Cyberdefence 24

aut. Sylwia Gliwa 29.10.2020

CISA: ALERT DLA SŁUŻBY ZDROWIA. CYBERPRZESTĘPCY NIE ODPUSZCZAJĄ SZPITALOM

Posiadamy wiarygodne informacje o zwiększonym i nieuchronnym zagrożeniu cyberprzestępczością dla amerykańskich szpitali i ich dostawców – informują amerykańskie instytucje. Działalność hakerów może być szczególnie szkodliwa z uwagi na zwiększoną pracę placówek medycznych w związku z pandemią koronawirusa.

Agencja ds. Cyberbezpieczeństwa i Infrastruktury (CISA), Federalne Biuro Śledcze (FBI) oraz U.S. Cyber Command Cyber National Mission Force wydały komunikat ostrzegający sektor medyczny przed działaniami mającymi na celu infekowanie systemów oprogramowaniem ransomware Ryuk w celu uzyskania korzyści finansowych. Jest to już kolejny wykryty przejaw działań cyberprzestępców przeciwko służbie zdrowia, który pojawia się w ostatnich miesiącach.

Jak czytamy w komunikacie, cyberataki mogą być szczególnie szkodliwe z uwagi na pandemię koronawirusa. Zalecane jest, aby w związku z wykrytym zagrożeniem administratorzy systemów zrównoważyli to ryzyko poprzez większe inwestycje w bezpieczeństwo. Działania cyberprzestępców prawdopodobnie ukierunkowane są na wykorzystanie ransomware mającym na celu zaszyfrowanie danych zaatakowanych podmiotów w celu wyłudzenia środków finansowanych w zmian za przekazanie klucza deszyfrującego.

Jest to już kolejny raz, kiedy cyberprzestępcy biorą na cel amerykańską służbę zdrowia. Pod koniec września informowaliśmy o komercyjnej sieci szpitali w Stanach Zjednoczonych Universal Health Services, który prawdopodobnie padł ofiarą ataku ransomware. W wyniku „problemu z bezpieczeństwem IT” jego sieć została wyłączona a personel zmuszony do przejścia w tryb pracy offline.

Czytaj też: Atak ransomware w USA. 400 placówek medycznych pod ostrzałem cyberprzestepców

Na początku października z kolei, poinformowano, że szpital uniwersytecki w New Jersey zdecydował się zapłacić hakerom okup w wysokości 670 000 dolarów w zamian za niepublikowanie 240GB skradzionych danych na temat pacjentów placówki. Do tak znacznego incydentu bezpieczeństwa doszło poprzez zainfekowane urządzenie jednego z pracowników, co umożliwiło hakerom na zablokowanie systemów szpitala.

Czytaj też: Zapłacili, by uniknąć katastrofy. Szpital w New Jersey uległ hakerom