Space 24

aut. Paweł Ziemnicki 02.11.2018

ROSNĄCE ZAGROŻENIE HAKERSKIE DLA SATELITÓW. BLISKOWSCHODNIE PODEJŚCIE [KOMENTARZ]

Podobnie jak wiele sektorów „naziemnej" gospodarki, również infrastruktura satelitarna jest coraz mocniej narażona na ataki w zakresie cyberbezpieczeństwa. Systemy tego rodzaju wymagają zatem należytej ochrony, co w istocie ma znaczenie dla całej gospodarki. Czynnikiem kluczowym są tutaj obsługujący i kontrolujący satelity ludzie.

Cyber-zagrożenia dla satelitów były jednym z tematów konferencji Next-Gen Space Tech Middle East, która odbyła się w dniach 22-23 października 2018 r. w Abu Dhabi, stolicy Zjednoczonych Emiratów Arabskich. O bezpieczeństwie informatycznym systemów satelitarnych mówił goszczący na tym wydarzeniu dr Ayad Aldaijy z Arabii Saudyjskiej. Jego prezentacja nosiła tytuł „The Usability of Space-based Systems: Addressing the Threats and Challenges".

Dr Aldaijy zwrócił uwagę na fundamentalną konieczność identyfikacji rosnącego zagrożenia atakami hakerskimi na satelity i zwiększania społecznej świadomości w tej materii. Dla zapobiegania tego typu zagrożeniom nie wystarczy instalacja optymalnego software'u na wysyłanych w przestrzeń kosmiczną urządzeniach. Konieczna jest również praca tutaj na Ziemi nad infrastrukturą, ale także nad przygotowaniem odpowiednich kadr. Niezbędny dla dobrego funkcjonowania systemu bezpieczeństwa dla satelitów jest właściwy przepływ informacji między wszystkimi zaangażowanymi w tej dziedzinie podmiotami.

Ekspert ds. cyberbezpieczeństwa z Bliskiego Wschodu podkreślał, jak mocno dzisiejsza globalna gospodarka opiera się na danych satelitarnych. Chodzi tu o wszelkie korzyści z satelitów obserwacji Ziemi, konstelacji GNSS i łączności za pośrednictwem sprzętu na różnych orbitach wokół naszej planety.

Przykładowe zagrożenia

Ataki na infrastrukturę satelitarna mogą polegać na tzw. jammingu (zakłócaniu) lub spoofingu (podszywaniu się) bądź komunikacji radiowej dla orbitalnych urządzeń telekomunikacyjnych bądź też satelitów GNSS. Celem nieprzyjacielskiej ingerencji może być przejęcie kontroli nad misją statku kosmicznego. Należy się wówczas liczyć z zakłóceniem przepływu informacji między stacją naziemną a satelitą, a nawet z niepożądaną przez jego prawowitego zarządcę zmianą pozycji satelity na orbicie.

Należy przy tym zdaniem arabskiego specjalisty rozróżnić ataki militarne o politycznym podłożu międzypaństwowym, od stricte terrorystycznych motywacji stojących za akcją hakerską. Aldaijy zwraca przy tym uwagę, że za cyberatakami na infrastrukturę satelitarną mogą stać najróżniejsze motywacje ich egzekutorów. Niekiedy może kryć się za tym przykładowo chora ambicja samych hakerów, którzy porywając się na ambitny, pozaziemski cel, chcą swoim skutecznym atakiem

udowodnić swoją wartość czy to samym sobie, czy innym zainteresowanym, którzy być może byliby skłonni w przyszłości za tego typu dywersję zapłacić.

Działania łatwo dostępne

Dr Aldaijy szczególnie podkreślił, że ataki cybernetyczne na infrastrukturę satelitarną są niestety, dla wykwalifikowanych przestępców, formą relatywnie łatwo dostępną. Jest to działanie niskokosztowe. Można je ponadto realizować praktycznie z dowolnego miejsca na kuli ziemskiej, dysponując jedynie komputerem z dostępem do sieci. Ofensywa tego typu nie stanowi wszak próby kradzieży konkretnych, ukrytych gdzieś towarów. Jest natomiast, w czystej postaci, atakiem na informacje.

Hakerzy, którzy decydują się na tego typu wywrotowe działania, chowają się za szeroką osłoną internetowej anonimowości. Drugim czynnikiem, który utrudnia ich ściganie, jest niespójność prawa w zakresie cyberbezpieczeństwa w różnych krajach, lub też niekiedy zupełny brak odpowiednich regulacji.

Wadliwy czynnik ludzki

Dr Ayad Aldaijy jest głęboko przekonany, że cyberataki bardzo często udają się wtedy, kiedy zawodzi czynnik ludzki, co związane jest z bardzo daleko dziś sięgającym uzależnieniem człowieka od technologii.

Związane z człowiekiem czynniki ryzyka w kwestii cyber-zagrożeń to m.in.:

- słabe hasła lub w ogóle ich brak;
- nieodpowiednie techniki identyfikacji;
- nadużywanie w systemie łączności bezprzewodowej;
- złe procedury zdalnego dostępu do baz danych lub dzielenia się informacjami;
- nieodpowiedzialne zachowania użytkowników;
- niekompetentna obsługa i ochrona systemu IT.

Niekiedy znacznie trudniejsze od wykrycia ataków podmiotów zewnętrznych może być wykrycie szkodliwych działań podmiotów znajdujących się wewnątrz systemu informatycznego. Ich działania mogą być przy tym celowo niszczycielskie lub stwarzać zagrożenie na skutek nieumyślnego zaniedbania czy zaniechania. Fundamentalne dla zapobiegania niebezpiecznym zdarzeniom jest właściwe dzielenie się informacjami przez wszystkie podmioty odpowiedzialne za bezpieczeństwo sieci informatycznej w danym przedsiębiorstwie czy sektorze gospodarki.

Podsumowania i rekomendacje

Ekspert z Arabii Saudyjskiej słusznie zauważył, że cyberataki będą stale podejmowane i nieuchronnie część z nich zakończy się sukcesem. Co zatem robić, żeby minimalizować prawdopodobieństwo owych niepożądanych sukcesów?

W duchu całej swojej wcześniejszej prezentacji dr Aldaijy podkreślił konieczność właściwego zadbania o kadry. Jego zdaniem niewykwalifikowany i niechętny personel to największe zagrożenie dla systemu IT organizacji, podczas gdy zmotywowany i kompetentny zespół może być jej największym atutem.

Wśród rekomendacji specjalista z Bliskiego Wschodu wymienił przykładowo stworzenie wizji, ustalenie priorytetów, budowę zespołu, kontrolę i monitorowanie sytuacji w zakresie IT, i wreszcie wdrożenie odpowiedniej kultury pracy w organizacji.

Doktor Ayad Aldaijy jest ekspertem w dziedzinie cyberbezpieczeństwa i prezesem firmy Strategic Consultancy Services Office z Rijadu. Doradza w tej kwestii Ministerstwu Środowiska, Zasobów Wodnych i Rolnictwa Arabii Saudyjskiej.