

Cyberzagrożenie w lotnictwie cywilnym

#Lotnictwo cywilne 19 stycznia 2016

Analicyści Thalesa przewidują, że lotnictwo komunikacyjne będzie coraz bardziej narażone na ataki hakerów.



Próby przejęcia kontroli nad układem sterowania lotem samolotu pasażerskiego mogą być podejmowane zarówno z jego pokładu, jak i z ziemi / Zdjęcie: Thales

Podczas ostatniego spotkania z francuskimi dziennikarzami, Bruno Nouzille, szef działu awioniki konsorcjum Thales, zwrócił uwagę na rosnące zagrożenie atakami hakerskimi na samoloty komunikacyjne. Problem dostrzegają także władze lotnicze i organizacje zrzeszające przewoźników i dostawców usług nawigacyjnych.

Wprawdzie nie ma dowodów na przejęcie przez Chrisa Roberta, eksperta ds. cyberbezpieczeństwa, kontroli nad układem sterowania silnika Boeinga 737-800 w ub.r., ale FBI prowadzi w tej sprawie dochodzenie. Zdaniem Nouzille'a nie można zlekceważyć tego zdarzenia.

W 2025 ponad 70% floty samolotów pasażerskich będzie umożliwiała pasażerom dostęp do Internetu. *Wprawdzie urządzenia awioniczne, stanowiące wyposażenie kabiny załogi i pokładowe systemy rozrywki nie zawierają zbyt wielu wspólnych informacji, nie można jednak wykluczyć, że haker będzie próbował przejąć sterowanie samolotem w ten właśnie sposób. Laptop można zaatakować nawet w trybie samolotowym, po wyłączeniu dostępu do Wi-Fi czy bluetootha - mówi Nouzille.*

W związku z tym przemysł i użytkownicy powinni podjąć środki zaradcze. Przede wszystkim inżynierowie powinni konstruować urządzenia w taki sposób, aby miały specjalny interfejs, służący do dostępu wyłącznie w celu przeprowadzenia obsługi technicznej lub podłączenia tzw. Electronic Flight Bag (EFB, elektronicznych pomocy nawigacyjnych i obsługowych, [FlySmart dla Peach Aviation](#), 2015-07-09, [Ryanair](#)

[wprowadza EFB, 2014-12-08](#)).

Oprócz tego należy wdrożyć programy wykrywające i przeciwdziałające próbom ataku hakerskiego. Niezależnie od nich powinien także działać specjalny zespół specjalistów, bezustannie monitorujący stan samolotu (awioniki, zespołu napędowego, itp.), odpowiedzialny także za terminową aktualizację oprogramowania. Obecnie 15 specjalistów Thalesa prowadzi takie prace w centrum w Tuluzie. Problem dostrzegła także Europejska Agencja Bezpieczeństwa Lotniczego (EASA), która zaproponowała utworzenie podobnego międzynarodowego zespołu.

W grudniu ub. r. Komisja Europejska opracowała plan działania w sprawie zachowania cyberbezpieczeństwa w transporcie lotniczym. Na starym Kontynencie ma odpowiadać za nie EASA. Natomiast obroną przed atakami hakerów w wymiarze globalnym zajęła się Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO), która opublikowała odpowiednie wytyczne. W przedsięwzięcie zaangażowały się też Międzynarodowe Zrzeszenie Przewoźników Lotniczych (IATA), Światowe Stowarzyszenie Agencji Kontroli Ruchu Lotniczego (CANSO) i Międzynarodowa Rada Portów Lotniczych (ACI).

Powiązane wiadomości

[Cyberzagrożenie w lotnictwie cywilnym \(2016-01-19\)](#)

[Ryanair wprowadza EFB \(2014-12-08\)](#)

[Tablety dla pilotów Delta Air Lines \(2013-10-04\)](#)

[Otwarcie bazy Ryanair w Gdańsku \(2014-10-29\)](#)

[Modlin czwartą bazą Ryanair \(2014-10-22\)](#)

[FlySmart dla Peach Aviation \(2015-07-09\)](#)

[Tablety dla pilotów Delta Air Lines \(2013-10-04\)](#)

[Ryanair wprowadza EFB \(2014-12-08\)](#)

[Tablety dla pilotów Delta Air Lines \(2013-10-04\)](#)

[Otwarcie bazy Ryanair w Gdańsku \(2014-10-29\)](#)