CYBERBEZPIECZEŃSTWO W OCHRONIE ZDROWIA – KLUCZOWE DLA ZDROWIA I ŻYCIA PACJENTÓW

Data publikacji 27.11.2020

W trudnym okresie, jakim jest dla systemu ochrony zdrowia pandemia COVID-19, dodatkowym obciążeniem mogą być ataki cyberprzestępców. Incydenty cyberbezpieczeństwa mogą skutecznie uniemożliwić przeprowadzanie planowanych operacji czy zagrozić prywatności danych pacjentów. Jak nie dopuścić do ataków i co robić w momencie ich wystąpienia - zaleca Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ENISA.

Trwające na całym świecie zmagania z pandemią stawiają przed służbą zdrowia dodatkowe wyzwania związane z cyberbezpieczeństwem. Z okazji starają się bowiem skorzystać internetowi przestępcy, którzy błyskawicznie potrafią dostosować metody działania do panujących wokół warunków. Aktualna sytuacja w Unii Europejskiej i na świecie stanowi dla przestępców podatny grunt do prowadzenia kampanii phishingowych czy ataków ransomware.

System ochrony zdrowia wrażliwy na ataki

Jak wynika z danych CERT Polska – zespołu, który zajmuje się w Państwowym Instytucie Badawczym NASK analizowaniem incydentów bezpieczeństwa – już w minionym roku odnotowano wzrost liczby ataków złośliwego oprogramowania typu ransomware w wielu sektorach gospodarki, w tym w służbie zdrowia. Ten trend się utrzymuje - w całym 2019 roku w Polsce zarejestrowano 53 incydenty cyberbezpieczeństwa dotyczące sektora ochrony zdrowia, tymczasem tylko do końca września 2020 roku odnotowano ich już ponad 90.

„Z infekcjami ransomware zmagał się też sektor medyczny w USA i Australii. Na celowniku przestępców znalazły się m.in. systemy wspomagające ochronę zdrowia. Działanie cyberprzestępców sparaliżowało prawidłowy przebieg hospitalizacji pacjentów i uniemożliwiało przeprowadzanie planowych operacji. Ataki spowodowały też problemy z rozliczaniem wydatków w ramach systemów powszechnej opieki zdrowotnej” – mówi Przemysław Jaroszewski Kierownik Działu CERT Polska.

Urządzenia medyczne też nie zawsze bezpieczne

Ubiegły rok przyniósł też doniesienia o odkryciu kilku groźnych podatności w urządzeniach medycznych różnych producentów. Dotyczyło to m.in. urządzeń regulujących pracę serca jednej z amerykańskich firm, które miały luki w protokołach służących do radiowej transmisji danych. Dane można było „podsłuchać” z niewielkiej odległości. Podatności wykryto również w urządzeniach przeznaczonych do zabiegów elektrochirurgicznych tej samej firmy oraz aparaturze anestezjologicznej innego producenta.

Jak przypomina CERT Polska, gwałtowny rozwój technologii w zakresie medycyny nie zawsze idzie w parze z zapewnieniem odpowiedniego poziomu bezpieczeństwa teleinformatycznego przez producentów. O ile kradzież środków

z konta czy zaszyfrowanie istotnych danych może być problematyczne, o tyle niekontrolowana zmiana parametrów pracy urządzenia medycznego może doprowadzić do utraty zdrowia lub życia pacjentów, którzy obok personelu medycznego stanowią istotną grupę użytkowników tych urządzeń. Dlatego producenci sprzętu i oprogramowania medycznego powinni kłaść szczególny nacisk na bezpieczeństwo swoich produktów.

Ochrona zdrowia a cyberbezpieczeństwo – zalecenia ENISA

Agencja ENISA, w oparciu o rozwój sytuacji i najpowszechniejsze incydenty, jakie obserwowano od początku pandemii, rekomenduje sektorowi medycznemu:

1. Dzielenie się informacjami z personelem medycznym w organizacji, budowanie świadomości na temat cyberzagrożeń, a w przypadku ataku poproszenie personelu o odłączenie się od sieci, aby powstrzymać rozprzestrzenianie się złośliwego oprogramowania.
2. W przypadku naruszenia bezpieczeństwa systemu wstrzymanie wszelkich prowadzonych w nim działań odłączenie zainfekowanych maszyn od innych oraz od zewnętrznych dysków lub urządzeń medycznych. Przejście do trybu offline z sieci. Niezwłoczne skontaktowanie się z krajowym zespołem CSIRT.
3. Zapewnienie skutecznych procedur tworzenia kopii zapasowych i przywracania systemu. Plany ciągłości działania powinny istnieć zawsze, gdy awaria systemu może zakłócić podstawowe usługi zapewniane przez szpital.
4. W przypadku ataku na urządzenia medyczne reagowanie na incydent w porozumieniu z producentem urządzenia. Współpraca z dostawcami w celu reagowania na incydenty w przypadku urządzeń medycznych lub szpitalnych systemów informacyjnych.
5. Wprowadzenie segmentacji sieci, dzięki której ruch sieciowy może być izolowany i/lub filtrowany w celu ograniczenia lub uniemożliwienia dostępu do poszczególnych stref sieci.

Partnerami akcji są Ministerstwo Zdrowia, Narodowy Fundusz Zdrowia, Polska Policja i Nowy Szpital Wojewódzki Sp. z o.o.

Cyberataki i wszelkie naruszenia w sieci należy zgłaszać do CERT Polska w Państwowym Instytucie Badawczym NASK pod adresem: **https://incydent.cert.pl**

(Źródło: NASK)