**aut. Szymon Palczewski** 29.11.2019

# CYBERBEZPIECZEŃSTWO EUROPEJSKICH PORTÓW DO POPRAWY

Cyberbezpieczeństwo portów morskich jest kluczowym elementem funkcjonowania, rozwoju i automatyzacji portów - twierdzą autorzy raportu opracowanego przez unijny organ. Zabezpieczenia muszą odpowiadać wyzwaniom przyszłości. Jak poważne są obecne zaniedbania?

Transport morski jest jednym z kluczowych obszarów gospodarki Unii Europejskiej. Umożliwia import i eksport towarów, zaopatrzenie w energię, a także przewóz pasażerów oraz innych pojazdów. Jest podstawowym elementem handlu międzynarodowego realizowanego przez Wspólnotę.

Jak wskazano w raporcie „Port Cybersecurity. Good practices for cybersecurity in the maritime sector" opracowanym przez ENISA, globalny trend cyfryzacji sprawia, że operatorzy portów morskich muszą sprostać wyzwaniom w obszarze technologii informacyjno-komunikacyjnych. Rozwój innowacji wymaga od nich wdrożenia najnowszych rozwiązań, aby w ten sposób były one bardziej konkurencyjne, spełniały określone standardy oraz swoje funkcje. To wszystko sprawia, że pojawiają się nowe wyzwania związane z cyberbezpieczeństwem, zarówno w zakresie technologii informatycznych (IT), jak i operacyjnych (OT).

Specjaliści ENISA zidentyfikowali najważniejsze wyzwania związane z „operacjami krytycznymi", a następnie przedstawili główne zagrożenia dla portów morskich. W treści raportu zawarto również potencjalne scenariusze cyberataków, które w sposób znaczący mogą wpłynąć na ich funkcjonowanie.

Szerokie podejście do zagadnienia pozwoliło ekspertom na wyciągnięcie wniosków oraz opracowanie rekomendacji dla operatorów, aby lepiej chronić systemy oraz sieci znajdujące się w portach morskich. Wśród nich można wskazać na:

- Konieczność zdefiniowania jasnych kryteriów zarządzania cyberbezpieczeństwem w portach, angażując wszystkie zainteresowane strony oraz podmioty z nich korzystające. W praktyce wiele firm odpowiada za sprawne funkcjonowanie obiektów i urządzeń przybrzeżnych, między innymi operatorzy, przedsiębiorstwa żeglugowe lub pilotażowe. W tym aspekcie bardzo ważne jest, aby wszystkie podmioty zapewniały najwyższy standard bezpieczeństwa;
- Podnoszenie świadomości na temat zagadnień związanych z cyberbezpieczeństwem w kontekście portów oraz szerzenie „wysokiej kultury zabezpieczeń". Według ENISA sektor żeglugi morskiej jako całość jest dobrze zabezpieczony przed tradycyjnymi zagrożeniami, jednak brakuje pełnego zintegrowania działań na rzecz cyberbezpieczeństwa. Aby to zmienić należy prowadzić specjalistyczne szkolenia, które pozwolą wszystkim podmiotom zrozumieć istotę i znaczenie wirtualnych zabezpieczeń;
- Egzekwowanie podstawowych technicznych zasad cyberbezpieczeństwa, w tym właściwa segregacja sieci czy sprawne wprowadzanie aktualizacji, ma kluczowe znaczenie z punktu widzenia bezpieczeństwa infrastruktury OT;
- Konieczność uwzględniania kwestii wirtualnego bezpieczeństwa już na fazie projektowania

systemów i sieci. Jak wskazano w raporcie, wiele portów używa aplikacji, które są otwarte dla stron trzecich, co może zostać wykorzystane przez hakerów na przykład do kradzieży danych. „Każda luka w tych systemach może być bramą do cyberataku na sieci portów" – czytamy w dokumencie;
- Wzmacnianie zdolności do wykrywania i reagowania na incydenty na poziomie portu w taki sposób, aby jak najszybciej odpowiedzieć na cyberatak, zanim wpłynie on na działanie całego obiektu. Według ENISA „porty mogą polegać na prostych środkach wykrywania, takich jak alerty lub opierać się na bardziej zaawansowanych technologiach, w tym sztucznej inteligencji, do identyfikacji zagrożeń".

Ze względu na fakt, że cyfrowa transformacja dotyczy również portów, cyberbezpieczeństwo powinno być postrzegane nie tylko jako kluczowy element, który należy wziąć pod uwagę w odniesieniu do potencjalnych zagrożeń, ale również jako czynnik umożliwiający dalszy rozwój i automatyzację. „Ze względu na złożoność czynników oraz wyzwań wpływających na kondycję cyberbezpieczeństwa, dbanie o jego jakość nie jest i nie będzie łatwe" – stwierdzono w dokumencie.

Raport ENISA jest skierowany również do podmiotów działających na terenie Polski. Rzeczpospolita z racji posiadania portów morskich oraz przynależności do Unii Europejskiej została zobowiązana do poprawy zabezpieczeń w swoich obiektach. Dbałość o dobro Wspólnoty zależy od wysiłków podejmowanych przez wszystkie państwa członkowskie. Polska jako jedno z nich jest zobligowana do zapoznania się z treścią raportu oraz wdrożenie rekomendacji opracowanych przez ENISA. Jednak czy Warszawa zastosuje się do wszystkich wytycznych wskazanych przez unijny organ?

**Czytaj też:** Ile kosztuje cyberatak na porty? Miliardowe straty dla globalnej gospodarki