania informacji dotyczących interwencji medycznych. Ratownicy awaryjnie korzystali z połączeń telefonicznych i prywatnych e-maili, więc na szczęście atak nie wpłynął znacząco na realizację misji ratunkowych i transportów między szpitalami. Specjaliści walczyli przez tydzień ze skutkami ransomware – hakerzy zaszyfrowali dostęp do danych i zażądali 390 tys. dolarów okupu za ich odblokowanie.
- Cyberatak na Universal Health Services (USA i Wielka Brytania)
  Innym przykładem jest szeroko zakrojony cyberatak ransomware przeprowadzony we wrześniu 2020 roku w USA. Celem była sieć placówek Universal Health Services, rozsiana po niemal całym terytorium Stanów Zjednoczonych oraz w Wielkiej Brytanii. Z ograniczonym dostępem do infrastruktury IT mierzyło się 400 szpitali i przychodni. Szczęśliwie atak udało się zneutralizować, ale działania cyberprzestępców sparaliżowały system informatyczny UHS na cały weekend (do ataku doszło w piątek). Przez ten czas personel musiał korzystać wyłącznie z papierowego obiegu informacji, a szpitale musiały relokować pacjentów oczekujących na pilne zabiegi. W efekcie UHS odnotowało straty finansowe na poziomie 67 mln dolarów.
- Atak na szpital w Düsseldorfie i śmierć pacjentki
  Również we wrześniu 2020 roku cyberprzestępcy zaatakowali Uniwersytet Heinricha Heinego. Hakerzy zaszyfrowali 30 serwerów, a na jednym z nich zostawili plik zawierający informację z żądaniem okupu za odblokowanie systemu. Klasyczny atak ransomware okazał się tragiczny w skutkach – doprowadził do śmierci pacjentki Szpitala Uniwersyteckiego w Düsseldorfie. Na skutek awarii systemu spowodowanej cyberatakiem, lekarze nie mogli przyjąć kobiety i byli zmuszeni odesłać karetkę do innej placówki, w oddalonym o 32 km Wuppertalu. Pacjentka zmarła w drodze.

Jak zadbać o cyberbezpieczeństwo szpitali?

Do najczęściej wymienianych problemów cyberbezpieczeństwa, należą m.in. luki w aplikacjach i

architekturze sieci. Kolejną kwestią jest kładzenie nacisku wyłącznie na monitorowanie sieci bez odpowiedniej dbałości o bezpieczeństwo dostępu do danych. Sposobem na szybkie usunięcie błędów, są regularne audyty i testy bezpieczeństwa. Pozwalają one wykryć nieprawidłowości i znaleźć sposób na ich skorygowanie. Równie ważne są także cykliczne szkolenia personelu w zakresie bezpieczeństwa IT – bardzo często hakerzy wykorzystują niską czujność pracowników i stosują różne techniki manipulacyjne, rozsyłając np. fałszywe maile czy wiadomości SMS. Często wykorzystują też nasze naturalne obawy i konteksty sytuacyjne, np. w 2020 r. bardzo często atakowali „na COVID".

– *Wzrost liczby cyberataków na ochronę zdrowia pokazuje, że zabezpieczenie infrastruktury IT szpitali i innych instytucji ochrony zdrowia to kluczowa kwestia. Zdarza się, że rozwiązania IT w szpitalach nie nadążają za tempem zmian narzuconym przez pomysłowość hakerów* – mówi Patrycja Tatara, ekspert ds. cyberbezpieczeństwa w Sprint S.A.

Jak dodaje ekspertka - dobrze przeprowadzony audyt daje nieocenioną wiedzę, umożliwiającą skuteczne podniesienie poziomu cyberbezpieczeństwa placówki. Jest to jednak spory wydatek dla szpitali, dlatego Ministerstwo Zdrowia uruchomiło program dofinansowania, pozwalający placówkom medycznym zainwestować w swoje cyberbezpieczeństwo. W zależności od wysokości kontraktu NFZ, może to być nawet od 240 do 900 tysięcy złotych.

Aby skorzystać z pieniędzy szpitale do 30 listopada 2022 roku powinny złożyć u dyrektora właściwego oddziału wojewódzkiego NFZ wniosek o zawarcie umowy. Szczegółowe informacje, co należy zrobić i jakie warunki spełnić zawiera zarządzenie prezesa NFZ.

Źródło: ip - Sprint S.A.