Petycja do Ministra Cyfryzacji

w sprawie wstrzymania instalacji urządzeń sieciowych H3C w polskich szkołach do czasu pełnej, niezależnej weryfikacji bezpieczeństwa

Adresat	Pan Krzysztof Gawkowski Wiceprezes Rady Ministrów Minister Cyfryzacji
Podstawa	Ustawa z dnia 11 lipca 2014 r. o petycjach
Przedmiot	Wniosek o pilne podjęcie działań nadzorczych i ochronnych wobec planowanego wdrożenia urządzeń H3C w szkołach.
Wnoszący	

Szanowny Panie Ministrze,

działając w interesie publicznym, wnoszę o pilne wstrzymanie wdrażania urządzeń sieciowych H3C w szkołach w ramach programu „Laboratoria AI" do czasu przeprowadzenia pełnej, niezależnej i udokumentowanej oceny ryzyka dla cyberbezpieczeństwa państwa, bezpieczeństwa danych oraz bezpieczeństwa infrastruktury publicznej.

Z załączonych dokumentów wynika, że w postępowaniu dotyczącym dostawy zestawów „Laboratoriów Sztucznej Inteligencji (Laboratoria AI)" wybrano czterech wykonawców. Jednocześnie w debacie wokół tego postępowania wskazywane jest, że elementem wdrożenia mają być access pointy / routery Wi-Fi producenta H3C, w bardzo dużej skali obejmującej szkoły w całej Polsce. Ponieważ skala ta sięga 16 tysięcy urządzeń, to mamy do czynienia z wdrożeniem o znaczeniu systemowym.

Szkoły nie są już wyłącznie miejscem prowadzenia zajęć dydaktycznych. Są częścią państwowej infrastruktury cyfrowej: przetwarzają dane uczniów, nauczycieli, rodziców i pracowników, korzystają z dzienników elektronicznych, usług chmurowych, systemów egzaminacyjnych oraz sieci jednostek samorządu i administracji. W tych warunkach masowe wdrożenie urządzeń sieciowych wysokiego ryzyka tworzy rozproszoną powierzchnię ataku o potencjalnie ogólnokrajowych skutkach.

1. Uzasadnienie petycji

- Centralny Ośrodek Informatyki odrzucił ofertę Data Experts opartą o serwery H3C. Z uzasadnienia wynika, że po przeprowadzonych czynnościach analitycznych uznano wprowadzenie serwerów H3C do infrastruktury zamawiającego za nieakceptowalne ryzyko, którego nie można

wyeliminować, zagrażające cyberbezpieczeństwu, bezpieczeństwu publicznemu oraz istotnemu interesowi bezpieczeństwa państwa.

- COI wskazał również, że w związku z wątpliwościami zwrócił się do Agencji Bezpieczeństwa Wewnętrznego o opinię. Otrzymana opinia ABW została opatrzona klauzulą „ZASTRZEŻONE", a po zapoznaniu się z jej treścią zamawiający uznał, że oferta powinna zostać odrzucona także na podstawie art. 226 ust. 1 pkt 16 ustawy Pzp.
- Ekspertyza sporządzona dla ZUS wskazuje na poważne kontrowersje dotyczące bezpieczeństwa sprzętu H3C w infrastrukturze publicznej, w szczególności tam, gdzie przetwarzane są dane osobowe. W raporcie wymieniono m.in. brak pełnej transparentności, niedostatek niezależnych audytów bezpieczeństwa, ograniczoną obecność w środowiskach o wysokich wymaganiach bezpieczeństwa oraz ryzyka związane z łańcuchem dostaw.
- Autorzy ekspertyzy dla ZUS wprost stwierdzili, że nie rekomendują wyboru urządzeń H3C do nowych wdrożeń ani do rozbudowy środowisk produkcyjnych bez pełnego, niezależnego audytu bezpieczeństwa oraz bez uzyskania pozytywnej opinii ABW.
- Załączony materiał FCC pokazuje, że amerykański regulator objął zakazem uzyskiwania nowych autoryzacji określone kategorie foreign-made consumer-grade routers, wskazując na „unacceptable risks" dla bezpieczeństwa narodowego i bezpieczeństwa osób w USA. Niezależnie od różnic między systemami prawnymi, kierunek oceny ryzyka dla urządzeń sieciowych pochodzących z jurysdykcji wysokiego ryzyka jest jednoznaczny.

2. Zakres żądania

1. niezwłoczne wstrzymanie wdrożenia urządzeń H3C w szkołach do czasu zakończenia pełnej oceny bezpieczeństwa;
2. przeprowadzenie niezależnego audytu bezpieczeństwa obejmującego hardware, firmware, mechanizmy zarządzania, aktualizacji i komunikacji zdalnej;
3. zasięgnięcie formalnych stanowisk ABW, NASK, CSIRT GOV oraz właściwych komórek odpowiedzialnych za Krajowy System Cyberbezpieczeństwa;
4. przegląd warunków postępowania i sposobu oceny ofert pod kątem ryzyka dla bezpieczeństwa państwa, bezpieczeństwa danych i ciągłości działania usług publicznych;
5. ujawnienie - w zakresie dopuszczalnym prawem - przesłanek, analiz i opinii stanowiących podstawę dopuszczenia takich urządzeń do szkół;
6. wprowadzenie do przyszłych postępowań wymagań bezpieczeństwa łańcucha dostaw, w tym oceny jurysdykcji producenta, transparentności firmware oraz dostępności niezależnych certyfikacji i audytów;
7. rozważenie zastąpienia urządzeń H3C rozwiązaniami pochodzącymi od dostawców o niższym profilu ryzyka.

Wniosek szczegółowy

Wnoszę również o udzielenie publicznej odpowiedzi, czy Ministerstwo Cyfryzacji uznaje za dopuszczalne instalowanie w polskich szkołach infrastruktury sieciowej producenta, wobec

którego w innych postępowaniach publicznych w Polsce formułowano zastrzeżenia związane z bezpieczeństwem państwa, a eksperci opiniujący potrzeby instytucji publicznych rekomendowali powstrzymanie nowych wdrożeń do czasu pełnego audytu bezpieczeństwa.

3. Interes publiczny

Państwo nie powinno reagować dopiero po incydencie. W obszarze cyberbezpieczeństwa właściwym standardem jest działanie wyprzedzające, oparte na zasadzie ostrożności, zwłaszcza gdy chodzi o urządzenia pracujące na styku sieci, danych i administracji publicznej.

Masowa instalacja urządzeń sieciowych w szkołach - szczególnie jeżeli dotyczy dziesiątek lub setek tysięcy punktów dostępowych - nie jest zwykłym zakupem sprzętu IT. Jest to decyzja infrastrukturalna, która może wpływać na bezpieczeństwo cyfrowe państwa przez wiele lat.

Z tego względu sprawa wymaga osobistego nadzoru Ministra Cyfryzacji i jednoznacznego rozstrzygnięcia, czy przy takiej skali wdrożenia zostały zastosowane standardy należytej staranności odpowiadające randze ryzyka.