aut. Szymon Palczewski 11.09.2019

KONTROLA CYBERZABEZPIECZEŃ W KANADYJSKIEJ ARMII

Dowodzone przez Stany Zjednoczone Północnoamerykańskie Aerospace Defence Command (Norad) poprosiło kanadyjskie wojsko o przeprowadzenie inwentaryzacji w strukturach armii oraz kompleksowe sprawdzenie infrastruktury cywilnej w celu znalezienia systemów podatnych na cyberataki – informuje CBC News.

List do szefa kanadyjskiego wojska, napisany przez dowódcę Norad adm. Williama Gourtneya, trafił do mediów na podstawie przepisów dotyczącego dostępu do informacji. Korespondencja powstała ponad trzy lata temu i wyrażała obawy amerykańskich wojskowych na temat kondycji cyberbezpieczeństwa sojusznika. Według Waszyngtonu, Kanada miała być najbardziej podatna na zagrożenia.

Jak podaje CBC, w liście dowódca Norad poprosił generała Jonathana Vance'a o „zidentyfikowanie i likwidację" luk w zabezpieczeniach systemów kontroli infrastruktury (ICS) w kanadyjskich bazach wojskowych, szczególnie w „instalacjach o kluczowym znaczeniu dla realizacji misji Norad". W treści wiadomości wezwano również dowódcę wojskowego Kanady do „popierania rozwoju zdolności reagowania na cyberincydenty wymierzone w CAF (przyp. red. systemy kontroli infrastruktury) i obronę CAF w razie potrzeby".

Jednak obawy Williama Gourtneya nie ograniczały się do instalacji obronnych. Amerykański dowódca zwrócił się do Jonathana Vance'a z prośbą o „współpracę z Public Safety Canada w celu zidentyfikowania infrastruktury cywilnej, która ma kluczowe znaczenie dla CAF i misji Norad". Mowa tu m.in. o opracowaniu procesów zgłaszania incydentów na zidentyfikowanej infrastrukturze cywilnej.

Strona kanadyjska pozytywnie odpowiedziała na list od przedstawicieli amerykańskiego wojska. Trzy miesiące po otrzymaniu korespondencji Jonathan Vance zlecił swoim specjalistom realizację zadań z zakresu poszukiwania i neutralizacji luk.

Równocześnie udzielił pisemnej odpowiedzi, w której stwierdził – „Podzielam obawy Norad dotyczące cyberbezpieczeństwa". W treści przedstawiciel wojska podkreślił, że rząd zidentyfikował „przeciwników", którzy stanowią „poważne zagrożenie, i podjęto wysiłki w celu zidentyfikowania i opracowania strategii ochronnych dla kanadyjskiej infrastruktury krytycznej".

Jak informuje CBC, dzięki sugestiom ze strony Stanów Zjednoczonych nadano kanadyjskim wojskowym nowe uprawnienia do prowadzenia ofensywnych operacji w cyberprzestrzeni. Utworzono również Canadian Centre for Cyber Security, które koncentruje się na ochronie infrastruktury cywilnej. Jego celem jest „stworzenie sytuacji, gdzie sektor prywatny i publiczny współpracują, aby rozwiązać najbardziej złożone problemy w kanadyjskiej cyberprzestrzeni".

Eksperci badający przypadek Kanady wskazują, że główną luką są tzw. systemy technologii operacyjnej. Służą one do wykonywania zadań sterowanych komputerowo w zakładach użyteczności

publicznej lub innych przedsiębiorstwach o kluczowym znaczeniu. Specjaliści podkreślają, że ich zabezpieczenie jest wyjątkowo trudne ze względu na różnorodność dostępnych systemów operacyjnych.

„Sprzęt oraz inne urządzenia, które odpowiadają za transport na przykład gazu lub wody pitnej mają kluczowe znaczenie dla Kanadyjczyków i naszych sił zbrojnych" – zaznaczył cytowany przez CBC kanadyjski dowódca gen. ppłk. Christopher Coates. Jak dodaje, Norad koncentruje się na zdolnościach niezbędnych do wykonywania swojej pracy w zakresie obrony Ameryki Północnej przed zagrożeniami, i starają się „zminimalizować te podatności tam, gdzie to możliwe".