SZPITALE BEZ DOSTĘPU DO SIECI. CYBERATAK PARALIŻUJE KOLEJNE PLACÓWKI MEDYCZNE

Cyberatak na szpitale spowodował, że w środę i czwartek niektóre szpitale w prowincji Quebec musiały odłączyć się od Internetu. Kanadyjskie media podały, że przestępcy zaatakowali także placówki w USA.

Publiczny nadawca francuskojęzyczny Radio-Canada cytował w czwartek rządowe maile, w których napisano, że „obecnie trwa na całym świecie kampania ransomware (ang. – oprogramowanie służące do wymuszania okupu - PAP), której celem są głównie szpitale amerykańskie i kanadyjskie(...) ataki są bardzo dobrze zorganizowane i w ciągu minionych 24 godzin dotyczyły kilku szpitali".

Ataki, których celem jest uzyskanie okupu w zamian za odblokowanie zaszyfrowanych danych na serwerach, spowodowały, że w Montrealu kilka szpitali odłączono profilaktycznie od internetu, wyłączono też zdalny dostęp do sieci. Choć – jak podawały media – systemy informatyczne funkcjonują sprawnie, szpitale dysponują też kopiami baz danych, to utrudnione jest np. automatyczne przekazywanie danych o wynikach testów na COVID-19.

Minister zdrowia prowincji Quebec Christian Dubé potwierdził w czwartek po południu, że systemy informatyczne jednego z centrów opieki szpitalnej w Montrealu zostały „szybko wyłączone" po wykryciu ataku jeszcze w środę, „by chronić dane pacjentów".

Nie wiadomo ile dokładnie szpitali w rejonie Montrealu było celem ataku, trwa dochodzenie przedstawicieli rządu Quebec, policji federalnej i Microsoftu.

Kanadyjskie media podały, że w minioną środę amerykańskie służby ostrzegły, iż tego typu ataki są „rosnącym i bliskim zagrożeniem". Według cytowanych opinii ekspertów, obecne ataki mogą być dokonywane z wykorzystaniem ransomware, do którego uruchomienia dochodzi poprzez kliknięcie załącznika w niegroźnie wyglądającym mailu.

Czytaj też: CISA: Alert dla służby zdrowia. Cyberprzestępcy nie odpuszczają szpitalom

Kanadyjskie rządowe Centrum Cyberbezpieczeństwa od 4 października ostrzegało przed ryzykiem „ataku o zakresie światowym prowadzonym z wykorzystaniem ransomware Ryuk". Media przypomniały, że ten typ przestępczego oprogramowania wykorzystuje inne programy, takie jak Emotet i Trickbot, które początkowo były napisane do kradzieży danych finansowych i haseł.

W czerwcu br. publiczny angielskojęzyczny nadawca CBC informował o dużej skali ataków właśnie na kanadyjską służbę zdrowia.

W maju br. kanadyjskie agencje wywiadu ostrzegły przed finansowanymi przez obce rządy próbami

kradzieży wyników badań naukowych, prowadzonych podczas pandemii w Kanadzie i przed zagrożeniami dla instytucji medycznych.

Wcześniej, pod koniec marca br. kanadyjski wywiad elektroniczny ostrzegał, że pandemia COVID-19 zwiększa zagrożenie systemów IT instytucji służby zdrowia i zalecało instalowanie aktualizacji. Wówczas w komunikacie podkreślono, że pandemia COVID-19 oznacza „podwyższony poziom ryzyka".

Zwrócono uwagę, że cyberprzestępcy mogą wykorzystać pandemię, aby wyłudzić np. okup, w związku z istniejącą presją na instytucje służby zdrowia. Wywiad wymieniał działania phishingowe, wykorzystywanie krytycznych słabości systemów czy słabości certyfikatów, a także działania „inżynierii społecznej".

Jak informowaliśmy we wrześniu w wyniku cyberataku na Szpital Uniwersytecki w Duesseldorfie (Niemcy) zablokowano możliwość przyjmowania pacjentów z nagłych wypadków. Kobieta, która potrzebowała natychmiastowej pomocy medycznej zmarła po tym jak została przewieziona do szpitala w innym mieście. W wyniku działań hakerów kobieta nie mogła być leczona przez około godzinę. Niemiecka prokuratura wszczęła śledztwo przeciwko nieznanym sprawcom w związku z podejrzeniem o nieumyślne spowodowania śmierci. Pacjentka jest prawdopodobnie pierwszą ofiarą śmiertelną ataku ransomware.

PAP / SG