

(NIE)BEZPIECZNY SEKTOR LOTNICZY? SKUTECZNOŚĆ PROCEDUR NA NIEZADAWAJĄCYM POZIOMIE

Transport lotniczy uznaje się za branżę wysoce wrażliwą na zagrożenia, co wynika z jej charakteru oraz oparcia na rozwiązaniach technologicznych, które mogą zostać zakłócone przez czynniki zewnętrzne. W związku z tym nowy raport opracowany przez Atlantic Council wskazuje na kluczowe wyzwania i problemy, które w znaczący sposób wpływają na poziom cyberbezpieczeństwa w lotnictwie. Czy według ekspertów mamy się czego obawiać?

Celem raportu „Aviation Cybersecurity. Scoping the Challenge” jest uchwycenie i zrozumienie różnorodności perspektyw postrzegania cyberbezpieczeństwa w lotnictwie. W treści przedstawiono proces ewolucji postrzegania ochrony wrażliwych systemów i sieci – od początkowego podejścia lekceważącego tą kwestię, po zrozumienie wagi problemu oraz ryzyka związanego z cyberatakami.

Dokument opiera się na analizie współczesnych wyzwań, aby w ten sposób zobrazować zmieniający się krajobraz perspektyw w postrzeganiu cyberbezpieczeństwa w sektorze lotniczym. Możliwości przeprowadzenia incydentu stale rosną, w związku z tym właściwe zarządzanie ryzykiem oraz skuteczna identyfikacja zagrożeń są trudne do osiągnięcia. Rozwój technologiczny sprawia, że cyberbezpieczeństwo staje się coraz bardziej złożonym problemem.

Autorzy raportu pracowali na podstawie danych, pochodzących z ankiet 244 respondentów oraz informacji zgromadzonych podczas wywiadów i warsztatów eksperckich z wybitnymi specjalistami, których tematyka dotyczyła kwestii wirtualnego bezpieczeństwa w lotnictwie.

Pomimo rozwoju technologicznego i rosnących możliwości cyberbezpieczeństwo nieustannie pozostaje jednym z kluczowych wyzwań dla całego sektora. Wśród nich można podkreślić między innymi wagę ochrony systemów i sieci dotyczących bezpośrednio lotów lub szeroko wykorzystywanej w branży technologii informacyjnej (IT). Kolejny obszar odnosi się do relacji między dostawcami z sektora lotniczego a klientami i ich pełnego zabezpieczenia.

„Zarządzanie cyberbezpieczeństwem w lotnictwie wymaga dokonywania przemyślanych wyborów w oparciu o jasne i świadome zrozumienie ryzyka” – czytamy w raporcie. Według respondentów problematyczna jest kwestia dzielenia się informacjami między poszczególnymi podmiotami działającymi w branży. Dla ekspertów większa obiektywność w odniesieniu do szacowania ryzyka stanowi kluczową kwestię, którą bezwzględnie należy rozwiązać, aby skutecznie podnieść poziom cyberbezpieczeństwa całej branży.

W dokumencie podkreślono, że dzięki innowacyjnym projektom oraz praktyce szkoleniowej sektor lotniczy regularnie pracuje nad podnoszeniem umiejętności w zakresie przewidywania zagrożeń lub minimalizacji ich skutków. Jednak wdrożenie kwestii cyberbezpieczeństwa do tego procesu nadal

stanowi poważne wyzwanie dla wszystkich podmiotów. Autorzy raportu wskazują, że szkolenie operacyjne (przeznaczone dla między innymi pilotów czy kontrolerów ruchu lotniczego) w niewielkim stopniu kształtuje zdolność rozpoznawania oraz zarządzania cyberincydentami.

W związku z tym w raporcie postawiono tezę, że w przypadku wystąpienia poważnego cyberataku jego opanowanie może okazać się bardzo trudne. Co więcej, działania hakerskie wymierzone w integralność danych mogą w znaczący sposób osłabić zdolność operatorów lotniczych do bezpiecznego realizowania swoich zadań. Wyzwania te muszą zostać uwzględnione na każdym szczeblu zarządzania w sektorze transportu powietrznego.

Prowadzone analizy wykazały również, że pomimo istnienia wielu standardów oraz procedur bezpieczeństwa, ich przejrzystość, a przede wszystkim skuteczność znajduje się na niezadowalającym poziomie. Wynika to z faktu, że przepisy tworzone są przez różne oddzielne podmioty zarówno na gruncie krajowym i regionalnym, ale także w ramach konkretnej organizacji. W ten sposób dochodzi do sytuacji, w której występuje złożoność regulacji, a przez to stają się one nieczytelne oraz trudne do praktycznego wykorzystania.

„Poprawa cyberbezpieczeństwa w lotnictwie to proces, a każdy zaangażowany podmiot musi być w stanie zrealizować swoje zadania, aby ryzyko mogło zostać skutecznie ograniczone” – stwierdzono w raporcie. Eksperti uważają, że najlepszym sposobem na poprawę skuteczności wirtualnych zabezpieczeń w lotnictwie jest realizacja zasady „likwidacji wszystkich luk”. Osiągnięcie wysokiego poziomu cyberbezpieczeństwa jest możliwe tylko dzięki wspólnemu wysiłkowi oraz skupieniu uwagi na całym sektorze.

Czytaj też: [Cyberbezpieczeństwo europejskich portów do poprawy](#)