aut. Szymon Palczewski 07.08.2019

CHIŃSKIE PRODUKTY W U.S. ARMY. KOLEJNE ZAKUPY POMIMO ZAGROŻENIA

Według najnowszego raportu wydanego przez U.S. Military's Inspector General poważnym zagrożeniem dla amerykańskiego wojska mogą być małe urządzenia, które zostały zakupione przez Departament Obrony. Dokument koncentruje się przede wszystkim na produktach posiadających znane luki w zabezpieczeniach, głównie z Chin.

Treść raportu wskazuje, że pomimo rosnących obaw Departamentu Obrony USA (DoD) dotyczących cyberbezpieczeństwa państwa, dokonano znacznych zakupów technologii informacyjnej COTS (commercial off-the-shelf), która może być uznana za zagrożenie. Według danych zaprezentowanych w dokumencie od 70 do 80 procent elementów składających się na systemy DoD to COTS.

Specjaliści wskazują, że co najmniej 33 miliony dolarów przeznaczono na zakup sprzętu od takich marek jak Lenovo, Lexmark czy GoPro. Przeciwnicy mogą wykorzystać znane luki w zabezpieczeniach tych produktów, a w rezultacie prowadzone misje wojskowe mogą być zagrożone – ostrzegają eksperci.

Raport mówi o ryzyku odnoszącym się do urządzeń, których wartość nie przekracza 10 tysięcy dolarów za sztukę. Zdecydowanie bardziej niepokojące niż wadliwe drukarki jest fakt zakupu w zeszłym roku przez DoD chińskiego sprzętu przeznaczonego do nadzoru. „Mimo, że Departament Stanu wydał w maju 2017 roku ostrzeżenie przed użyciem kamer wideo firm Hikvision i Dahua, powołując się na obawy cyberszpiegowskie ze strony Chin, DoD kontynuował zakup i używanie tych przedmiotów do monitorowania bezpieczeństwa instalacji, dopóki Kongres nie wprowadził zakazu". Chińskie kamery monitorujące były używane w amerykańskich bazach wojskowych na tydzień przed wejściem w życie federalnego zakazu. Mowa tutaj o kamerach firmy Hikvision, której właścicielem połowy akcji jest chiński rząd.

W raporcie przywołano również przykład drukarek Lexmark. Według przedstawionych statystyk, zakupiono ich co najmniej 8 000 dla armii i sił powietrznych, pomimo ostrzeżeń wydanych przez Kongres. „Lexmark jest firmą powiązaną z chińskimi programami wojskowymi, nuklearnymi i cyberszpiegowskimi" – tłumaczą specjaliści. Obawa wynika z faktu, że urządzenia koncernu służą jako narzędzia do cyberszpiegostwa lub przeprowadzania ataków hakerskich.

W tym miejscu pojawia się pytanie, dlaczego Departament Obrony nie zakazał kupna, a następnie używania produktów Lenovo, pomimo znanego zagrożenia? Według raportu Inspector General, firma jest „mistrzem w swojej dziedzinie", podobnie jak Huawei w branży smartfonów czy 5G. Departament Bezpieczeństwa Wewnętrznego, Kongres oraz inne agencje rządowe już znacznie wcześniej wydały specjalne ostrzeżenie w tej sprawie, jednak DoD dopiero w ubiegłym roku zdecydował się na przeprowadzenie badań ryzyka produktów Lenovo. Zanim analiza miała miejsce, armia zakupiła kolejne produkty firmy o łącznej wartości 268 tysięcy dolarów. Podobna sytuacja ma miejsce w przypadku pozostałych produktów innych marek – wskazano w raporcie.

Istniejące luki mogą zostać wykorzystane do złośliwych celów. Słabość zabezpieczeń wykorzystywana jest m.in. przez Chiny. Cyberataki ze strony Pekinu wymierzone w DoD zostały zauważone w 2005 roku, czyli w momencie wykrycia operacji hakerskiej „Titan Rain". Był to incydent trwający od 2003 do 2007 roku, którego celem były amerykańskie i brytyjskie sieci. Ten cyberatak zmienił strategię USA wobec Chin oraz podejście do kwestii cyberbezpieczeństwa.