aut. Szymon Palczewski 16.12.2019

F-15 PODATNE NA CYBERATAKI? ARCHAICZNE ZABEZPIECZENIA AMERYKAŃSKIEGO MYŚLIWCA

Myśliwce F-15 podatne na cyberataki? Sprzęt U.S. Air Force został poddany testom bezpieczeństwa przez hakerów, którym udało się bez problemu przełamać zabezpieczenia kluczowych systemów. Prezentują one poziom z lat 90. - alarmują przedstawiciele amerykańskich sił zbrojnych.

Podczas konferencji DEFCON 2019, która miała miejsce w Las Vegas, sprzęt U.S. Air Force został przetestowany przez hakerów. Głównym celem eksperymentu był system transferu danych dla myśliwca F-15. Specjaliści bez trudu poradzili sobie z jego zabezpieczeniami, co zszokowało dowództwo amerykańskich sił powietrznych – informuje serwis The Fifth Domain.

„To, co powiedzieli mi, w jaki sposób złamali zabezpieczenia, to rzeczy, o których przemysł nie wie lub nie jest tego świadomy. A przecież jest to element naszego łańcucha dostaw" – powiedział przedstawiciel U.S. Air Force Will Roper, cytowany przez The Fifth Domain. Dodał, że Pentagon musi zacząć wywierać większą presję na dostawcach, aby realnie podnosić cyberbezpieczeństwo armii. „Obecnie wygląda to tak, że otrzymujemy od kontrahentów jedynie minimum tego, o co ich prosimy" – zaznaczył przedstawiciel amerykańskiego wojska.

W tym celu konieczne jest bardziej szczegółowe zdefiniowanie wymagań w zawieranych umowach i kontraktach. Konieczne jest również opracowanie zasad i reguł, które muszą być weryfikowalne. Przykładowo, rząd powinien wymagać od podmiotów sektora przemysłowego dostarczenia wszystkich elementów, w tym między innymi kodów do systemów oraz sieci – wskazuje The Fifth Domain.

Waszyngton musi podjąć zdecydowane kroki, aby siły zbrojne USA były w pełni bezpieczne. Will Roper podkreśla, że obecne mechanizmy cyberbezpieczeństwa, jakie realnie działają w U.S. Army odpowiadają ostatniej dekadzie XX wieku. „Nie przeszły one do kolejnej dekady" – alarmuje przedstawiciel U.S. Air Force.

W wywiadzie udzielonym C4ISRNET, wojskowy zaznaczył także, że bardzo dobrym rozwiązaniem jest również poddawanie systemów i urządzeń testom prowadzonym w „kontrolowanym środowisku". Specjaliści w ten sposób mogli by sprawdzać podatność sprzętu w rzeczywistych warunkach. Jeśli eksperci potrafiliby podczas eksperymentów znaleźć luki w zabezpieczeniach, to również hakerzy, w tym grupy zarządzane przez rządy narodowe, z pewnością by to zrobili. W tym kontekście kluczową rolę odgrywa eliminacja podatności oraz zapobieganie cyberatakom.

Czytaj też: Amerykańskie testy wojskowego wykorzystania 5G