aut. Szymon Palczewski 18.09.2019

LUKI W SYSTEMACH F-15. WYMOWNY SYMBOL STANU CYBERBEZPIECZEŃSTWA U.S. AIR FORCE

Luki umożliwiające cyberatak w systemach danych myśliwca F-15? Will Roper, asystent sekretarza U.S. Air Force, twierdzi, że małe urządzenie odpowiedzialne za gromadzenie danych na pokładzie maszyny jest podatane na działania hakerów. Według specjalisty stanowi ono symbol stanu cyberbezpieczeństwa amerykańskich sił powietrznych. W odpowiedzi na rosnące zagrożenia dowództwo planuje pozyskać zewnętrznych specjalistów, aby podnieść jakość zabezpieczeń. Pomóc ma w tym innowacyjny konkurs zorganizowany przez U.S. Air Force – informuje serwis Wired.

Will Roper jest silnie zaangażowany w zmianę sposobu , w jaki Air Force będzie realizowało politykę cyberbezpieczeństwa. „Musimy przezwyciężyć strach przed zatrudnieniem zewnętrznych ekspertów, którzy podniosą nasz poziom bezpieczeństwa. Nadal realizujemy procedury, które były właściwe w latach 90. XX wieku" – podkreślił Will Roper. „Mamy bardzo zamknięty model. Zakładamy, że jeśli budujemy rzeczy za zamkniętymi drzwiami w tajemnicy i nikt inny nie ma do nich dostępu, to finalnie będą bezpieczne. Tak może być w realnym świecie, ale w cyberprzestrzeni jest inaczej. W świecie cyfrowym wszystko ma w sobie jakieś oprogramowanie".

Każde oprogramowanie zawiera błędy, które można wykorzystać. Nie chodzi tu tylko o sprzęt wojskowy. Urządzenia codziennego użytku stają się „inteligentne", a przez to niebezpieczne. Dowództwo jest tego świadome, dlatego podejmuje liczne inicjatywy w celu poprawy cyberbezpieczeństwa. Przykładem może być inicjatywa Hack the Air Force, w której zewnętrzni hakerzy wykryli luki w systemach należących do amerykańskich sił powietrznych, a następnie je zlikwidowali. Nagrodą było 130 000 dolarów.

Oczywiście U.S. Air Force posiada swój wewnętrzny zespół ds. cyberbezpieczeństwa, ale jego zasoby są mocno ograniczone, przez co często nie jest w stanie samodzielnie rozwiązać kluczowych problemów. Według Will'iego Ropera dowództwo potrzebuje pomocy z zewnątrz.

„Można oczekiwać bardzo rygorystycznych procedur bezpieczeństwa dotyczących F-15, które sprzęt i piloci spełniają. Ale co z zrobić z takim małym nośnikiem danych posiadającym luki?" – zaznaczył przedstawiciel armii. – „Taki element można przeoczyć. Tego typu komponenty są zwykle budowane przez mniejsze firmy, które mogą nie być skupione na cyberbezpieczeństwie lub cyberodporności".

Dostrzegając problem podzespołów i ich producentów, dowództwo powinno zawierać konkretne i sprecyzowane umowy z kontrahentami, nakładając na nich obowiązek zapewnienia najwyższego poziomu cyberbezpieczeństwa. W ten sposób cały łańcuch dostaw będzie gwarantował jakość, a samoloty i inne maszyny staną się dużo bardziej odporne na działania zewnętrznych aktorów.

Jak wskazuje serwis Wired, nadal pozostaje wiele do zrobienia, aby podnieść bezpieczeństwo nie tylko U.S. Air Force, ale całego sektora lotniczego. Wiele maszyn jest niedostępnych do sprawdzenia przez zewnętrznych specjalistów, a duże koncerny odrzucają możliwość, że ich produkty są wadliwe lub

posiadają luki w zabezpieczeniach. Taki stan rzeczy w obecnych czasach jest bardzo poważnym problemem, ponieważ dotyczy wielu innych dziedzin życia – zaznaczył Pete Cooper, dyrektor Aviation Village. „Współpraca i dobre relacje między sektorami to podstawa. W odniesieniu do lotnictwa takowej brak" – podkreślił specjalista.

Czas na satelity

Dowództwo sił powietrznych planuje konkurs, w którym wszyscy zainteresowani specjaliści będą mogli wziąć udział. Całe wydarzenie ma polegać na zhakowaniu satelity lub stacji naziemnej. Najlepsi eksperci zostaną zaproszeni do przetestowania swoich zdolności w fazie symulacji. Końcowym etapem konkursu będzie możliwość wystąpienia podczas konferencji Defcon i zaprezentowanie umiejętności przed wybitymi specjalistami z różnych dziedzin.

„Planujemy wysłać na orbitę satelitę z kamerą, skierować ją w stronę Ziemi, a następnie poprosić specjalistów biorących udział w konkursie, aby przejęły nad nim kontrolę i zwróciły obiektyw w stronę księżyca" – wyjaśnił Roper.

Jak informuje serwis Wired, wiele szczegółów dotyczących tego przedsięwzięcia nadal nie zostało ustalonych. Na przykład, który satelita zostanie zaangażowany, jak duże będą konkursowe zespoły specjalistów oraz ile wynosić będzie końcowa nagroda pieniężna.

„Jeśli chcesz dostać się do satelity, możesz albo przejść przez stację naziemną, albo spróbować znaleźć drogę do satelity bezpośrednio za pomocą własnych narzędzi. Zawodnicy będą mieli okazję zrobić jedno i drugie" – podkreślił Will Roper. „Ich celem będzie przejęcie satelity za pomocą wszelkich dostępnych środków".

Według Wired inicjatywa jest zabiegiem czysto PR-owiskim. Eksperci jednak dostrzegają w niej praktyczną wartość. „Dzięki konkursowi przynajmniej jeden satelita będzie bezpieczniejszy" – stwierdził z uśmiechem Pete Cooper. „Przestrzeń kosmiczna stała się tak istotną częścią cyberbezpieczeństwa sektora lotniczego, że następna edycja Defcon będzie poświęcona przestrzeni kosmicznej".