

ATAK RANSOMWARE W USA. 400 PLACÓWEK MEDYCZNYCH POD OSTRZAŁEM CYBERPRZESTĘPCÓW

Jeden z największych komercyjnych operatorów szpitali w Stanach Zjednoczonych Universal Health Services Inc potwierdził, w wyniku nieokreślonego „problemu z bezpieczeństwem IT” jego sieć została wyłączona. Sieć prowadzi około 400 szpitali i ośrodków opiekuńczych na terenie Stanów Zjednoczonych i Wielkiej Brytanii.

UHS nie poinformował opinii publicznej o charakterze zdarzenia, jednak z informacji do których dotarł Reuters wynika, że do pracowników sieci rozsyłane są wiadomości instruujące, aby unikali podłączania swoich urządzeń do firmowej sieci, co jak stwierdzają eksperci wskazuje na atak ransomware. „NIE próbuj łączyć się z pocztą e-mail UHS lub innymi aplikacjami sieciowymi UHS” - brzmiał jeden z komunikatów cytowany przez Agencję Reutera. W wewnętrznej komunikacji operator miał wskazywać również, że zakłócenia mogą trwać 24 godziny lub dłużej.

Jak wskazuje NBC news powołując się na anonimowe pielęgniarki systemy zaczęły zawodzić w weekend a niektóre z jednostek musiały uciekać się do wypełniania informacji o pacjentach za pomocą pióra i papieru.

Operator podkreślił również, że z godnie zasadami korporacyjnymi placówki tworzą kopie zapasowe w tym również prowadzenie dokumentacji offline. UHS zapewnił, że opieka nad pacjentem „nadal jest zapewniana bezpiecznie i skutecznie” a także, że żadne dane pacjentów ani pracowników nie zostały naruszone.

Ataki ransomware coraz częściej stają się zmorą placówek medycznych a także jednostek zajmujących się prowadzeniem badań nad szczepionką na koronawirusa.

Jak informowaliśmy wcześniej w wyniku ataku ransomware na szpital w niemieckim w Duesseldorfie, jednostka nie mogła przyjmować pacjentów z nagłych wypadków. W trakcie awarii sieci do szpitala nie mogła zostać przyjęta pacjentka, która zmarła z uwagi na brak natychmiastowej pomocy medycznej i konieczności do placówki medycznej oddalonej o około 30 kilometrów. Kobieta ta jest prawdopodobnie pierwszą ofiarą śmiertelną ataku ransomware. W przypadku tego ataku, systemy szpitala były zakłócone przez tydzień. W konsekwencji ataku hakerów systemy ulegały stopniowej awarii, a personel szpitala nie był w stanie uzyskać dostępu do danych pacjentów. Operacje odroczone, a pacjentów z nagłymi przypadkami przenoszono do innych szpitali.

We wrześniu zaatakowany został także system informatyczny hiszpańskiej służby zdrowia, który od marca, zgodnie z informacjami przekazanymi przez hiszpańską policję miała być atakowana trzykrotnie. Wszystkie trzy akcje cyberprzestępców nastąpiły w okresie ogłoszonego stanu zagrożenia epidemicznego.

Również na początku września podano do publicznej wiadomości, że incydent w rosyjskim Regionalnym Centrum Klinicznym w obwodzie swierdłowskim uniemożliwił lekarzom pracę. Hakerzy użyli oprogramowania ransomware, atakując bazy danych placówki. W wyniku działań cyberprzestępców dane na temat 400 pacjentów zostały skutecznie zaszyfrowane przez hakerów.