CYBERATAK NA SERWERY ADMINISTRACJI STANOWEJ W LUIZJANIE

Serwery administracji stanowej w Luizjanie zostały dotknięte cyberatakiem - poinformował jej szef John Bel Edwards za pomocą Twittera. Wiele urządzeń zainfekowano złośliwym oprogramowaniem ransomware. W odpowiedzi na incydent władze podjęły decyzję o wdrożeniu "protokołów bezpieczeństwa".

Według Edwardsa to właśnie wdrożenie procedur po wykryciu aktywności hakerów stało się przyczyną zakłóceń w prawidłowym funkcjonowaniu wielu aplikacji, stron internetowych i poczty elektronicznej w licznych placówkach administracji publicznej Luizjany. Gubernator stanu podkreślił, że atak hakerski nie powiódł się. Poinformował też, że choć sprawność niektórych elementów infrastruktury zaczęto przywracać już kilka godzin po zdarzeniu, to pełen powrót do prawidłowej funkcjonalności może potrwać nawet kilka dni.

Według agencji Bloomberga atak na infrastrukturę stanową Luizjany należy łączyć z niedawnymi wyborami gubernatora stanu, które wygrał Edwards niewielką różnicą 40 tys. głosów w stosunku do głównego kontrkandydata. Jak podkreśla Bloomberg, próba ataku na Luizjanę podkreśla wagę problemów, przed którymi ostrzega wielu ekspertów z branży cyberbezpieczeństwa w związku ze zbliżającymi się wyborami prezydenckimi w USA zaplanowanymi na rok 2020. Uważają oni, że oprócz maszynowego liczenia głosów powinny istnieć manualne systemy ich zliczania. Tymczasem Luizjana jest jednym z 11 stanów, w których istnieją jurysdykcje nieposiadające już takich systemów.

Władze Luizjany oceniają, że zakończony niepowodzeniem atak ransomware był zbliżony w swojej naturze do tych, które wcześniej w tym roku dotknęły instytucje lokalnej administracji m.in. na Florydzie. Eksperci związani z firmą FireEye z branży cyberbezpieczeństwa wskazują, że jednym z najpopularniejszych rodzajów złośliwego oprogramowania używanego w tego typu atakach jest ransomware Ryuk. Cyberprzestępcy, którzy z niego korzystali, żądali około 300 tys. dolarów okupu, a sam proces naprawiania strat po ataku z jego użyciem kosztował "dziesiątki milionów dolarów".

FireEye podkreśla również, że liczba ataków ransomware na instytucje administracji publicznej w 2019 roku niemalże podwoiła się.

Czytaj też: 5 mln USD za odblokowanie systemów przedsiębiorstwa naftowego. Haker stawia żądania