ROK 2019 ZDOMINOWANY PRZEZ CYBERATAKI NA WŁADZE SAMORZĄDOWE

2019 rok został zdominowany przez ataki hakerskie, których celem były władze samorządowe - wskazują specjaliści Kaspersky Lab. Odnotowano szczególnie dużą liczbę incydentów wykorzystujących oprogramowanie ransomware. Według prognoz ich popularność w środowisku cyberprzestępczym będzie rosła.

Celem ataków z użyciem ransomware było w 2019 roku 174 instytucji miejskich i ponad 3 tys. podległych im organizacji. Eksperci szacują, że to wzrost o 60 proc. w stosunku do liczby tego rodzaju ataków hakerskich w roku 2018.

Organizacje samorządowe mają mniejsze możliwości zapłaty wysokiego okupu żądanego przez hakerów za odszyfrowanie danych, jednakże są bardziej skłonne do ulegania szantażowi cyberprzestępców. Blokada usług komunalnych, do której prowadzą ataki ransowmare, wpływa bowiem bezpośrednio na życie mieszkańców i powoduje straty nie tylko finansowe - uważają specjaliści.

Kaspersky Lab dokonało również zestawienia kwot okupu najczęściej żądanych przez hakerów atakujących organizacje i instytucje związane z władzami samorządowymi. Z dostępnych publicznie światowych danych wynika, że cyberprzestępcy w 2019 roku domagali się nawet 5,3 mln USD. Średni okup żądany przez hakerów to 1,03 mln dolarów. Firma uważa jednak, że sam haracz, jakiego żądają dla siebie cyberprzestępcy, to nie koniec kosztów, jakie ponoszą ofiary ataków ransomware.

Według badacza bezpieczeństwa Fiedora Sinicyna "spełnianie żądań szantażystów działa na krótką metę (...) zachęcając ich i zapewniając im środki finansowe do prowadzenia dalszych ataków". Sinicyn podkreśla, że w przypadku ataków na miasto dodatkowe koszty wynikają z konieczności przeprowadzenia dochodzenia i audytu infrastruktury po ataku.

W 2019 roku w atakach na władze lokalne z wykorzystaniem ransomware wyróżniły się trzy rodziny złośliwego oprogramowania. To Ryuk, który pojawił się ponad rok temu i był aktywny na całym świecie zarówno w sektorze publicznym jak i prywatnym, Purga - szkodnik znany od 2016 roku, który wykorzystywany jest przede wszystkim do ataków na władze miast, a także Stop, który szczególną popularność zyskał w III kwartale mijającego roku.

Eksperci zalecają, aby chronić się przed atakami ransomware przede wszystkim poprzez regularne aktualizacje bezpieczeństwa używanego oprogramowania, obronę zdalnego dostępu do sieci korporacyjnych (np. przy użyciu VPN) i stosowanie bezpiecznych haseł do kont. Istotne są również

szkolenia personelu dotyczące higieny cyberbezpieczeństwa oraz regularne tworzenie kopii zapasowych danych.

Czytaj też: Hakerzy zmieniają taktykę cyberataków na przedsiębiorstwa