



8

MIĘDZYNARODOWY
**KONGRES
MORSKI**

▪ 14-15.09.2021 SZCZECIN

**CYBERBEZPIECZEŃSTWO
I SZYBKIE REAGOWANIE
W GOSPODARCE MORSKIEJ**

ZAREJESTRUJ SIĘ

KONGRES-MORSKI.COM.PL

POJAWIENIE SIĘ ZAGROŻEŃ ATAKÓW CYBERNETYCZNYCH

Ilość cybernetycznych ataków wzrasta z roku na rok wraz z rozwojem technologii informatycznych oraz automatyzacji procesów w gospodarce.

Gospodarka morska chętnie korzysta z nowoczesnych technologii. Korzyści płynące z wykorzystywania technologii informatycznych i komunikacyjnych dotyczą między innymi możliwości optymalizacji procesów, poprawy ich efektywności, redukcji kosztów operacyjnych, zwiększenia niezawodności.

Wykorzystanie nowoczesnych technologii przynosi wiele korzyści, ale też niesie ze sobą szereg zagrożeń, w tym zagrożenia ataków cybernetycznych.

POTENCJALNE I RZECZYWISTE SKUTKI ATAKÓW CYBERNETYCZNYCH

Potencjalne skutki ataków cybernetycznych:

- Przerwanie/utrata dostępu do krytycznych systemów lub infrastruktury skutkujące opóźnieniami logistycznymi
- Utracona lub opóźniona sprzedaż i dochód
- Wpływ na zdrowie, bezpieczeństwo i środowisko
- Zwiększone wydatki
- Kary nałożone z powodu naruszeń przepisów
- Kary umowne lub utrata premii umownych
- Niezadowolenie klienta/utrata reputacji

POTENCJALNE I RZECZYWISTE SKUTKI ATAKÓW CYBERNETYCZNYCH

Rzeczywiste skutki ataków cybernetycznych na firmy branży morskiej

- A.P. Moeller-Maersk – duński koncern działający głównie w branży transportu morskiego, 2017
- APM Terminals –terminale kontenerowe w Rotterdamie, 2017
- COSCO Shipping Lines – dostawca usług spedycyjnych i logistycznych obsługujący ponad 1100 statków, 2018
- Port San Diego – port na zachodnim wybrzeżu USA, 2018
- Pemex – największy meksykański koncern naftowy, 2019
- Port Shahid Rajaee – port w Iranie, 2020
- Vard – norweska stocznia , 2020

ZAGROŻENIA DLA INFRASTRUKTURY KRYTYCZNEJ KRAJU – BEZPIECZEŃSTWO NARODOWE

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016, zwana Dyrektywą NIS
- Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018
- Zarządzenie MGMiŻŚ z 07.04.2020 w sprawie warunków organizacyjno-technicznych oraz zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego

OBSZARY GOSPODARKI MORSKIEJ NARAŻONE NA ATAKI CYBERNETYCZNE

- Transport i logistyka
- Porty wraz z funkcjonującymi na jego terenie centrami logistycznymi i otaczającą infrastrukturą komunikacyjną
- Stocznie
- Żegluga, statki, przedsiębiorstwa armatorskie
- Inne, np. podmioty działające na rzecz bezpieczeństwa żeglugi i statków, właściwego korzystania z dróg morskich, portów i przystani, ochrony środowiska, ratowania życia na morzu, specjalistycznego dozoru technicznego, ochrony brzegów morskich, itp.

OBSZARY GOSPODARKI MORSKIEJ NARAŻONE NA ATAKI CYBERNETYCZNE

- Rezolucja MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (przyjęta 16.06.2017)
- MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management (wydany 05.07.2017)
- IMO MSC 104/7/1 Measures to Enhance Maritime Security - IAPH Cybersecurity Guidelines for Ports and Port Facilities (wydany 02.07.2021)

DZIAŁANIA NIEZBĘDNE DO OBRONY PRZED ATAKAMI CYBERNETYCZNYMI I MINIMALIZACJI SKUTKÓW ATAKÓW

Działania w oparciu o zarządzanie ryzykiem:

- identyfikacja usług kluczowych oraz aktywów kluczowych
- identyfikacja zagrożeń, podatności, oceny funkcjonujących zabezpieczeń
- analiza ryzyka
- określenie działań niezbędnych dla minimalizacji skutków, bądź obniżenia prawdopodobieństwa
- monitorowanie ryzyka
- raportowanie

CZYNNIK LUDZKI A CYBERBEZPIECZEŃSTWO ORGANIZACJI

Firma może dokonać zakupu najlepszych i najdroższych technologii bezpieczeństwa,
wyszkolić personel tak, aby każda poufna informacja była trzymana w zamknięciu,
wynająć najlepszą firmę chroniącą obiekty i wciąż pozostać niezabezpieczoną.
(Kevin Mitnick)

CZYNNIK LUDZKI A CYBERBEZPIECZEŃSTWO ORGANIZACJI

(...) Jeżeli atakujący znajdzie choć jedną podatną na sugestie osobę wewnątrz organizacji,

i osoba ta pozwoli sobie manipulować,
wszystkie te pieniądze wyłożone na ochronę będą zmarnowaną inwestycją.

(Kevin Mitnick)

CZYNNIK LUDZKI A CYBERBEZPIECZEŃSTWO ORGANIZACJI

Socjotechnika – mechanizmy w oparciu o które człowiek pozwala sobą manipulować:

- Władza
- Sympatia
- Wzajemność
- Konsekwencja
- Przyzwolenie społeczne
- Rzadka okazja

BEZPIECZEŃSTWO CYBERNETYCZNE JAKO ELEMENT BEZPIECZEŃSTWA NA MORZU

Kwestie zarządzania ryzykiem związanym z zagrożeniami cybernetycznymi zostały podjęte przez Międzynarodową Organizację Morską IMO.

- Komitet Bezpieczeństwa na Morzu (MSC)
- Komitet Ułatwień w Obrocie Morskim (FAL)
- MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management (wydany 05.07.2017)
- Rezolucja MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (przyjęta 16.06.2017)

BEZPIECZEŃSTWO CYBERNETYCZNE JAKO ELEMENT BEZPIECZEŃSTWA NA MORZU

Wytyczne IMO wskazują na systemy statkowe, które mają krytyczne znaczenie dla bezpieczeństwa lub ochrony i mogą być podatne na zagrożenia cybernetyczne.

- Systemy mostka nawigacyjnego
- Systemy przeładunkowe
- Systemy napędowe i maszynowe oraz sterowania nimi
- Systemy kontroli dostępu
- Systemy obsługi pasażerów
- Systemy komunikacyjne

BEZPIECZEŃSTWO CYBERNETYCZNE JAKO ELEMENT BEZPIECZEŃSTWA NA MORZU

Wytyczne wskazują również kilka elementów funkcjonalnych, które wspierają proces efektywnego zarządzania zagrożeniami cybernetycznymi:

- Identyfikacja
- Ochrona
- Wykrywanie
- Odpowiedź
- Odzyskanie

BEZPIECZEŃSTWO CYBERNETYCZNE JAKO ELEMENT BEZPIECZEŃSTWA NA MORZU

Wytyczne w sprawie bezpieczeństwa cybernetycznego na statkach przygotowały inne organizacje i stowarzyszenia branży morskiej np.:

- BIMCO (Baltic and International Maritime Council)
- ICS (International Chamber of Shipping)
- Stowarzyszenia armatorskie: CLIA, INTERCARGO, INTERTANKO
- Morski przemysł wydobywczy: OCIMF (Oil Companies International Marine Forum)
- Ubezpieczyciele: IUMI (International Union of Marine Insurance)

BEZPIECZEŃSTWO CYBERNETYCZNE JAKO ELEMENT BEZPIECZEŃSTWA NA MORZU

Rola Towarzystw klasyfikacyjnych IACS oraz cele w zakresie bezpieczeństwa cybernetycznego:

- Zapewnienie środków wspierających uzyskanie odporności na incydenty cybernetyczne
- Stworzenie rozwiązań prewencyjnych, które wzmocnią ochronę statków przed celowymi lub incydentalnymi zagrożeniami cybernetycznymi
- Określenie kryteriów do projektowania i weryfikacji, które branża morska wykorzysta jako podstawę do przeciwdziałania zagrożeniom cybernetycznym

DZIĘKUJĘ ZA UWAGĘ



LESZEK POKORA
GŁÓWNY INSPEKTOR
POLSKI REJESTR STATKÓW S. A.