AMERYKAŃSKIE SZPITALE SPARALIŻOWANE PRZEZ HAKERÓW. PLACÓWKI ZAPŁACIŁY OKUP

Według doniesień medialnych trzy amerykańskie szpitale w stanie Alabama, które były celem cyberataku zdecydowały się na zapłatę haraczu żądanego przez hakerów. W skutek incydentu placówki musiały wstrzymać przyjmowanie pacjentów.

Jak podaje serwis Ars Technica powołując się na doniesienia lokalnej gazety "Tuscaloosa News", przedstawiciele administracji dotkniętych atakiem placówek w końcu ubiegłego tygodnia otrzymali klucz deszyfrujący do zablokowanych przez hakerów systemów i rozpoczęli przywracanie funkcjonalności infrastruktury. W sobotę szpitale informowały o wciąż obowiązującej procedurze przekierowywania pacjentów do innych placówek.

"Tuscaloosa News" nie podaje, ile wynosił okup, jaki administracja szpitali zapłaciła hakerom, ani kim są cyberprzestępcy, którzy zaatakowali szpitale należące do operatora Druid City Hospital (DCH).

W oświadczeniu DCH czytamy, że z sukcesem ukończono testy deszyfrujące na wielu serwerach wchodzących w skład infrastruktury teleinformatycznej dotkniętych atakiem szpitali, a obecnie trwa procedura przywracania sprawności wszystkich systemów. Administracja placówek zapowiedziała jednak, że proces ten "potrwa" oraz wskazała, że nie może podać bardziej szczegółowych informacji na temat planowanego terminu zakończenia prac naprawczych.

Pierwsze informacje o ataku ransomware na systemy komputerowe trzech szpitali pojawiły się w ubiegły wtorek. Dzień później DCH informował, że działalność cyberprzestępców znacząco ograniczyła możliwość korzystania z systemów teleinformatycznych, a wysokość okupu żądanego za odszyfrowanie komputerów nie jest jeszcze znana.

Wszyscy nowi pacjenci zgłaszający się do dotkniętych incydentem placówek byli odsyłani do innych szpitali, a przyjmowano jedynie osoby w stanie krytycznym. Przełożono również zaplanowane zabiegi medyczne.

Według serwisu Ars Technica szpitale zostały zaatakowane z użyciem ransomware znanego jako Ryuk, używanego jest przez hakerów chcących głęboko penetrować atakowane sieci i pozyskiwać duże sumy w ramach żądanego okupu. Związany z firmą Emsisoft Brett Callow ocenił w rozmowie z AT, że "Ryuk to szczególnie złośliwe ransomware, które zawiera kod niszczący każdy jeden spośród ośmiu znajdujących się w atakowanym systemie plików". Jego zdaniem w przypadku ataku z użyciem tego oprogramowania szyfrującego "niemal zawsze występują straty, nawet w przypadku uregulowania okupu".

Ars Technica podkreśla, że wzrost popularności ransomware jako narzędzia do ataków hakerskich w ostatnich latach wskazuje, jak ważne jest utrzymanie sprawnego systemu tworzenia kopii zapasowych w sieciach firmowych, które personel mógłby wykorzystać w razie tego rodzaju ataku lub innego zdarzenia, uniemożliwiającego dostęp do danych.