Zagrożenia cyberbezpieczeństwa dla infrastruktury lotniczej

Cybersecurity threats to aviation infrastructure

Hanna Dzido

Dr

Katedra Transporty i Logistyki
Wydział Nawigacyjny
Uniwersytet Morski w Gdyni

h.dzido@wn.umg.edu.pl

Streszczenie: Lotnictwo stanowi przykład sektora o rozległych wzajemnych połączeniach i złożoności, wysokim poziomie ekspozycji w mediach oraz kluczowej roli w rozwoju społeczno - gospodarczym państw. Infrastruktura lotnicza (liniowa i punktowa) stanowi elementy infrastruktury krytycznej, przez co podlega szczególnej ochronie. Wobec zachodzących zmian, cyfryzacji wielu procesów w funkcjonowaniu lotnisk, linii lotniczych, obsługi pasażerów, transferu danych bezpośrednio związanych z charakterem lotnictwa, za komponenty infrastruktury lotniczej należy uznać również systemy informatyczne wykorzystywane przez podmioty rynku lotniczego w tym m.in.: lotniska, linie lotnicze, organizacje obsługowe, służby lotniskowe. W artykule przedstawiono zagadnienia cyberbezpieczeństwa w lotnictwie cywilnym oraz główne kierunki działań organów nadzoru nad lotnictwem cywilnym światowego ICAO oraz europejskiego EASA. Autorka przedstawia wiodące dokumenty oraz dotychczasowe działania podjęte w kwestiach zapewnienia cyberbezpieczeństwa w zakresie ochrony danych wszystkich uczestników runku lotniczego opracowane na szczeblu międzynarodowym. Autorka wskazuje inicjatywy ICAO i EASA odnoszące się do cyberprzestrzeni, potrzebę skoordynowania krajowych regulacji z odpowiednimi przepisami dotyczącymi zarządzania bezpieczeństwem i ochroną danych oraz włączenia cyberbezpieczeństwa do państwowych systemów nadzoru nad bezpieczeństwem i ochroną lotnictwa jako części kompleksowych ram zarządzania ryzykiem. W artykule przedstawione zostały również przykłady cyberincydentów w branży lotniczej w kontekście zdarzeń monitorowanych przez Eurocontrol oraz zalecenia dotyczące poprawy zdolności przewidywania, wykrywania, reagowania i łagodzenia cyberzagrożeń w lotnictwie cywilnym.

Słowa kluczowe: *Cyberbezpieczeństwo; Cyberbezpieczeństwo lotnicze; Lotnictwo cywilne; Cyberatak; Infrastruktura cyfrowa; Infrastruktura krytyczna*

Abstract: Aviation is an example of a highly interconnected and complex sector, with a high level of media exposure and a key role in the socio-economic development of countries. Aviation infrastructure (line and point) constitutes elements of critical infrastructure, which is why it is subject to special protection. In view of the ongoing changes, digitization of many processes in the functioning of airports, airlines, passenger service, data transfer directly related to the nature of aviation, IT systems used by aviation market entities, including: airports, airlines , maintenance organizations, airport services. The article presents the issues of cyber security in civil aviation and the main directions of activities of the civil aviation supervision authorities of the global ICAO and the European EASA. The author presents the leading documents and actions taken so far to ensure cyber security in the field of data protection of all participants of the aviation market, developed at the international level. The author points to ICAO and EASA initiatives relating to cyberspace, the need to coordinate national regulations with relevant regulations on data security and protection management, and to include cybersecurity in state aviation safety and security oversight systems as part of a comprehensive risk management framework. The article also presents examples of cyber incidents in the aviation industry in the context of events monitored by Eurocontrol and recommendations for improving the ability to predict, detect, respond and mitigate cyber threats in civil aviation.

Keywords: *Cybersecurity; Aviation cybersecurity; Civil aviation; Cyberattack; Digital infrastructure; Critical infrastructure*

Globalna infrastruktura cyfrowa stanowi obecnie podstawę niemal każdego aspektu życia gospodarczego i społecznego, a tym samym prowadzi do zmiany paradygmatu w wymianie informacji. Unikalność tej zmiany przejawia się nie tylko szybkim rozwojem technologicznym, ale także bezprecedensowym poziomem globalnej wzajemnej łączności systemów i sieci. To wszystko niesie za sobą skutki w postaci stałego wzrostu cyberataków. Lotnictwo stanowi przykład sektora o rozległych wzajemnych połączeniach i złożoności, wysokim poziomie ekspozycji w mediach oraz kluczowej roli w rozwoju społeczno - gospodarczym państw. Infrastruktura lotnicza (liniowa i punktowa) stanowi elementy infrastruktury krytycznej, przez co podlega szczególnej ochronie. Wobec zachodzących zmian, cyfryzacji wielu procesów w funkcjonowaniu lotnisk, linii lotniczych, obsługi pasażerów, transferu danych bezpośrednio związanych z charakterem lotnictwa, za komponenty infrastruktury lotniczej należy

uznać również systemy informatyczne wykorzystywane przez podmioty rynku lotniczego w tym m.in.: lotniska, linie lotnicze, organizacje obsługowe, służby lotniskowe. Ze względu na swój globalny charakter, sektor lotnictwa podobnie jak interakcje systemów i przepływy danych mu towarzyszące, wykraczające poza granice państw i poszczególnych organizacji, podlegają wysokiemu potencjalnemu ryzyku cyberataków. Na przestrzeni lat, zgodnie ze stałym wzrostem zapotrzebowania na efektywną mobilność ludzi i towarów, sektor lotnictwa cywilnego przeszedł kilka transformacji cyfrowych, których celem było wykorzystanie potęgi technologii dla zwiększenia wydajności i efektywności branży. Pozwoliło to na utrzymanie szybkiego tempa wzrostu przy jednoczesnym zachowaniu bezpieczeństwa. Jednocześnie konsekwencją postępu cyfrowego stała się ekspozycja wszystkich interesariuszy sektora na zagrożenie bezpieczeństwa cybernetycznego. Udane cyberataki mogą mieć (mają) negatywny wpływ na ciągłość i bezpieczeństwo świadczenia usług, reputację podmiotów lotniczych, efektywność finansową, bezpieczeństwo ludzi, samolotów, obiektów infrastruktury lotniczej czy sprzętu używanego w obsłudze pasażerów. Dlatego też podejście do zagadnienia cyberbezpieczeństwa oraz zagrożeń dla lotnictwa cywilnego musi przyjąć kompleksowy charakter opierając się na globalnych ramach, implikujących współpracę pomiędzy państwami oraz wszystkimi zainteresowanymi stronami (organami nadzoru lotniczego, służbami, podmiotami rynku lotniczego, podróżnymi).

Forum do rozwijania współpracy międzynarodowej na rzecz cyberbezpieczeństwa lotnictwa cywilnego stwarza zarówno Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) jak i Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA). Prace nad cyberbezpieczeństwem lotniczym, ewoluowały wraz ze wzrostem uzależnienia lotnictwa cywilnego od technologii. Przestrzeń oraz zwierzchnictwo obu instytucji gwarantuje spójność, harmonizację, zgodność z międzynarodowymi priorytetami lotnictwa cywilnego dla międzynarodowej społeczności transportu lotniczego wraz z zapewnieniem objęcia nadzorem wszystkich dziedzin lotnictwa cywilnego.

Działania ICAO w kwestiach cyberbezpieczeństwa

Prace ICAO w zakresie cyberbezpieczeństwa lotnictwa są wszechstronne i złożone. Obejmują one:

- opracowywanie norm i zalecanych metod postępowania (SARP) (Norma 4.9.1 i Zalecana praktyka 4.9.2 w Załączniku 17 – *Ochrona lotnictwa* [8] do Konwencji o międzynarodowym lotnictwie cywilnym (konwencja chicagowska));
- opracowywanie procedur i materiałów pomocniczych;
- zapewnienie, że ramy międzynarodowego prawa lotniczego są odpowiednie do zwalczania cyberataków na lotnictwo cywilne;
- podnoszenie świadomości na temat znaczenia działań z zakresu cyberbezpieczeństwa w lotnictwie cywilnym;
- wspieranie dyskusji na temat cyberbezpieczeństwa lotnictwa na szczeblu krajowym, regionalnym i globalnym;
- rozwijanie inicjatyw wspierających tworzenie i wdrażanie zdolności dotyczących cyberbezpieczeństwa lotnictwa dla państw oraz szerszej społeczności lotniczej.

Znaczenie działań na rzecz cyberbezpieczeństwem w lotnictwie cywilnym zostało dodatkowo podkreślone przez przyjęcie trzech rezolucji zgromadzenia ICAO:

1. Rezolucja A39-19 – *Zajęcie się cyberbezpieczeństwem w lotnictwie cywilnym* z 2016 r., (zastąpiona w 2019 r. rezolucją nr 2)
2. A40-10 – *Zajęcie się bezpieczeństwem cybernetycznym w lotnictwie cywilnym* oraz (zastąpiona w 2022 rezolucją nr 3)
3. A41-19 – *Rozwiązanie problemu cyberbezpieczeństwa w lotnictwie cywilnym*.

Rezolucje zawierają ważne klauzule, które m.in. uznają wzajemne powiązania pomiędzy cyberbezpieczeństwem a bezpieczeństwem, ochroną i wydajnością lotnictwa. Przedmiotem obrad na zgromadzeniach ICAO w zakresie cyberbezpieczeństwa stało się m.in. zapewnienie przekrojowego, holistycznego podejścia do cyberbezpieczeństwa lotnictwa na poziomie krajowym i międzynarodowym. W ramach 41 Zgromadzenia ICAO wezwano państwa do przyjęcia i wdrożenia Konwencji pekińskiej z 2010 r. (Konwencja o zwalczaniu bezprawnych czynów dotyczących międzynarodowego lotnictwa cywilnego [6]) oraz Protokołu pekińskiego z 2010 r. (Protokół uzupełniający do Konwencji o zwalczaniu bezprawnego zajmowania statków powietrznych [7]) jako sposób radzenia sobie z cyberatakami na lotnictwo cywilne.

Działania EASA w kwestiach cyberbezpieczeństwa

EASA opracowała Plan Działania w Zakresie Bezpieczeństwa Cybernetycznego (ang. Strategy for Cybersecurity in Aviation) [2], który został zatwierdzony przez zarząd w listopadzie 2015 r. Od tego czasu EASA pracuje nad jego wdrożeniem. Podjęto szereg inicjatyw mających na celu lepsze przeciwdziałanie zagrożeniom cybernetycznym w lotnictwie, poprawę odporności oraz wspieranie wbudowanych zabezpieczeń. Oprócz swoich instytucjonalnych działań w zakresie stanowienia przepisów, EASA pracuje nad poprawą międzynarodowej współpracy w tej dziedzinie, jak również nad promowaniem wymiany informacji między zainteresowanymi stronami z branży lotniczej. Osiągnięcie cyberodpornego systemu lotniczego i włączenie cyberbezpieczeństwa do obecnego pojęcia bezpieczeństwa wymaga skoordynowanych wysiłków interesariuszy systemu lotniczego. W tym zakresie EASA uczestniczy i przewodniczy Europejskiej Platformie Koordynacji Strategicznej (ang. European Strategic Coordination Platform, ESCP), w skład której

***1**. Komponenty systemu cyberbezpieczeństwa lotniczej infrastruktury krytycznej. Źródło: opracowanie własne*

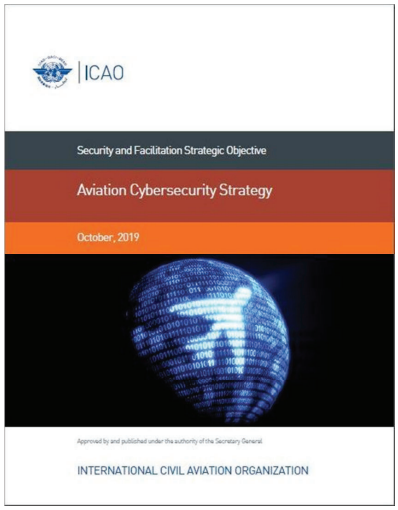
wchodzą przedstawiciele kluczowych zainteresowanych stron z branży, państw członkowskich i instytucji UE. Współpraca przyczynia się do harmonizacji celów interesariuszy lotniczych i umożliwiła opracowanie pierwszej wspólnej strategii cyberbezpieczeństwa w lotnictwie. Zaangażowane zainteresowane strony są również w trakcie określania wspólnego planu działania w celu wdrożenia tej strategii. W celu promocji dobrowolnej wymiany informacji i współpracy ekspertów, EASA wspiera tworzenie Europejskiego Centrum Cyberbezpieczeństwa w Lotnictwie (ECCSA) i zapewnia wstępne zdolności operacyjne we współpracy z CERT-UE.

Strategia Cyberbezpieczeństwa w Lotnictwie Cywilnym według ICAO

Podstawę wizji cyberbezpieczeństwa ICAO stanowi *Strategia bezpieczeństwa cybernetycznego lotnictwa*, zgodnie z którą globalny sektor lotnictwa cywilnego ma być odporny na cyberataki, bezpieczny i chroniony, a jednocześnie nadal zachować możliwości wprowadzania innowacji i rozwoju. Uznając wieloaspektowy i multidyscyplinarny charakter cyberbezpieczeństwa oraz zauważając, że ataki cybernetyczne mogą jednocześnie wpływać na wiele obszarów i szybko się rozprzestrzeniać, konieczna jest wspólna wizja i zdefiniowanie globalnej strategii bezpieczeństwa cybernetycznego. Strategia dostosowana została do innych inicjatyw ICAO związanych z cyberprzestrzenią i skoordynowana z odpowiednimi przepisami dotyczącymi zarządzania bezpieczeństwem i ochroną.

Strategia wyznacza ramy oparte na siedmiu filarach:

1. Współpracy międzynarodowej.
2. Zarządzaniu.
3. Skuteczności ustawodawstwa i przepisów.



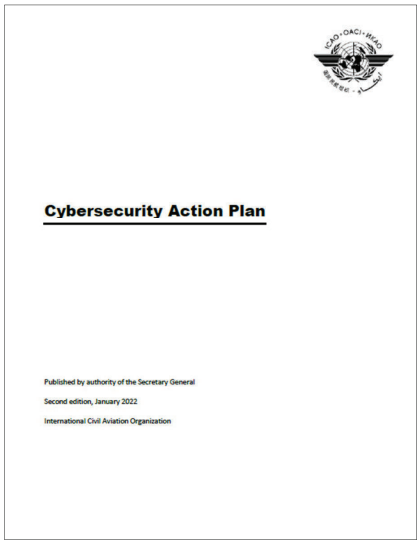
***2**. Publikacja ICAO pt. Strategia Cyberbezpieczeństwa Lotnictwa. Źródło: https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx*

4. Polityce cyberbezpieczeństwa.
5. Udostępnianiu informacji.
6. Zarządzaniu incydentami i planowaniu awaryjnym.
7. Budowaniu potencjału, szkoleniach i kulturze bezpieczeństwa cybernetycznego.

Aspekt współpracy międzynarodowej wynika z ponadgranicznego charakteru zarówno cyberbezpieczeństwa, jak i lotnictwa. Oba wymagają współpracy na poziomie krajowym i międzynarodowym oraz wzajemnego uznawania wysiłków na rzecz rozwoju, utrzymania i poprawy cyberbezpieczeństwa w celu ochrony sektora lotnictwa cywilnego przed wszelkimi cyberzagrożeniami dla bezpieczeństwa i ochrony. Możliwość promocji globalnej spójności i zapewnienia pełnej interoperacyjności środków

***3**. Komponenty ekosystemu lotniczego. Źródło: opracowanie własne*

***4**. Ekosystem lotniczy - interoperacyjność wymiany informacji między użytkownikami. Źródło: Informal Briefing to the ICAO Council, Update on Cybersecurity The Trust Framework, https://www.icao.int/SAM/Documents/2018-GREPECAS18/GRP18_P03.pdf*



***5**. Publikacja ICAO pt. Plan działania w zakresie cyberbezpieczeństwa. Źródło: https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx*

ochrony i systemów zarządzania ryzykiem, wymusza konieczność zharmonizowanych działań na poziomie światowym, regionalnym i krajowym. Państwa członkowskie ICAO, zgodnie ze Strategią Cyberbezpieczeństwa Lotnictwa, muszą sformułować i stosować odpowiednie przepisy ustawowe i wykonawcze zgodne z przepisami ICAO przed wdrożeniem krajowej polityki bezpieczeństwa cybernetycznego w lotnictwie cywilnym.

Cyberbezpieczeństwo ma zostać włączone do państwowych systemów nadzoru nad bezpieczeństwem i ochroną lotnictwa jako część kompleksowych ram zarządzania ryzykiem. W międzyczasie zachęca się państwa do ratyfikowania instrumentów ICAO, w tym: Konwencji o zwalczaniu bezprawnych czynów dotyczących międzynarodowego lotnictwa cywilnego (konwencja pekińska) oraz Protokołu uzupełniającego do Konwencji o zwalczaniu bezprawnego zajmowania statków powietrznych (protokół pekiński).

Z uwagi na fakt istnienia różnych metodologii oceny ryzyka, priorytet należy nadać zmianie i ewentualnemu opracowaniu nowych wytycznych związanych z ocenami zagrożeń i ryzyka dla cyberbezpieczeństwa, w celu osiągnięcia porównywalności wyników takich ocen.

W całym sektorze lotnictwa cywilnego polityka bezpieczeństwa cybernetycznego może uwzględniać pełny cykl życia systemu lotniczego i obejmować takie elementy, jak:

- kulturę bezpieczeństwa cybernetycznego,
- promowanie bezpieczeństwa już w fazie projektowania,
- bezpieczeństwo łańcucha dostaw oprogramowania i sprzętu,
- integralność danych, odpowiednia kontrola dostępu,
- proaktywne zarządzanie lukami w zabezpieczeniach,
- poprawę sprawności aktualizacji zabezpieczeń bez narażania bezpieczeństwa, a także
- włączenie systemów i procesów do monitorowania danych związanych z cyberbezpieczeństwem.

Cyberataki mogą się łatwo rozprzestrzeniać i mieć globalny wpływ. Celem wymiany informacji jest umożliwienie zapobiegania, wczesnego wykrywania i łagodzenia istotnych zdarzeń związanych z cyberbezpieczeństwem, zanim doprowadzą one do szerszych skutków dla bezpieczeństwa lub ochrony lotnictwa. Odpowiednie mechanizmy wraz z kulturą wymiany informacji znacznie zmniejszą systemowe ryzyko cybernetyczne w całym sektorze lotniczym, którego wartość została już udowodniona w zakresie bezpieczeństwa i ochrony lotnictwa. Dzielenie się informacjami na temat takich aspektów, jak słabe punkty, zagrożenia, zdarzenia i najlepsze praktyki, za pośrednictwem ustalonych i zaufanych relacji, może zmniejszyć wpływ trwających ataków.

W kwestii zarządzania incydentami i planowania awaryjnego zgodnie z podejściem ICAO niezbędne jest posiadanie odpowiednich i skalowalnych planów zapewniających ciągłość transportu lotniczego podczas incydentów cybernetycznych. ICAO zaleca, aby państwa i sektor lotniczy korzystały z istniejących planów awaryjnych, które zostały już opracowane i wprowadzały do nich zmiany w celu uwzględnienia przepisów dotyczących cyberbezpieczeństwa. Wysoce zalecane są ćwiczenia w zakresie bezpieczeństwa cybernetycznego jako użyteczne narzędzie do testowania istniejącej odporności cybernetycznej i określania ulepszeń. Ćwiczenia takie mogą mieć różne formaty, np.: ćwiczenia stacjonarne, symulacje lub ćwiczenia w czasie rzeczywistym oraz różną skalę: międzynarodową, krajową, organizacyjną.

Podstawą cyberbezpieczeństwa pozostaje jednak element ludzki. Sektor lotnictwa cywilnego musi podejmować konkretne i skuteczne kroki w celu zwiększenia liczby wykwalifikowanych pracowników posiadających wiedzę zarówno z obszaru lotnictwa, jak i cyberbezpieczeństwa. Cel ten można osiągnąć poprzez zwiększanie świadomości oraz edukację i szkolenia. Programy nauczania związane z cyberbezpieczeństwem oraz cyberbezpieczeństwem lotnictwa na wszystkich poziomach powinny być włączone do krajowych ram edukacyjnych, jak również do odpowiednich międzynarodowych programów szkoleniowych. W lotnictwie należy dążyć do innowacyjnych sposobów łączenia i krzyżowania tradycyjnych technologii informacyjnych i ścieżek kariery w cyberprzestrzeni. Wspieranie i stymulowanie rozwoju umiejętności obecnej i nowej siły roboczej powinno prowadzić do wspierania innowacji w zakresie cyberbezpieczeństwa oraz odpowiednich badań i projektowania rozwiązań dedykowanych branży lotniczej i branż współpracujących.

Lotnictwo cywilne osiągnęło godne pozazdroszczenia wyniki w zakresie bezpieczeństwa (safety i secyrity), które opierają się na proaktywnej kulturze bezpieczeństwa (just culture), którą tworzą i za którą odpowiadają wszyscy. Zasady tej kultury bezpieczeństwa mają być stosowane w celu rozwijania i utrzymywania kultury cyberbezpieczeństwa w całym sektorze lotniczym.

Rezolucja zgromadzenia ICAO A40-10 zwróciła się do ICAO o opracowanie Planu działania w zakresie cyberbezpieczeństwa (ang. Cybersecurity Action Plan CyAP) w celu wsparcia państw i przemysłu w przyjęciu strategii cyberbezpieczeństwa lotnictwa. Pierwsza edycja CyAP została opublikowana w listopadzie 2020 r., a druga w styczniu 2022 r.

CyAP zapewnia podstawę do współ-

pracy ICAO, państw i interesariuszy oraz proponuje szereg zasad, środków i działań, aby osiągnąć cele siedmiu filarów strategii bezpieczeństwa lotniczego. W tym celu CyAP rozwija filary strategii w 32 działaniach priorytetowych, które są następnie podzielone na 51 zadań do wdrożenia przez ICAO, państwa oraz zainteresowane strony.

ICAO kontynuuje opracowywanie materiałów zawierających wytyczne celem dalszego wspierania państw i zainteresowanych stron w zakresie cyberbezpieczeństwa w lotnictwie cywilnym i wdrażania ich obowiązków określonych w normach i zalecanych praktykach ICAO związanych z cyberbezpieczeństwem lotnictwa.

Dotychczas ICAO opublikowało następujące wytyczne:

1. *Rozdział 18 w Podręczniku ochrony lotnictwa ICAO (Doc 8973 – Restricted)*

Rozdział zawiera wytyczne dla państw w zakresie wdrażania ich zobowiązań związanych z normą 4.9.1 w Załączniku 17 – *Ochrona lotnictwa*.

2. Materiał w P*odręczniku ochrony zarządzania ruchem lotniczym* (Doc 9985 – Ograniczony).
   Podręcznik bezpieczeństwa ATM zapewnia całościowe podejście do bezpieczeństwa w środowisku ATM, łącząc wytyczne dotyczące elementów bezpieczeństwa fizycznego i cyberbezpieczeństwa.
3. *Wytyczne dotyczące protokołu sygnalizacji świetlnej.*
   Dokument zawiera wytyczne dotyczące korzystania z protokołu sygnalizacji świetlnej (TLP) w celu ułatwienia wymiany informacji dotyczących cyberbezpieczeństwa. TLP zapewnia prosty i intuicyjny sposób określania przez źródło informacji ograniczeń dotyczących możliwości dalszego udostępniania tych informacji przez odbiorców, minimalizując w ten sposób błąd ludzki polegający na omyłkowym udostępnianiu poufnych informacji poza zamierzonymi odbiorcami.
4. *Wytyczne dotyczące polityki bezpieczeństwa cybernetycznego*
   Dotyczą one ochrony i odporności infrastruktury krytycznej międzynarodowego lotnictwa cywilnego przed zagrożeniami cybernetycznymi oraz wymogu wielostronnej współpracy w lotnictwie cywilnym, a także z organami zewnętrznymi, takimi jak wojsko, organy bezpieczeństwa cybernetycznego i organy bezpieczeństwa narodowego. Materiał zawiera ponadto szablon wspierający opracowanie polityki cyberbezpieczeństwa lotnictwa na poziomie krajowym.
5. *Kultura cyberbezpieczeństwa w lotnictwie cywilnym.*
   Wytyczne opierają się na doświadczeniach lotnictwa cywilnego we wdrażaniu udanych i skutecznych kultur bezpieczeństwa lotniczego i ochrony lotnictwa, łączą odpowiednie elementy z obu kultur i uzupełniają je elementami specyficznymi dla cyberbezpieczeństwa lotnictwa, aby wesprzeć projekt oraz wdrożenie solidnej organizacyjnej kultury cyberbezpieczeństwa w lotnictwie cywilnym.

W ramach działań na rzecz ustalania międzynarodowych ram zaufania lotniczego w 2019 r., kierując się rekomendacją 13 Konferencji Żeglugi Powietrznej, ICAO rozpoczęło prace nad zapewnieniem bezpieczeństwa i odporności systemu żeglugi powietrznej na cyberataki. Działalność ta obejmowała również przechowywanie, przetwarzanie i wymianę danych i informacji spełniającą wymogi poufności, integralności oraz dyspozycyjności. Bieżące prace obejmują opracowanie zasad, polityk i wytycznych dotyczących ram zaufania międzynarodowego lotnictwa (ang. International Aviation Trust Framework IATF). Prace obejmują również zdefiniowanie wymagań wydajnościowych dotyczących przetwarzania, wymiany i przechowywania informacji w aplikacjach sieciowych, w tym opracowanie wymagań technicznych potrzebnych do zaspokojenia obecnych i przyszłych potrzeb lotnictwa.

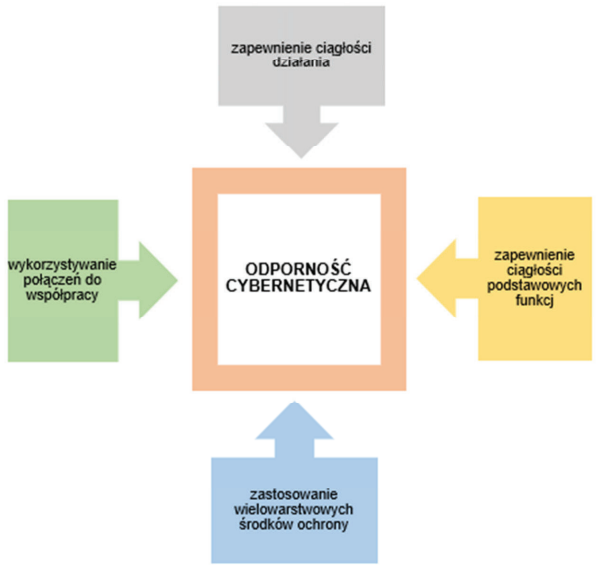
Strategia Cyberbezpieczeństwa w Lotnictwie Cywilnym według EASA

Dokument Strategii Cyberbezpieczeństwa w Lotnictwie (ang. Strategy for Cybersecurity in Aviation) został przyjęty przez Europejską Platformę Koordynacji Strategicznej (ESCP) na krótko przed 40. Sesją Zgromadzenia Ogólnego ICAO. ESCP uznaje znaczenie przeglądu dokumentu strategicznego ESCP z wynikami zgromadzenia oraz zapewnienia spójności i aktualizacji języka odnoszącego się do rezolucji zgromadzenia ICAO w sprawie cyberbezpieczeństwa. Strategia EASA przewiduje przyszły system lotnictwa charakteryzujący się dwoma głównymi udoskonaleniami. Przyszły system lotniczy to:

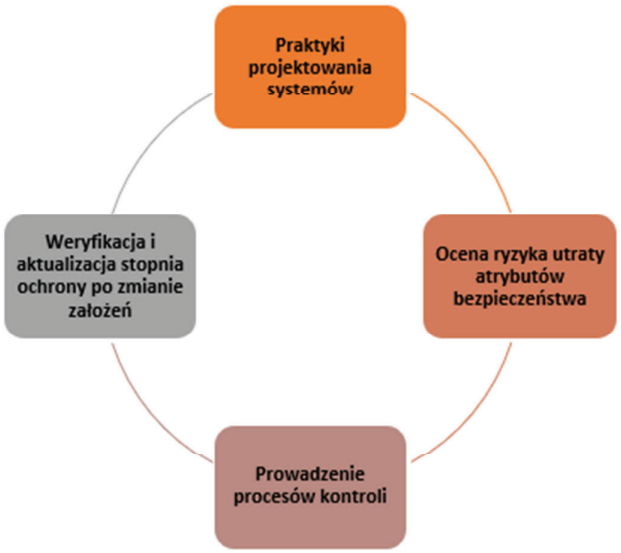
- godnego zaufania i niezawodnego środowiska, aby interesariusze lotnictwa mogli polegać na usługach i informacjach dostarczanych przez innych w celu realizacji swoich celów operacyjnych;
- stworzenie systemu systemów zdolnych do przystosowania się, a tym samym przeciwstawienia się nowym zagrożeniom bez znaczących zakłóceń. System ten ma zostać opracowany poprzez systemowe podejście do cyberbezpieczeństwa w lotnictwie z wykorzystaniem obecnych i starszych systemów.

Osiągnięcie pożądanego ulepszenia, wymaga od zainteresowanych stron z sektora lotnictwa podjęcia wspólnego wysiłku skoncentrowanego na dwóch kierunkach:

1. Uczynienie z lotnictwa ewolucyjnego systemu odpornego na cyberataki, który w przypadku ataku może zachować swoje podstawowe funkcje.
2. Samowzmocnienie lotnictwa poprzez przyjęcie podejścia „wbudowanego bezpieczeństwa", które uwzględnia cele bezpieczeństwa jakie należy osiągnąć od momentu powstania systemów, wraz z tradycyjnymi celami operacyjnymi i bezpieczeństwem.



6. Cele poprawy odporności cybernetycznej wg EASA. Źródło: opracowanie własne



7. Cele samowzmacniającego się systemu lotnictwa wdrażającego wbudowane podejście do bezpieczeństwa. Źródło: opracowanie własne

EASA ustaliła cztery wymierne cele poprawy odporności cybernetycznej:

1. Zapewnienie ciągłości działania dzięki środkom ochronnym rozmieszczonym wzdłuż łańcuchów funkcjonalnych (adekwatnym do poziomu ryzyka),
2. Zapewnienie ciągłości podstawowych funkcji systemów operacyjnych,
3. Stosowanie wielowarstwowych środków ochrony w ramach systemów operacyjnych, które utrudniają postęp ataku,
4. Wykorzystywanie do współpracy istniejących relacji i połączeń w ramach transorganizacyjnego charakteru systemu

oraz cztery wymierne cele dla samowzmacniającego się systemu lotnictwa, wdrażającego wbudowane podejście do bezpieczeństwa:

1. Praktyki projektowania systemów (mają na celu uniknięcie niezamierzonego użycia funkcji dostępnych dla użytkowników),
2. Ocena ryzyka utraty atrybutów bezpieczeństwa oraz wdrożenia środków ochrony, w tym rozwiązań adaptacyjnych,
3. Prowadzenie procesów kontroli (pozwalają na skuteczność bezpieczeństwa systemów w całym cyklu życia),
4. Weryfikacja i aktualizacja stopnia ochrony po zmianie pierwotnych założeń.

Najważniejsze cyberzagrożenia dla branży lotniczej

Branża lotnicza obejmując szerokie spektrum interesariuszy, m.in.: lotnicze, porty lotnicze, służby zarządzania przestrzenia powietrzną, dostawców technologii itp., stanowią jedna z najważniejszych infrastruktur krytycznych wraz z całą jej siecią, zasobami i systemami. Dodatkowo współpracuje również z różnymi branżami podstawowej infrastruktury, w tym z obronnością i bezpieczeństwem narodowym, transportem, komunikacją, bankowością i energią. W rezultacie zakłócenie funkcjonowania branży lotniczej pociąga za sobą negatywne konsekwencje w zakresie zaprowadzenia ładu społecznego i świadczenia usług publicznych.

Przemysł lotniczy, którego działania obejmują skalę międzynarodową obejmując wiele podsektorów, takich jak turystyka i handel zagraniczny, aby sprostać potrzebom tej złożonej struktury musi korzystać z rozwiązań technologicznych. W tym kontekście sektor stopniowo przechodził proces cyfryzacji, przy coraz większym wykorzystaniu innowacyjnych technologii. Pandemia COVID- 19, podobnie jak inne sektory gospodarki, zmusiła branżę lotniczą do implementacji dodatkowych rozwiązań oraz dalszego przeniesienia działalności do sieci. Konsekwencją tak daleko zaistniałej cyfryzacji stała się większa (wzmożona) podatność na cyberataki. Ze względu na charakter branży lotniczej cyberprzestępcy są motywowani dostępem do wrażliwych danych, takich jak paszporty i informacje o kartach kredytowych dużej wartości.

Wśród aktorów stanowiących zagrożenia dla cyberbezpieczeństwa lotniczego można wyróżnić:

- organizacje przeprowadzające ataki sponsorowane przez państwo w celu kradzieży własności intelektualnej i informacji wywiadowczych w celu osłabienia zdolności lotniczych innych krajów, poprawy lokalnych zdolności lotniczych i opracowania technologii zapobiegawczych przeciwko zdolnościom innych krajów [3],
- cyberprzestępcy posiadający niezbędną wiedzę i umiejętności, którzy przeprowadzając ataki koncentrują się na spowodowaniu jak największych szkód,
- cyberterroryści, wywoływani przez czynniki polityczne, religijne, ideologiczne i społeczne. Działania ich skupiają się na zagrożeniu bezpieczeństwa narodowego, powodowaniu masowych ofiar, zaszkodzeniu gospodarce atakowanego państwa, zakłócaniu porządku publicznego oraz podważaniu zaufaniu do systemów lotniczych,
- cyberszpiedzy celujący w przemysł lotniczy, stanowiący jedną z najważniejszych infrastruktur krytycznych. Celem ich działań jest szpiegostwo finansowe, przemysłowe,

politycznego i dyplomatyczne,
- znawcy – tym mianem określani są niezadowoleni pracownicy, byli pracownicy lub partnerzy biznesowi. Motywacją cyberataków z ich strony może być zysk pieniężny lub chęć zemsty,
- aktywiści, którzy nie kierują się względami finansowymi ani politycznymi. Atakują, aby zyskać większy wpływ, rozwinąć umiejętności i uznanie w gronie cyberprzestępców,
- bierni obserwatorzy, działający z zamiarem zebrania informacji. Uzyskują w czasie rzeczywistym obraz ruchu lotniczego i komunikacji z publicznych i prywatnych stron internetowych oraz aplikacji mobilnych, które wyświetlają ruch lotniczy, wykorzystując otwarty charakter protokołów ruchu lotniczego.

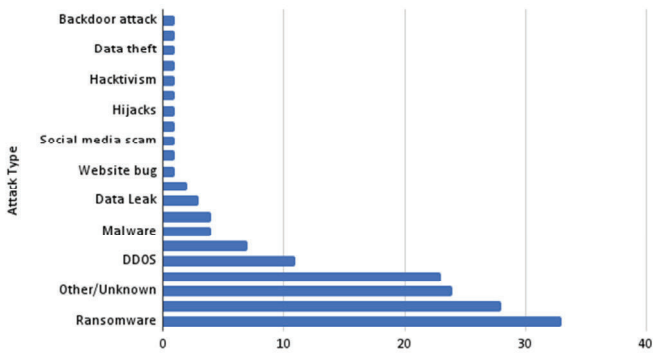
Ataki i luki w zabezpieczeniach

Wykorzystanie złożonych i wzajemnie połączonych systemów informatycznych w przemyśle lotniczym wzrasta z dnia na dzień. Od połączeń Wi-Fi i systemów rozrywki pokładowej dla pasażerów po oprogramowanie używane na lotniskach i liniach lotniczych do zarządzania kontrolą bezpieczeństwa i rezerwacjami - złożone rozwiązania informatyczne są wykorzystywane w całym łańcuchu dostaw przemysłu. Te nowoczesne technologie mają znaczący pozytywny wpływ na systemy sterowania samolotami, poprawiając jakość operacji lotniczych oraz zwiększając bezpieczeństwo i osiągi lotów. Jednak zasila ekosystem, w którym dane przepływają między licznymi interesariuszami a systemami wewnętrznymi/zewnętrznymi. W rezultacie poszerza powierzchnię ataku. Podstawowe technologie stosowane w przemyśle lotniczym można podzielić na kategorie:
- inteligentne systemy,
- urządzenia Internetu rzeczy (ang. Internet of things IoT),
- infrastruktury chmurowe,
- Bigdata,
- Blockchain.

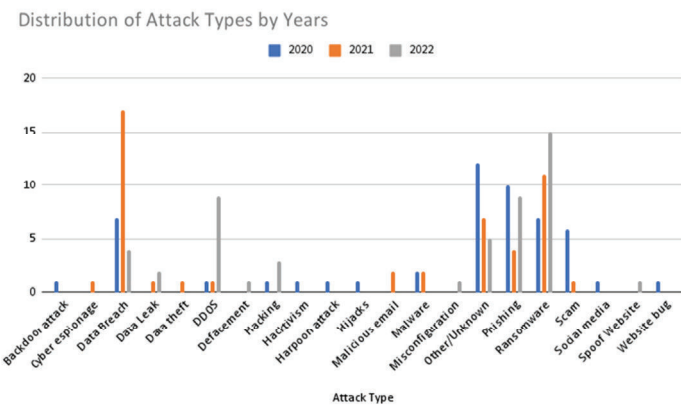
Celem atakujących są zwłaszcza zdalnie atakowane systemy inteligentne (systemy biometryczne, systemy robotyczne itp.), urządzenia IoT (czujniki, siłowniki itp.) oraz systemy chmurowe. Główne systemy często narażone na cyberzagrożenia w branży lotniczej to:
- samolotowe sieci IP lotów,
- cyfrowa kontrola ruchu lotniczego (ATC) i systemy zarządzania ruchem,
- systemy Flight By Wire,
- urządzenia interfejsu podczas lotu,
- serwery historii lotów,
- systemy planowania floty i tras,
- systemy rezerwacji pasażerów oraz programy lojalnościowe lub lojalnościowe,
- portale rezerwacji biletów,
- obsługa i wysyłka ładunków,
- systemy kontroli dostępu, odlotów i paszportów,
- urządzenia personelu pokładowego,
- zagrożenia wewnętrzne.

Cyberataki na przemysł lotniczy w ostatnich latach

W ostatnich latach cyberincydenty w branży lotniczej zostały poddane przeglądowi w kontekście zdarzeń monitorowanych przez Eurocontrol. Eurocontrol (ogólnoeuropejska organizacja cywilno-wojskowa zajmująca się wspieraniem europejskiego lotnictwa) publikuje mapę EATM-CERT (ang. European Air Traffic Management Computer Emergency Response Team) Aviation Cyber Event Map. Dane na tej mapie doprowadziły do następujących ustaleń i wykresów:
- w 2020 r. zgłoszono 52 ataki , w 2021 r. – 48 , a do końca sierpnia 2022 r. – 50 ataków. Tak więc cyberincydenty w 2022 r. osiągnęły średnią z lat 2020 i 2021 zaledwie osiem miesięcy.
- najczęściej obserwowane typy ataków w ciągu ostatnich trzech lat (2020, 2021 i 2022) to ransomware (22 proc.) , naruszenie danych (18,6 proc.) , phishing (15,3 proc.) i DDoS (7,3 proc.). Jako inny/nieznany typ ataku wskazano 16 proc.
- oprócz ataków lotnictwa cywilnego zgłoszono osiem incydentów wojskowych. Niektóre z tych ataków miały na celu cyberszpiegostwo i kradzież danych. Dwa z tych ataków zostały przeprowadzone przy użyciu oprogramowania ransomware , dwa przy użyciu złośliwego oprogramowania, a jeden przy użyciu backdoora. Nie wiadomo, w jaki sposób przeprowadzono trzy z nich.



8. Rodzaje ataków wymierzonych w przemysł lotniczy w latach 2000 - 2022. Źródło: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/



9. Rozkład rodzajów ataków według lat. Źródło: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Tylko w sierpniu 2022 roku miało miejsce siedem ataków. Trzy z nich zostały sklasyfikowane jako wysokie, a cztery jako średnie. Publikowane na ten temat informacje wskazują na naruszenie (zagrożenie) bezpieczeństwa generujące lub mogące wygenerować daleko idące konsekwencje [3]. Wśród przykładowych cyberataków wymienić można:

- cyberatak na portugalską linię lotniczą (TAP Air Portugal), po którym linia lotnicza w wydanym oświadczeniu zapewniła, że jej mechanizmy bezpieczeństwa zostały niezwłocznie aktywowane, a nieautoryzowany dostęp został zablokowany.
- wyciek niektórych baz danych pasażerów linii lotniczych z Malezji i Zjednoczonych Emiratów Arabskich na skutek działań hakerów,
- naruszenie bezpieczeństwa danych osobowych pasażerów Indyjskiej linii lotniczej (Akasa Air), ujawnionych poprzez cyberatak,
- ujawnienie danych osobowych użytkowników aplikacji kanadyjskiej linii lotniczej (WestJet),
- cyberatak, któremu uległa firma American Airlines Group Inc (AAL.O). Zgłosiła ona naruszenie danych na kontach e-mail niewielkiej liczby członków swojego zespołu. Adresy, numery telefonów, numery prawa jazdy, numery paszportów i/lub informacje medyczne mogły uzyskać dostęp do nieautoryzowanych cyberprzestępców.
- cyberatak na linie lotnicze Philippine Airlines. Naruszenie bezpieczeństwa cybernetycznego miało wpływ na zewnętrznego dostawcę IT w ramach programu dla osób często podróżujących. Nazwiska członków, daty urodzenia, narodowość, płeć, data dołączenia, poziom i saldo punktów były wśród naruszonych informacji. Linia lotnicza zaleciła członkom natychmiastową zmianę haseł.
- Ransomware LockBit zaatakował Agencję Bezpieczeństwa Żeglugi Powietrznej w Afryce i na Madagaskarze (ASECNA). Podczas tego bardzo poważnego incydentu dane z 18 krajów członkowskich agencji zostały zaszyfrowane, a agencja zagroziła ujawnieniem naruszonych danych w ciemnej sieci, chyba że zostanie zapłacony okup w wysokości 25 000 USD.

W branży lotniczej, podobnie jak w wielu innych branżach, ewolucja cyfrowa wpływa na wszystkich interesariuszy w ekosystemie lotniczym. Dotyczy zarówno systemów, jak i ludzi, a zmiany w jednym obszarze odczują wszyscy. Cyberprzestępcy kierują się celami finansowymi i politycznymi oraz chęcią zdobycia poufnych informacji. Oprócz ryzyka strat finansowych czy utraty reputacji, udane ataki w sektorze lotniczym mogą spowodować zakłócenia w ruchu lotniczym, wypadki, a nawet utratę życia. Branża lotnicza wykorzystująca liczne rozwiązania technologiczne, celem zapewnienia swoim klientom jak najlepszych doświadczeń użytkowników, musi wykazać się taką samą wrażliwością w wykrywaniu i reagowaniu na cyberzagrożenia.

W tym kontekście dla branży lotniczej można przedstawić zalecenia dotyczące poprawy jej zdolności przewidywania, wykrywania, reagowania i łagodzenia cyberzagrożeń;

- edukacja pracowników w zakresie cyberbezpieczeństwa, a także wyposażenie ich w niezbędne narzędzia o dużej pojemności,
- zidentyfikowanie punktów ryzyka łańcucha dostaw,
- zapewnienie bezpieczeństwa transmisji danych pomiędzy ziemią a samolotem,
- wdrożenie zabezpieczeń dostępu do urządzeń i systemów sieciowych,
- ochrona urządzeń końcowych,
- budowa solidnych systemów zarządzania tożsamością i dostępem z pozycji podmiotu lotniczego oraz z pozycji klienta (podróżnego),
- szyfrowanie wszystkich danych przesyłanych, przechowywanych i przetwarzanych w środowiskach od początku do końca.

Ocena wszystkich systemów lotniczych pod kątem luk w zabezpieczeniach, ustalenie oceny ryzyka i ustalenie priorytetów powinna obejmować kilka elementów. Do niezbędnych zalicza się określenie powierzchni ataku i możliwość ochrony wszystkich zasobów cyfrowych i oszacowanie potencjału wykorzystania informacji pod kątem zagrożenia cybernetycznego oraz do określenia możliwych zagrożeń i proaktywnego reagowania ma kluczowe znaczenie. ◄

Materiały źródłowe

[1] European Strategic Coordination Platform
[2] European Strategic Coordination Platform, Strategy for Cybersecurity in Aviation, First Issue – September 10th, 2019
[3] https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/
[4] https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities#group-easa
[5] https://www.icao.int/aviationcybersecurity/Pages/default.aspx
[6] https://www.icao.int/secretariat/legal/Docs/beijing_convention_multi.pdf
[7] https://www.icao.int/secretariat/legal/Docs/beijing_protocol_multi.pdf
[8] https://www.ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17.pdf
[9] Podręczniku ochrony zarządzania ruchem lotniczym (ICAO Doc 9985)
[10] Rezolucja A39-19 – Zajęcie się cyberbezpieczeństwem w lotnictwie cywilnym z 2016 r.,
[11] Rezolucja A40-10 – Zajęcie się bezpieczeństwem cybernetycznym w lotnictwie cywilnym
[12] Rezolucja A41-19 – Rozwiązanie problemu cyberbezpieczeństwa w lotnictwie cywilnym
[13] Strategy for Cybersecurity in Aviation – Analysis and Objectives