KANADYJSKI WYWIAD OSTRZEGA PRZED CYBERATAKAMI NA INFRASTRUKTURĘ ENERGETYCZNĄ

Kanadyjski wywiad ostrzegł w opublikowanym w środę raporcie przed „bardzo prawdopodobnymi" cyberatakami na infrastrukturę krytyczną w Kanadzie, w tym na sieci energetyczne.

Raport Communications Security Establishment (CSE), agencji kanadyjskiego wywiadu elektronicznego, wskazuje na pięć głównych przyczyn zagrożeń, na pierwszym miejscu stawiając zależność coraz większej liczby systemów od łączności internetowej i powiązanie działań komputerowych systemów operacyjnych z internetem. Dotyczy to również sieci elektrycznych i wodociągowych.

„Oceniamy, z prawie całkowitą pewnością, że największe zagrożenia fizycznego bezpieczeństwa Kanadyjczyków wiążą się z systemami operacyjnymi i krytyczną infrastrukturą (...) Oceniamy, że podmioty sponsorowane przez rządy prawdopodobnie będą pracować nad metodami umożliwiającymi przerwanie dostaw prądu w Kanadzie" - napisano w raporcie.

Raport wymienia cztery kraje jako główne źródło cyberzagrożeń wywoływanych przez przestępców sponsorowanych przez rządy: Chiny, Rosję, Iran i Koreę Północną.

CSE przypomniało, że przemysłowe systemy kontroli (Industrial Control Systems – ICS) były już obiektem ataków, szczególnie w sektorze energetycznym, zaś ataki były przeprowadzane przez podmioty działające na zlecenie rządów.

„W 2019 r. podmioty związane z Rosją testowały odporność systemów przesyłowych elektryczności w USA i Kanadzie. Irańskie grupy hakerskie brały na cel infrastrukturę ICS w państwach takich jak USA, Izrael i Arabia Saudyjska. Złośliwe oprogramowanie z Korei Północnej zostało znalezione w sieciach IT elektrowni w Indiach, a pracownicy amerykańskich firm obsługujących dostawy energii, gazu i wody dla konsumentów byli celem chińskich podmiotów powiązanych z rządem" - napisano w raporcie.

Autorzy ocenili, że w ciągu najbliższych dwóch lata ataki na krytyczną infrastrukturę będą się nasilać i będą powiązane z żądaniami okupu. Przypomniano, że w czerwcu br. jeden z amerykańskich producentów samochodów, który ma zakłady także w Kanadzie, musiał wstrzymać działalność i było to spowodowane najprawodpodobniej właśnie próbą wymuszenia okupu.

Przy tym raport uważa za „bardzo nieprawdopodobne" próby zamierzonego uszkodzenia krytycznej infrastruktury, powodującego znaczne szkody czy nawet utratę życia, zastępującego tradycyjne konflikty zbrojne. Autorzy uważają natomiast, że prawdopodobne jest zaangażowanie w zbieranie informacji, którą w przyszłości można wykorzystać np. do zastraszania.

Autorzy przypomnieli o zagrożeniach dla własności intelektualnej, dużych przedsiębiorstw, a także sektora służby zdrowia. Wskazali że już podczas pandemii „cyberprzestępcy współpracujący z rządami", w tym z rządem Rosji, próbowali ukraść wyniki badań naukowych nad COVID-19.

Zwrócono uwagę, że Kanadyjczycy coraz bardziej polegają na internecie, zarówno w życiu prywatnym, pracy, jak np. relacjach z bankami, zaś pandemia COVID-19 nasiliła tę zależność. „Wykorzystujący cyberzagrożenia – w tym przestępcy i podmioty działające na zlecenie rządów – przystosowują swoją działalność, by pozyskać informacje ważne dla Kanadyjczyków" – ostrzegli autorzy raportu, wskazując że „najnowocześniejszymi metodami dysponują przestępcy sponsorowani przez rządy".

Jednym z kluczowych punktów raportu jest ostrzeżenie przed próbami wpływania na opinię publiczną. „Zagraniczne próby wywierania wpływów online są nową normą i nie ograniczają się do kluczowych wydarzeń takich jak wybory (…) Oceniamy jednak, że Kanada jest na dole listy priorytetów (…) Niemniej kanadyjskie media są blisko powiązane z mediami amerykańskimi i w innych krajach sojuszniczych, co oznacza, że mieszkańcy tych krajów również mogą być celem".

Raport jest aktualizacją poprzedniego z 2018 r., zawiera też prognozy sięgające do 2022 r. Autorzy powołują się zarówno na niecytowane tajne źródła informacji, jak i na oficjalne jawne opracowania