aut. Szymon Palczewski 08.11.2019

AMERYKAŃSKIE SATELITY BEZBRONNE? „ANI RZĄD, ANI PRODUCENCI NIE DBAJĄ O ICH OCHRONĘ”

„Ani rząd, ani sami producenci nie robią wystarczająco dużo, aby zapewnić pełną ochronę amerykańskim satelitom przed cyberatakami” – wynika z raportu opracowanego przez Aerospace Corporation. Specjaliści alarmują o wysokiej podatności urządzeń zaliczanych do infrastruktury kosmicznej USA – informuje serwis Breaking Defence.

W raporcie „Defending Spacecraft in the Cyber Domain” specjaliści wyraźnie podkreślili, że „ani polityka kosmiczna, ani polityka cyberbezpieczeństwa nie są przygotowane na wyzwania związane z przenikaniem się domeny kosmicznej z cyberprzestrzenią”. Sytuacja odnosi się nie tylko do wojskowych satelitów, ale wszystkich amerykańskich urządzeń znajdujących się w kosmosie. Wrogowie Stanów Zjednoczonych z pewnością są zainteresowani złośliwymi kampaniami wymierzonymi w komercyjne obiekty – wskazuje Breaking Defence.

„Wraz z rosnącą listą podmiotów stanowiących zagrożenie oraz świadomości na temat potencjalnych luk w zabezpieczeniach, wszystkie sektory przestrzeni kosmicznej muszą inwestować w poprawę cyberbezpieczeństwa, w szczególności systemów znajdujących się na pokładzie statku kosmicznego” – stwierdzili specjaliści Aerospace w raporcie.

Jak przypomina Breaking Defence, cyberbezpieczeństwo systemów pracujących w kosmosie stało się poważnym problemem nie tylko dla U.S. Air Force oraz Pentagonu, ale również innych podmiotów zaangażowanych w politykę kosmiczną USA, w tym National Security Council (NSC). Cybersecurity Directorate, funkcjonujące przy NSC, silniej postawiło na partnerstwo publiczno-prywatne, którego bezpośrednim celem jest cyberochrona satelitów. Inicjatywa została nazwana Space-ISAC (Space Information Analysis and Sharing Center).

Raport opracowany przez Aerospace zawiera również rekomendacje, których wdrożenie ma przyczynić się do poprawy bezpieczeństwa kluczowych elementów infrastruktury kosmicznej. Wśród nich należy wskazać na:

- wykrywanie oraz zapobieganie incydentom poprzez wykorzystanie sygnatur i uczenia maszynowego w celu identyfikacji, a następnie neutralizacji cyberataków na pokładzie statku kosmicznego,
- opracowanie programu zarządzania ryzykiem w łańcuchu dostaw w celu ochrony przed złośliwym oprogramowaniem umieszczanym w systemach oraz modułach,
- wdrożenie właściwego oprogramowania w łańcuchu dostaw w celu zmniejszenia podatności systemów lotniczych oraz kosmicznych,
- wprowadzenie zaawansowanego systemu logowania na pokładzie statku kosmicznego, aby zweryfikować legalność dokonywanych operacji,

- tak zwany „Root of Trust” (przyp. red. zestaw zaufanych funkcji) w celu ochrony integralności oprogramowania oraz systemów układowych,
- skuteczniejsze zabezpieczenie przed modyfikacją funkcji przeprowadzaną przez złośliwych aktorów w ramach danego urządzenia.

Według autorów raportu problemem jest również fakt, że w polityce rządowej „brakuje niezbędnej integracji między cyberbezpieczeństwem a domeną kosmiczną”.

Gdzie leży problem?

Tradycyjnie stacje naziemne komunikujące się z satelitami uważane były za najbardziej prawdopodobny cel cyberataku – wskazuje Breaking Defence. W przypadku incydentu mogłoby to doprowadzić do uszkodzenia zbioru danych lub bezpośrednio satelity. Jednak istnieje także wiele innych zagrożeń, których skutki mogą być równie dotkliwe.

Atrakcyjnym celem z punktu widzenia hakerów są podmioty zaangażowane w łańcuch dostaw. Autorzy raportu wspominają o „szeregu scenariuszy”, które mogą prowadzić do wielu złożonych problemów – od „nieodwracalnych szkód materialnych” po „przerwanie prowadzonej misji”. Każda z nich rodzi poważne konsekwencje, ponieważ „im bardziej przeciwnik może ingerować w nasze systemy kosmiczne, tym większy wpływ będzie posiadał na nasze systemy wojskowe”.

Według Breking Defence głównym celem Stanów Zjednoczonych powinno być dołożenie wszelkich starań, aby zidentyfikować, a następnie zlikwidować wszelkie podatności, aby zagwarantować niezawodność oraz jakość swoich urządzeń i systemów kosmicznych. „Trzeba wziąć odpowiedzialność za wszystkie słabości bezpieczeństwa” – stwierdzono w raporcie.

Specjaliści są zdania, że w przyszłości problem jeszcze się nasili. Wynika to z faktu szybszej produkcji przy minimalizacji kosztów budowy urządzeń kosmicznych. „Małe satelity będą bazować na większej ilości części komercyjnych niż te, które powstają dla wojska” – podkreślają eksperci. „Te małe urządzenia są budowane bardzo szybko, więc może zabraknąć cennego czasu, aby za każdym razem ściśle kontrolować danego dostawcę, bo to znacznie wydłuży cały proces i zwiększy koszty”.

Najlepszym sposobem na zbudowanie „statku kosmicznego odpornego na cyberataki” byłoby opracowanie systemu wykrywania włamań (IDS), który stale monitorowałby „dane telemetryczne, sekwencje poleceń, wspólny ruch magistrali oraz konfigurację oprogramowania lotu, a także stany operacyjne” – czytamy w raporcie.

Specjaliści Aerospace wskazują również, że wiele elementów wykorzystywanych do budowy satelitów bazuje na przestarzałych rozwiązaniach, które „zostały zaprojektowane jeszcze przed pojawieniem się terminu cyberbezpieczeństwo”. W związku z tym część kluczowych komponentów wykazuje wysoką podatność i w łatwy sposób mogą zostać uszkodzone lub zmodyfikowane.

Czytaj też: Amerykanie uziemili swoje drony. Obawiają się chińskiego szpiegostwa