

Cyberatak na szpital na Florydzie

09.02.2023

Niedawny cyberatak ransomware, mający miejsce 2 lutego 2023 r., zmusił amerykański szpital Tallahassee Memorial HealthCare do chwilowego porzucenia cyfrowego systemu rejestru służącego do opieki nad pacjentami i zastąpienia go w pełni analogowym, czyli zapisami na kartkach papieru.

„Dobrą wiadomością jest to, że nasz dział IT szybko wykrył problem i aktywnie pracuje nad jego rozwiązaniem” – powiedział przedstawiciel TMH.

TMH to prywatny, społeczny system opieki zdrowotnej typu non-profit obsługujący dwadzieścia jeden hrabstw obejmujących północną Florydę, południową Georgię i południową Alabamę. Ta instytucja medyczna składa się oddziału doraźnego, oddziału chirurgicznego, oddziału intensywnej terapii dla dorosłych, szpitala psychiatrycznego i wielu innych specjalistycznych ośrodków opieki, a także z trzech programów rezydencyjnych oraz trzydziestu ośmiu stowarzyszonych praktyk lekarskich i partnerstw.

Powrót do pióra i papieru

Firma TMH na bieżąco informuje opinię publiczną o postępach w przywracaniu systemu po cyberataku na szpital. Niestety lekarze zostali zmuszeni do przekierowywania pacjentów w stanie krytycznym do innych

ośrodków oraz przesuwania terminów niektórych operacji. Część placówek musiała całkowicie zrezygnować z systemów cyfrowego magazynowania danych i powrócić do korzystania z papierowych formularzy.

„Pacjenci i rodziny mogą zauważyć przejście na dokumentację papierową podczas rejestracji, przyjęcia lub opieki nad chorymi, ponieważ nasi usługodawcy będą używać papierowych formularzy, bloków recept, odręcznych notatek zamiast ich elektronicznych odpowiedników” – czytamy w najnowszej aktualizacji. – „Przepraszamy za wszelkie opóźnienia, które może to spowodować. Jesteśmy przygotowani do zapewnienia naszym pacjentom bezpiecznej opieki podczas przestoju systemu komputerowego”.

Coraz częstsze cyberataki na szpitale

Ataki na placówki medyczne są wyjątkowo bestialskimi incydentami i do tej pory wydają się tematem tabu w grupach cyberprzestępczych. Część hakerów, którzy korzystają z oprogramowania ransomware, tacy jak członkowie niesławnego gangu LockBit, często próbują się wybielić, mówiąc, że zdecydowali się nie hakować sektora opieki zdrowotnej (co zakrawa na śmieszność, jeśli wziąć pod uwagę ich kryminalną działalność). Jednak najnowsze raporty firmy Bitdefender ukazują, że prawda jest zgoła inna.

„W ostatnich latach oprogramowanie ransomware było wykorzystywane podczas ataków na szpitale i placówki medyczne wyjątkowo często. Większość hakerów nie ma żadnych oporów przed niszczeniem infrastruktury sieciowej instytucji zdrowotnych, nawet jeśli może to zagrozić życiu i zdrowiu wielu pacjentów. Dlatego apelujemy do zespołów dbających o bezpieczeństwo sieci placówek medycznych, aby zachowali szczególną czujność i proponujemy oprogramowanie antywirusowe

zintegrowane z technologiami EDR i XDR” – skomentował Mariusz Politowicz z firmy Marken, dystrybutora rozwiązań Bitdefender.

Źródło:<https://www.bitdefender.com/blog/hotforsecurity/cyberattack-sends-florida-hospital-back-to-pen-and-paper-emergency-patients-diverted/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 09.02.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań cyberbezpieczeństwa oraz światowy lider, chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty, służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, wielkim korporacjom, jak i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz tego, że wyposażają swoje oprogramowanie w najnowsze technologie takie, jak uczenie maszynowe, heurystyka oraz EDR i XDR.