Sokołowski Wojciech
Akademia Marynarki Wojennej

WYBRANE ASPEKTY CYBERBEZPIECZEŃSTWA AUTONOMICZNYCH STATKÓW MORSKICH

STRESZCZENIE

W artykule poruszono zagadnienia dotyczące cyberbezpieczeństwa autonomicznych statków morskich. Scharakteryzowano wybrane cyberataki, które miały miejsce w sektorze morskim. Omówiono cele, sekwencję i skutki cyberataków oraz regulacje prawne w zakresie cyberbezpieczeństwa morskiego. Jednak najwięcej uwagi poświęcono sposobom zapobiegania cyberzagrożeniom i kształtowaniu przemyślanej polityki cyberbezpieczeństwa morskiego.

Słowa kluczowe:
statek autonomiczny, cyberatak, zarządzanie cyberryzykiem

WSTĘP

Cyberbezpieczeństwo obejmuje szereg technologii, procesów i praktyk mających na celu ochronę sieci, komputerów, oprogramowania i danych przed atakiem, uszkodzeniem lub nieuprawnionym dostępem[1], przy czym bardziej dotyczy to ochrony danych i informacji niż bezpieczeństwa fizycznego. Jednak wraz ze wzrostem cyberprzestępczości i pojawieniem się nowych technologii, takich jak Internet Rzeczy, pojawiają się nowe wyzwania w zakresie zapewnienia bezpieczeństwa. Konieczność odpowiedniej ochrony systemów, sieci i danych w cyberprzestrzeni staje się bardziej istotna niż kiedykolwiek wcześniej.

Sektor morski jest również narażony na cyberzagrożenia, gdyż dotyczą one dowolnego systemu komputerowego, który nie musi być koniecznie podłączony do sieci. W ostatnim dziesięcioleciu wzrosła liczba incydentów związanych z cyberprzestępczością. Ataki różnią się skalą i zakresem wyrządzonych

[1] https://searchsecurity.techtarget.com/definition/cybersecurity, dostępny 15.10.2020 r.

szkód, ale nie ma żadnych wątpliwości co do ich negatywnego wpływu. Szczególne obawy budzą zagrożenia wewnętrzne, od nieświadomej lub przypadkowej interwencji po złośliwe działania niezadowolonego pracownika.

Główną różnicą w cyberbezpieczeństwie morskim w stosunku do innych sektorów jest geolokalizacja statków. Obecnie statki na morzu polegają w dużej mierze na łączności satelitarnej, a dostępna szerokość pasma jest znacznie zmniejszona w porównaniu do tej, która jest dostępna, gdy statek znajduje się na doku lub w strefie przybrzeżnej. Jednak wraz ze wzrostem cyfryzacji i podłączania statków do nowych lub istniejących sieci to ograniczenie (lub w pewnym sensie ochrona cybernetyczna) ulegnie zmniejszeniu, a wpływ określonej lokalizacji statku stanie się nieistotny.

Obecnie wykorzystywane statki posiadają oddzielnie zarządzane systemy operacyjne OT (ang. *Operational Technology*), takie jak np. systemy mostkowe czy systemy sterowania napędem, jednak coraz częściej również i one zostają podłączane do sieci, co w pewnym sensie prowadzi do konwergencji systemów OT i systemów IT (ang. *Information Technology*). Dodatkowo sensory i efektory będące na wyposażeniu statków przesyłają dane za pomocą określonych technologii komunikacyjnych CT (ang. *Communication Technology*). W konsekwencji na statkach powstają nowe zintegrowane technologie, które z jednej strony umożliwiają płynne działanie systemów autonomicznych, natomiast z drugiej narażają je na potencjalne cyberataki.

Cyberataki mogą wywoływać określone skutki ekonomiczne i wpływać negatywnie na infrastrukturę portową, a to, przynajmniej obecnie, rodzi wiele wątpliwości chociażby w zakresie likwidacji potencjalnych szkód z polis ubezpieczeniowych. Sieć łącząca kontrolę ruchu oraz urządzenia supra i infrastruktury portowej jest już obecnie narażona na ataki, a pojawienie się w portach całkowicie lub częściowo autonomicznych statków dodatkowo zwiększy poziom zagrożenia. Co gorsza, w przeciwieństwie do systemów IT, systemy OT są bardziej podatne na zagrożenia, ponieważ nie mają pulpitu nawigacyjnego, który umożliwia operatorom monitorowanie stanu wszystkich połączonych systemów.

W przemyśle morskim i nie tylko, widać wyraźny trend w kierunku większej cyfryzacji i coraz większej zależności od systemów sieciowych i autonomicznych, tym samym podatność na ataki zintegrowanych w ten sposób różnych systemów statkowych na pewno ulegnie zwiększeniu. Incydenty cybernetyczne, takie jak złośliwe oprogramowanie, phishing lub DDoS, mogą potencjalnie prowadzić do znacznej utraty zaufania klientów lub branży, pogorszenia reputacji, potencjalnie poważnych strat finansowych lub kar, a także do sporów sądowych. W najgorszym przypadku naruszenia określonych systemów statkowych mogą powodować przerwanie działalności, zanieczyszczenie środowiska, utratę ładunku, fizyczne obrażenia członków załogi oraz utratę lub uszkodzenie jednostek.

W ten syntetyczny sposób można scharakteryzować nowo kształtujący się świat cyberprzestępczości morskiej.

Celem niniejszego opracowania jest analiza wybranych aspektów cyberbezpieczeństwa statków autonomicznych. Autor, jako główny problem badawczy, sformułował następujące pytanie: jakie elementy tworzą środowisko cyberbezpieczeństwa statków autonomicznych i w jaki sposób na nie wpływają? Główny problem badawczy zdekomponowano na problemy szczegółowe, które przybrały formę następujących pytań:

1. Jaka była skala i zakres dotychczasowych cyberataków w przemyśle morskim?
2. Czy istnieją określone regulacje prawne tworzące ramy budowy stosownych architektur cyberbezpieczeństwa morskiego?
3. Jakie negatywne implikacje mogą powodować dla jednostek pływających incydenty cybernetyczne?
4. Jakie są sposoby i metody przeciwdziałania zagrożeniom cybernetycznym, na które narażone są statki autonomiczne?
5. Czy istnieją systemy zarządzania ryzykiem cybernetycznym w sektorze morskim?
6. Jakie są metody oceny cyberryzyka jednostek pływających?

Natomiast wśród zadań badawczych wyróżnić można następujące:

- analiza incydentów cybernetycznych w sektorze morskim,
- analiza norm, regulacji, standardów w obszarze cyberbezpieczeństwa morskiego,
- analiza celów, skutków i sprawców cyberataków,
- analiza środków i procedur przeciwdziałania cyberatakom,
- analiza systemów zarządzania cyberryzykiem morskim.

Główne metody badawcze wykorzystane w procesie badawczym to metoda badania dokumentów, metoda analizy i krytyki piśmiennictwa, oraz metoda analizy i konstrukcji logicznej.

PRZYKŁADY CYBERATAKÓW W PRZEMYŚLE MORSKIM

Liczba cyberataków na statkowe systemy operacyjne OT wzrosła o 900% w ciągu ostatnich trzech lat. W 2017 roku zgłoszono 50 znaczących włamań do systemów OT, w 2018 roku liczba ta wzrosła do 120 i ponad 310 w 2019 r. Z kolei bieżący rok najprawdopodobniej zakończy się około 500 poważnymi naruszeniami bezpieczeństwa cybernetycznego.[2] Warto podkreślić również to, że od

[2] N. Blenkey, *Cybersecurity: Attacks on OT systems are on the increase*, https://www.marinelog.com/news/cybersecurity-attacks-on-ot-systems-are-on-the-increase/, dostępny 20.10.2020 r.

czasu wybuchu pandemii koronawirusa liczba cyberataków na sektor morski, szczególnie na Bliskim Wschodzie i w Chinach, wzrosła aż o 400 %.[3]

Cyberatak Maersk

Jako pierwszy przykład takiego cyberataku można wskazać ten, który dotknął w czerwcu 2017 r. duńskiego giganta morskiego – przedsiębiorstwo Maersk. Ten największy operator kontenerowców i statków zaopatrzeniowych z biurami w 130 krajach i ponad 80 000 pracowników stał się „ślepy" po zainfekowaniu jego systemów informatycznych wirusem NotPetya.

Wirus rozprzestrzenił się w sieci w siedem minut. Ekrany komputerów zrobiły się czarne, a pracownicy usiłowali odłączyć wszystkie podłączone urządzenia w biurach, aby uchronić się przed szybko rozprzestrzeniającym się złośliwym oprogramowaniem. Z wyjątkiem nieuszkodzonego kontrolera domeny z biura w Ghanie, który akurat w momencie ataku nie miał zasilania, Maersk stracił większość swoich danych z ponad 49 000 laptopów i 4000 serwerów, które zostały zniszczone. Szkody oszacowano na ponad 300 milionów dolarów[4].

Co ciekawe wirus NotPetya, chociaż ma ogólne cechy oprogramowania ransomware, z technicznego punktu widzenia nie jest oprogramowaniem ransomware. Jest w stanie rozprzestrzeniać się samodzielnie. Opiera się na narzędziach takich jak exploity EternalBlue i EternalRomance opracowane przez Amerykańską Agencję Bezpieczeństwa Narodowego (NSA)[5]. NotPetya szyfruje wszystko na swojej drodze i uszkadza dane w sposób niemożliwy do naprawienia i bez możliwości odzyskania[6]. To, co miało być rzekomo sponsorowanym przez państwo rosyjskie cyberatakiem wymierzonym w ukraińskie firmy, rozprzestrzeniło się poza ukraińskie granice i spowodowało szkody na całym świecie szacowane na około 10 miliardów dolarów.

[3] Maritime Logistics Professional, *Total Shipping Losses Are Declining, But Challenges Persist – Report*, https://www.maritimeprofessional.com/news/total-shipping-losses-declining-challenges-360154, dostępny 21.10.2020 r.

[4] A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, dostępny 27.10.2020 r.

[5] J. Fruhlinger, *Petya ransomware and NotPetya malware: What you need to know now*, https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html, dostępny 27.10.2020 r.

[6] M. Suiche, *Petya.2017 is a wiper not a ransomware*, https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b, dostępny 27.10.2020 r.

Cyberatak COSCO

Na kolejny poważny cyberatak nie trzeba było czekać zbyt długo. Nastąpił on już w lipcu 2018 r., kiedy to przedsiębiorstwo China Ocean Shipping Company (COSCO) stało się ofiarą oprogramowania ransomware SamSam[7]. Atak ten spowodował awarię w sieciach COSCO w Stanach Zjednoczonych, Kanadzie, Panamie, Argentynie, Brazylii, Peru, Chile i Urugwaju.

Podobnie jak w przypadku NotPetya, gdy SamSam przeniknie do sieci, hakerzy mogą uzyskać prawa administracyjne i uruchamiać pliki wykonywalne bez udziału człowieka lub autoryzacji. Grupa stojąca za SamSam nie zarządza swoim oprogramowaniem ransomware w modelu SaaS, tylko programuje je wewnętrznie i często aktualizuje, aby uniknąć zabezpieczeń korporacyjnych[8].

Atak SamSam miał miejsce wkrótce po przejęciu przez COSCO jednego ze swoich rywali, Orient Overseas Container Lines[9]. Przedsiębiorstwo, dzięki posiadaniu planów awaryjnych, wróciło do normalnego funkcjonowania w ciągu pięciu dni, przy czym nie ujawniło skali i zakresu poniesionych strat[10].

Ponieważ COSCO odizolował swoje sieci wewnętrzne na całym świecie, zakres wyrządzonych szkód był zdecydowanie mniejszy niż w przypadku duńskiego Maerska. W tym aspekcie pozytywnie należy także ocenić posiadanie alternatywnych procedur komunikacji z klientami i obsługi zgłoszeń serwisowych. Mimo tego, że sam proces komunikacji z klientami za pośrednictwem e-maili i rozmów telefonicznych zajmował więcej czasu, to pracownicy firmy byli w stanie kontynuować obsługę ładunków w Stanach Zjednoczonych i Kanadzie bez jakichkolwiek zakłóceń.

[7] E. Lopez, *Ransomware attack hits COSCO in US*, https://www.supplychain-dive.com/news/COSCO-US-ransomware-attack/528557/, dostępny 28.10.2020 r.
[8] S. Ragan, *SamSam explained: Everything you need to know about this opportunistic group of threat actors*, https://www.csoonline.com/article/3263777/samsam-explained-everything-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html, dostępny 27.10.2020 r.
[9] C. Paris, *China's Cosco Shipping Hit by Cyberattack in U.S.*, https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557, dostępny 27.10.2020 r.
[10] E. Lopez, *COSCO restores service 5 days after cyberattack*, https://www.supplychain-dive.com/news/COSCO-cyberattack-restores-service/528897/, dostępny 27.10.2020 r.

Cyberatak Norsk Hydro

Kolejny atak miał miejsce w marcu 2019 r. Tym razem jego obiektem była światowa sieć Norsk Hydro, a sprawcą oprogramowanie ransomware LockerGoga[11]. Mimo, że Norsk Hydro nie jest bezpośrednio związany z morzem, może służyć jako sygnał ostrzegawczy dla branży morskiej.

Użyty do ataku wirus LockerGoga jest o tyle niebezpieczny, gdyż wyłącza kartę sieciową komputera, odłączając go tym samym od sieci, zmienia hasła użytkownika i administratora oraz wylogowuje komputer. LockerGoga czasami pozostawia ofiarę bez możliwości zobaczenia tzw. wiadomości z okupem lub nawet bez wiedzy, że została ona zainfekowana, co dodatkowo opóźnia zdolność organizacji do odzyskania swoich systemów.

Norsk Hydro oszacował, że hakerzy dostali się do ich sieci dwa lub trzy tygodnie przed ich wykryciem. Poprzez zainfekowanie ponad 22 000 komputerów i tysięcy serwerów na pięciu kontynentach, LockerGoga zniszczył całą światową sieć Norsk Hydro, wpływając na ich produkcję i działalność biurową. Szkody oszacowano na 71 milionów dolarów[12].

Przedsiębiorstwo potrzebowało kilku miesięcy, aby odbudować swoją infrastrukturę i wdrożyć podzieloną na segmenty sieć zapewniającą właściwą ochronę firmowych systemów. W czasie wstępnych badań odkryto także kilka wariantów wirusa, które hakerzy wprowadzili na wypadek, gdyby nie udało im się za pierwszym razem.

Cyberatak Shahid Rajaee

Ostatnim przykładem cyberataku, może być ten z 9 maja 2020 roku, kiedy to cały ruch żeglugowy w terminalu portowym Shahid Rajaee w Iranie został gwałtownie zatrzymany. Według The Washington Post, nieznany zagraniczny haker na krótko wyłączył komputery regulujące przepływ statków, ciężarówek i towarów w porcie, co doprowadziło do masowych zatorów na drogach wodnych i drogach lądowych prowadzących do terminala. Obiekt portowy Shahid Rajaee jest jednym z dwóch głównych terminali żeglugowych w irańskim mieście Bandar Abbas, położonym na wybrzeżu Cieśniny Ormuz[13].

---

[11] A. Greenberg, *A Guide to LockerGoga, the Ransomware Crippling Industrial Firms*, https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/, dostępny 28.10.2020 r.

[12] L. Tomter, M. Gundersen, *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*, https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043, dostępny 28.10.2020 r.

[13] J. Warrick, E. Nakashima, *Officials: Israel linked to a disruptive cyberattack on Iranian port facility*, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html, dostępny 28.10.2020 r.

Atak na komputery portu został potwierdzony dzień później przez Mohammada Rastada, dyrektora zarządzającego PMO (ang. *Ports and Maritime Organisation*), który stwierdził: „Niedawny cyberatak nie zdołał przeniknąć do systemów PMO i był w stanie zinfiltrować i uszkodzić tylko pewną liczbę prywatnych systemów operacyjnych w portach".

Istnieją spekulacje, że atak na Shahid Rajaee był odwetem ze strony Izraela, po wcześniejszych, również oficjalnie niepotwierdzonych, atakach Iranu na wybrane obiekty izraelskiej infrastruktury technicznej zapewniającej zaopatrzenie w wodę i miał na celu wysłanie do Iranu ostrzeżenia, bez powodowania jakichkolwiek ofiar. I chociaż brakuje szczegółowych informacji na temat rzeczywistej realizacji cyberataku na terminal portowy Shahid Rajaee, jest więcej niż prawdopodobne, że system operacyjny terminala (TOS), który kontroluje i zarządza całym portem, był celem ataku, do którego wykorzystano systemy różnych firm podłączonych do niego za pomocą określonych interfejsów. Domniemanie to, potwierdza uszkodzenie podczas ataku tylko kilku prywatnych systemów operacyjnych.

NORMY, REGULACJE, STANDARDY W ZAKRESIE CYBERBEZPIECZEŃSTWA MORSKIEGO

Niezawodna i bezpieczna łączność oraz zależność od Internetu to obecnie czynniki bezpośrednio wpływające, a w zasadzie warunkujące obsługę i zarządzanie statkami morskimi, szczególnie statkami autonomicznymi. Dostrzegając ich stale rosnące znaczenie, przemysł morski uznaje potrzebę regulacji i nadzoru w zakresie cyberbezpieczeństwa. Głównym celem tych działań jest potrzeba zapewnienia skutecznego zarządzania i łagodzenia ewoluujących zagrożeń cybernetycznych. W grupie norm i różnego rodzaju regulacji, które podejmują problematykę cyberbezpieczeństwa morskiego, można wymienić rezolucję IMO MSC. 428 (98), ISA/IEC 62443, ISO/IEC 27001 oraz TMSA. Przy czym należy wyraźnie podkreślić, że istnieje wiele innych standardów branżowych i regulacji, obowiązujących w określonych krajach.

Rezolucja IMO MSC. 428 (98)

Aby stawić czoła rosnącym obawom związanym z cyberzagrożeniami, Międzynarodowa Organizacja Morska (IMO) ustaliła jako ostateczny termin 1 stycznia 2021 r., w którym to morskie ryzyko cybernetyczne powinno zostać uwzględnione w systemach zarządzania bezpieczeństwem statków (zgodnie z definicją w Kodeksie ISM). Głównym celem tych działań jest wprowadzenie środków ochrony zarówno systemów OT, jak i IT. IMO zidentyfikowała także

(w 2017 roku) szereg kluczowych obszarów ryzyka cybernetycznego w sektorze morskim. Obejmują one między innymi[14]:

- systemy mostkowe,
- systemy przeładunku i zarządzania ładunkami,
- układy napędowe i zarządzania maszynami oraz sterowania mocą,
- systemy kontroli dostępu,
- systemy obsługi i zarządzania pasażerami,
- sieci publiczne dostępne dla pasażerów,
- systemy łączności,
- systemy administracyjne i systemy socjalne dla załogi.

W rezolucji stwierdzono także że, zapewnienie skutecznego zarządzania ryzykiem cybernetycznym musi opierać się na podejściu polegającym na ocenie i porównaniu aktualnego i pożądanego stanu w zakresie zarządzania tym ryzykiem. Może to ujawnić określone luki, które dzięki ich identyfikacji można wyeliminować i osiągnąć tym sposobem postawione cele zarządzania ryzykiem. Także skuteczny plan zarządzania ryzykiem cybernetycznym może pozwolić wykorzystać zasoby określonego podmiotu w najbardziej efektywny sposób[15].

Normy ISA/IEC 62443

Seria norm ISA/IEC 62443 została opracowana wspólnie przez Międzynarodowy Komitet ISA99 i Komitet Techniczny (TC 65) Międzynarodowej Komisji Elektrotechnicznej i dostosowana do potrzeb projektowania niezawodności i odporności z punktu widzenia cyberbezpieczeństwa w systemach sterowania automatyki przemysłowej (IACS)[16].

Seria tych norm i zaleceń podzielona jest na cztery zasadnicze grupy, są to[17]:

1. Ogólna – zawierająca dokumenty dotyczące tematów wspólnych dla całej serii;
2. Warunki i procedury – dokumenty w tej grupie koncentrują się na politykach i procedurach związanych z bezpieczeństwem systemów sterowania automatyki przemysłowej;
3. Wymagania systemowe – dokumenty z trzeciej grupy dotyczą wymagań na poziomie całego systemu;

[14] IMO, *Guidelines on maritime cyber risk management,* MSC-FAL.1/Circ.3, 5 July 2017, Aneks, s. 1.
[15] https://safety4sea.com/guidelines-on-maritime-cyber-risk-management/, dostępny 02.11.2020 r.
[16] https://www.iec.ch/cybersecurity/?ref=extfooter, dostępny 02.11.2020 r.
[17] A. D'mello, *IEC 62443: How to achieve the highest levels of industrial security*, https://www.iotglobalnetwork.com/iotdir/2020/04/16/iec-62443-how-to-achieve-the-highest-levels-of-industrial-security-24420/, dostępny 02.11.2020 r.

4. Wymagania dotyczące poszczególnych podsystemów – ostatnia grupa zawiera dokumenty, które dostarczają informacji o bardziej specyficznych i szczegółowych wymaganiach związanych z rozwojem produktów sterowania automatyką przemysłową.

Normy ISO/IEC 27001

ISO 27001 to neutralny technologicznie, niezależny od producenta standard (zbiór wymagań) zarządzania bezpieczeństwem informacji, który zawiera opis cech skutecznego systemu zarządzania bezpieczeństwem informacji (ang. *Information Security Management System* – ISMS). Obowiązkowe wymagania dla ISO 27001 są zdefiniowane w rozdziałach od 4 do 10, a wyłączenie któregokolwiek z nich jest nieakceptowalne, jeżeli organizacja chce otrzymać certyfikację lub przejść audyt i deklarować zgodność z przedmiotową normą[18]. Poniżej przedstawiono charakterystykę poszczególnych rozdziałów[19]:

- Rozdział 4. Kontekst Organizacji – określa wymagania niezbędne dla zrozumienia zagadnień zewnętrznych i wewnętrznych, zainteresowanych stron i ich wymagań oraz definiuje zakres Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- Rozdział 5. Przywództwo – określa obowiązki kierownictwa organizacji, ustalając role i zakres odpowiedzialności oraz treść polityki bezpieczeństwa informacji na najwyższym poziomie,
- Rozdział 6. Planowanie – określa wymagania dotyczące oceny ryzyka, zarządzania ryzykiem, zakresu zastosowania, planu zarządzania ryzykiem i ustalania celów bezpieczeństwa informacji,
- Rozdział 7. Wsparcie – określa wymagania dotyczące dostępności zasobów, kompetencji, świadomości, komunikacji i kontroli dokumentów i zapisów,
- Rozdział 8. Działania operacyjne – określa sposób wdrażania oceny i zarządzania ryzykiem, a także kontroli i innych procesów niezbędnych do osiągnięcia określonych celów zapewnienia bezpieczeństwa informacji,
- Rozdział 9. Ocena wyników – określa wymagania dotyczące monitorowania, dokonywania pomiarów, analizy, oceny, audytu wewnętrznego i przeglądów,
- Rozdział 10. Doskonalenie - definiuje wymagania dotyczące niezgodności, działań korygujących i ciągłego doskonalenia.

[18] https://sklep.pkn.pl/pn-en-iso-iec-27001-2017-06p.html, dostępny 02.11.2020 r.

[19] J. Staśkiewicz, *System Zarządzania Bezpieczeństwem Informacji wg ISO 27001*, https://opensecurity.pl/bezpieczenstwo-informacji-wg-iso-27001/, dostępny 02.11.2020 r.

T M S A

W 2004 roku Oil Companies International Marine Forum (OCIMF) wprowadziła *Program zarządzania tankowcami i samooceny* (ang. *the Tanker Management and Self Assessment* – TMSA), aby pomóc operatorom statków oceniać, mierzyć i ulepszać ich systemy zarządzania bezpieczeństwem. Stanowi on uzupełnienie branżowych norm i standardów i ma na celu zachęcanie do tworzenia własnych regulacji zapewniających bezpieczeństwo i promowanie ciągłego doskonalenia w tym zakresie wśród operatorów tankowców[20].

Ramy TMSA oparte są na 13 elementach praktyki zarządzania. Każdy element zawiera jasny cel i zestaw wspierających wskaźników KPI. Żeby uzyskać możliwie dokładną i obiektywną ocenę należy dokonać analizy wszystkich 13 elementów. Ocena pozwala przeprowadzić analizę luk w celu określenia, które elementy i etapy nie zostały jeszcze osiągnięte oraz jak najlepiej opracować program poprawy wydajności. W grupie tych 13 elementów znajdują się następujące[21]:

- zarządzanie, przywództwo i odpowiedzialność,
- rekrutacja i zarządzanie personelem lądowym,
- rekrutacja i zarządzanie załogami statków,
- bezpieczeństwo nawigacyjne,
- niezawodność, standardy obsługi i konserwacji,
- operacje ładunkowe, balastowe i cumownicze, czyszczenie zbiorników,
- zarządzanie zmianami,
- analiza incydentów, dochodzenie i ich zgłaszanie,
- zarządzanie bezpieczeństwem,
- zarządzanie środowiskiem i energią,
- gotowość na sytuacje kryzysowe i planowanie awaryjne,
- pomiar, analiza i doskonalenie,
- bezpieczeństwo morskie.

CELE I SEKWENCJA CYBERATAKU

Należy sobie zdawać sprawę, że podmioty dokonujące cyberataków nie mają ani tych samych motywów, ani tych samych zasobów podczas atakowania systemów statkowych. Potencjalnych sprawców ataków oraz ich cele przedstawiono w Tabeli 1.

[20] https://www.ocimf.org/sire/about-tmsa/, dostępny 03.11.2020 r.
[21] https://www.sertica.com/tmsa/#gref, dostępny 03.11.2020 r.

Tabela 1. Cele cyberataków

Lp.	Grupa	Cel ataku
1	Zwykli hakerzy	Rozpowszechnianie złośliwego oprogramowania w sieci internetowej w celu uzyskania okupu
2	Hakerzy amatorzy	Doskonalenie i szkolenie umiejętności hakerskich
3	Etyczni hakerzy	Znajdowanie luk w systemie w celu jego usprawnienia
4	Niezadowoleni byli pracownicy	Zemsta na armatorze
5	Niezadowoleni dostawcy zewnętrzni	Kradzież danych dotyczących urządzeń i ich stanu
6	Aktywiści	Opóźnienie lub anulowanie wprowadzenia statków autonomicznych lub innych rodzajów statków
7	Hakerzy – przestępcy kryminalni	Kradzież statku, jego ładunku, komponentów lub oczekiwanie okupu
8	Konkurenci	Kradzież cennych danych lub sabotowanie i uszkodzenie statku
9	Terroryści	Uszkodzenie statku i/lub spowodowanie ofiar śmiertelnych
10	Przestępcy kryminalni	Przekazywanie nielegalnego ładunku lub osób
11	Państwo	Uszkodzenie statku lub przejęcie kontroli. Tworzenie stref bez dostępu/zerowych GPS

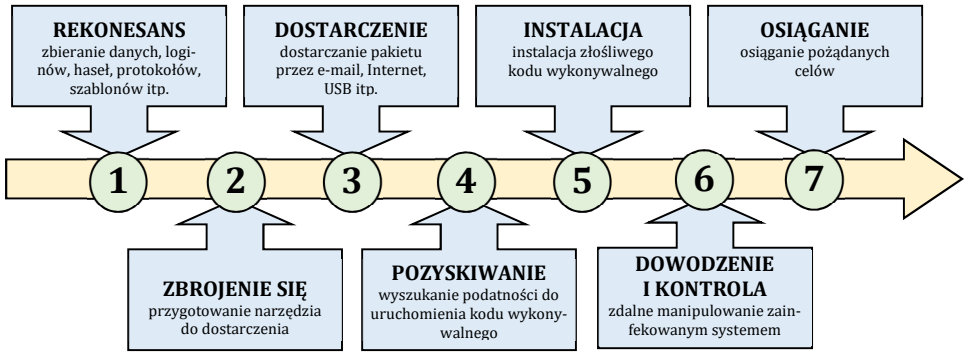
źródło: V. Bolbota, G. Theotokatosa, E. Boulougourisa, D. Vassalosa, A novel cyber-risk assessment method for ship systems, „Safety Science" Nr 131 (2020) 104908, s. 4.

Z kolei w typowej sekwencji cyberataku, haker prawdopodobnie spróbuje zinfiltrować sieć OT statku za pomocą różnych metod. Będzie szukać wrażliwych punktów wejścia wykorzystując terminale łączności satelitarnej, otwarte lub niezabezpieczone sieci Wi-Fi, punkty końcowe w sieci IT i w systemach statkowych. Niektóre typowe kierunki ataków obejmują spear phishing, niewłaściwie skonfigurowane punkty końcowe oraz skradzione poświadczenia. Jeśli haker jest na pokładzie, może infiltrować systemy bezpośrednio za pomocą zainfekowanych pendrive'ów USB.

Po włamaniu się do określonych systemów hakerzy ukrywają się za pomocą różnych metod i ostatecznie przejmują kontrolę nad krytycznymi systemami i urządzeniami sterującymi. W tym momencie są w stanie ingerować

w systemy nawigacyjne i komunikacyjne, otwierać lub zamykać krytyczne zawory oraz przejmować sterowanie statkiem, czego konsekwencje mogą być katastrofalne.

Najczęściej spotykaną sekwencję cyberataku przedstawiono na Rysunku 1.



Rys. 1. Sekwencja typowego cyberataku

źródło: Opracowanie własne na podstawie: Mission Secure, Maritime Security Challenges: The Physical Impact of Maritime Cyber Threats, https://www.missionsecure.com/blog/the-physical-impact-of-maritime-cyberthreats, dostępny 11.11.2020 r.

PRZECIWDZIAŁANIE

Sposoby i metody zapewnienia bezpieczeństwa cybernetycznego jednostkom autonomicznym zasadniczo nie będą się różniły od jednostek konwencjonalnych. Należy pamiętać, że zanim jednostki te osiągną pełną autonomię minie jeszcze trochę czasu, więc pewne charakterystyczne elementy dla obecnych statków będą również towarzyszyć statkom autonomicznym, chociażby będzie to ograniczona załoga. Z określonych powodów zapewnienie bezpieczeństwa cybernetycznego jednostkom autonomicznym będzie nawet łatwiejsze. Już w początkowym okresie eksploatacji będą one wyposażone w najnowsze technologie, oprogramowanie i urządzenia, które z założenia będą zapewniały pożądany poziom bezpieczeństwa cybernetycznego. Producenci będą mogli korzystać z obecnych doświadczeń i już funkcjonujących systemów zarządzania ryzykiem cybernetycznym.

Obecnie obowiązujące przepisy i regulacje w zakresie morskiego bezpieczeństwa cybernetycznego nie dokonują podziału jednostek pływających wg kryterium poziomu autonomiczności, stąd można postawić tezę, że określone w nich wymagania dotyczą także statków autonomicznych. Przy czym pewne

wymagania w zakresie zapewniania cyberbezpieczeństwa jednostkom autonomicznym, można odnaleźć także w wytycznych, rekomendacjach i innych dokumentach dotyczących tylko tego typu jednostek.

Korzystanie z technologii informacyjno-komunikacyjnych umożliwia nieautoryzowane lub złośliwe działania wobec statków autonomicznych. Do grupy potencjalnych zagrożeń, które mogą wywołać lub wpłynąć na cyberbezpieczeństwo statków autonomicznych, można zaliczyć niżej wymienione[22]:

- urządzenia wykorzystujące porty USB (np. pendrive) można podłączyć do dowolnego systemu na statku pracującego w sieci, zarówno na etapie budowy jak i w czasie prac konserwacyjnych,
- przejęcie kontroli nad statkiem poprzez łącze komunikacyjne,
- zagłuszanie sygnału kierowanego do urządzeń pozycjonujących na pokładzie lub do urządzeń nawigacyjnych statku, np. GPS,
- blokowanie lub wykorzystanie sygnału między brzegowym centrum kontroli a statkiem,
- fałszowanie sygnału GPS odbieranego przez odbiornik na pokładzie.

Można spodziewać się, że atakujący będą celować w systemy, które muszą być często aktualizowane, np. przy użyciu portów USB, nośników CD/DVD i Internetu lub łączy satelitarnych, takie jak AIS, NAVTEX, ECDIS. Chociaż w przypadku statków autonomicznych dostęp poprzez USB lub nośniki CD/DVD będzie raczej niemożliwy, szybciej wykorzystywane będą do tego bezprzewodowe systemy łączności. Na przykład dostęp do łączności internetowej będzie możliwy poprzez łącze do brzegowego centrum kontroli, tym samym atakujący będzie musiał najpierw włamać się do tego centrum, aby uzyskać dostęp do statku.

Paradoksalnie, w porównaniu do statków konwencjonalnych, dostęp do statku tylko i wyłącznie przez Internet z punktu widzenia cyberbezpieczeństwa należy ocenić jak najbardziej pozytywnie, sieć pokładowa w tym przypadku jest bramą do Internetu.

Należy także zwrócić uwagę na to, że często na statkach konwencjonalnych stosuje się przestarzałe systemy, które były lub są używane od chwili wprowadzenia statku do eksploatacji. Zdarza się, że producenci tego oprogramowania przestali aktualizować te systemy. W przypadku statku autonomicznego system operacyjny będzie aktualizowany na bieżąco, co zapewnia stałe połączenie z brzegowym centrum nadzoru. Odbywać się to będzie w sposób synchroniczny, jednocześnie aktualizowane będą systemy w centrach nadzoru i na pokładach jednostek autonomicznych.

[22] K. Said. M. Agamy, *The impact of cybersecurity on the future of Autonomous ships*, International Journal of Recent Research in Interdisciplinary Sciences (IJRRIS), Vol. 6, Issue 2, Month: April - June 2019, s. 12.

Najważniejszym czynnikiem zapewniającym cyberbezpieczeństwo jest czynnik ludzki. Wbrew pozorom najskuteczniejszym sposobem przeciwdziałania cyberatakowi jest dobrze wyszkolony i świadomy członek załogi, a w przypadku statku autonomicznego członek zespołu brzegowego centrum nadzoru. Niezadowolony lub szantażowany członek załogi lub centrum nadzoru, mając łatwy dostęp do systemu statku, jest w stanie wyrządzić wiele szkód, nieważne czy dokona tego samodzielnie czy ułatwi dostęp stronie trzeciej. Stąd też właściwe szkolenie członków załogi i sprawdzanie ich pod kątem dawania rękojmi zachowania tajemnicy może być pierwszym krokiem do zabezpieczenia statku przed cyberatakiem, obejmującym świadomość cybernetyczną.

Ochrona systemów statkowych, szczególnie środowiska OT nie jest łatwym zadaniem, ale dzięki zastosowaniu odpowiednich środków bezpieczeństwa i procedur operatorzy i armatorzy jednostek autonomicznych są w stanie zachować integralność i ciągłość operacji.

Najogólniej rzecz ujmując, skuteczne zarządzanie ryzykiem cybernetycznym można scharakteryzować w następujący sposób:

- poza ochroną, należy skupić się na planach reagowania, które powinny być często testowane i aktualizowane, pozwalając w ten sposób identyfikować wszelkie niedociągnięcia, doskonalić procesy i określać nowe działania usprawniające,
- opracowania wymaga strategia ochrony i odzyskiwania danych. Plan ochrony i odzyskiwania danych stworzy możliwość funkcjonowania w przypadku odłączenia od sieci,
- powinno zapewnić się segmentowanie sieci, które pozwala ograniczyć rozprzestrzenianie się cyberataku na krytyczne systemy statków,
- nieodłącznym elementem jest opracowanie i posiadanie planu awaryjnego pozwalającego utrzymać ciągłość prowadzenia operacji po cyberataku,
- istotne jest także dzielenie się informacjami w zakresie cyberataków z innymi podmiotami z branży morskiej, co stwarza możliwość lepszego przygotowania się na przyszłe zagrożenia,
- ochrona posiadanych systemów morskich wymaga budowy stałej świadomości zagrożeń, edukacji oraz ciągłego monitorowania ram cyberbezpieczeństwa.

W literaturze przedmiotu można znaleźć zalecenia zarówno w zakresie budowy systemów zarządzania bezpieczeństwem cybernetycznym w sektorze morskim, jak i propozycje metod oceny cyberryzyka. Najistotniejsze z nich, zdaniem autora, przedstawiono w dalszej części referatu.

Cyberochrona wg Bureau Veritas

System ochrony cybernetycznej według francuskiego towarzystwa klasyfikacyjnego z siedzibą centrali w Paryżu, powinien być zorganizowany w sposób zapewniający spełnienie następujących funkcji[23]:

a) identyfikacja,
b) ochrona,
c) wykrywanie,
d) odpowiedź,
e) przywrócenie stanu pierwotnego.

W ramach pierwszej funkcji należy zdefiniować role i obowiązki personelu w zakresie zarządzania ryzykiem cybernetycznym oraz zidentyfikować systemy, aktywa i dane wrażliwe na różnego rodzaju zakłócenia, mogące stwarzać ryzyko dla operacji statkowych.

Należy także stworzyć dokładną mapę systemów IT, która powinna opisywać architekturę sieci i zawierać listę urządzeń (identyfikowanych przez numer modelu) i oprogramowania (identyfikowanych przez numer wersji) oraz być regularnie aktualizowana. Dodatkowo sporządzony powinien być spis wszystkich kont użytkowników odzwierciedlający faktyczny poziom uprawnień nadanych każdemu użytkownikowi.

Druga funkcja wiąże się z szeroko rozumianą ochroną. Wymaga wdrożenia środków kontroli ryzyka oraz planowania awaryjnego w celu ochrony przed cyberzagrożeniem oraz zapewnienia ciągłości operacji żeglugowych. Inne zalecenia dotyczą[24]:

- zarządzania dostępem użytkowników, co powinno opierać się na bezpiecznym protokole uwierzytelniania, wykorzystującym najlepsze praktyki, takie jak unikanie ogólnych lub anonimowych kont czy regularną zmianę haseł o wymaganym wysokim poziomie złożoności,
- stworzenia i przestrzegania procedur dotyczących przyjazdu i wyjazdu użytkowników (dostęp do brzegowego centrum nadzoru lub poufnej dokumentacji),
- aktualizacji oprogramowania, które należy przeprowadzać regularnie i zgodnie z zasadami. Polityka ta powinna obejmować:
  - listę komponentów (maszyny i oprogramowania) do aktualizacji,
  - obowiązki różnych podmiotów w procesie aktualizacji,
  - środki użyte do uzyskania i oceny aktualizacji,
  - weryfikację aktualizacji przed instalacją,

[23] Bureau Veritas, *Guidelines for Autonomous Shipping*, Guidance Note NI 641 DT R00 E, Paris 2017, s. 24-25.
[24] Bureau Veritas, *Guidelines for Autonomous Shipping*, Guidance Note NI 641 DT R00 E, Paris 2017, s. 25.

- procedurę przywracania poprzedniej konfiguracji w przypadku niepowodzenia aktualizacji.

Automatyczne pobieranie i instalowanie aktualizacji może odbywać się tylko i wyłącznie z zaufanych źródeł (najlepiej od oryginalnego dostawcy oprogramowania).

– zabezpieczenia sieci, zwłaszcza sieci bezprzewodowych, które powinny być chroniona za pomocą bezpiecznych protokołów. Połączenie internetowe powinno być zabezpieczone bramą umożliwiającą oddzielenie dostępu do Internetu od sieci wewnętrznej.

Trzecia funkcja ma na celu opracowanie i wdrożenie działań niezbędnych do szybkiego wykrycia zdarzenia cybernetycznego. W tym celu należy wdrożyć stałe monitorowanie pozwalające wykryć nietypowe zdarzenia lub włamania, np. masowe transfery danych (w zależności od zwykłych trybów pracy) czy kilka błędnych logowań na aktywne lub nieaktywna konta.

Z kolei funkcja odpowiedzi obejmuje przygotowanie i wprowadzenie planów zapewniających odporność i możliwość przywrócenia sprawności systemów niezbędnych do prowadzenia działalności lub świadczenia usług żeglugowych, które zostały zakłócone w wyniku cyberataku.

Ostatnia funkcja, pozwalająca na sprawny i szybki powrót do stanu sprzed ataku, łączy się z koniecznością posiadania określonych środków tworzenia kopii zapasowych i przywracania systemów cybernetycznych niezbędnych do prowadzenia operacji żeglugowych, które zostały zakłócone. Na wypadek takiego zdarzenia należy określić plan pracy awaryjnej o obniżonych, względem normalnych, parametrach. Pierwszym krokiem powinno być odizolowanie wszystkich zainfekowanych maszyn i urządzeń od sieci. W przypadku każdego incydentu informacja o nim powinna być raportowana, co w założeniu powinno zapewnić bardziej skuteczne radzenie sobie z podobnym zdarzeniem w przyszłości.

System zarządzania cyberryzykiem wg BIMCO i partnerów

Bałtycka i Międzynarodowa Rada Żeglugowa (BIMCO) wraz z wieloma partnerami opracowała *Wytyczne dotyczące bezpieczeństwa cybernetycznego na statkach*, które zawierają procedury i działania mające na celu zapewnienie i utrzymanie bezpieczeństwa systemów cybernetycznych w samej organizacji oraz na pokładach statków.

Opracowanie, wdrożenie i utrzymanie programu zarządzania bezpieczeństwem cybernetycznym zgodnie z podejściem przedstawionym na rysunku nr 2 to dosyć pracochłonne i skomplikowane przedsięwzięcie. Z tego też względu ważne jest, aby kierownictwo wyższego szczebla pozostawało zaangażowane w całym procesie. Zapewnia to równowagę kwestii ochrony, planów awaryjnych

i planów reagowania w odniesieniu do podatności na zagrożenia, narażenia na ryzyko i skutków potencjalnego incydentu cybernetycznego. Należy także pamiętać, że niektóre aspekty zarządzania ryzykiem cybernetycznym mogą obejmować wrażliwe lub poufne informacje handlowe. Firmy powinny zatem rozważyć odpowiednią ochronę tych informacji i o ile to możliwe, nie umieszczać ich w swoim systemie zarządzania bezpieczeństwem.

Rys. 2. Zarządzanie ryzykiem cybernetycznym wg BIMCO, CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, IUMI, OCIMF i WSC

źródło: BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, The Guidelines on Cyber Security Onboard Ships, ver. 3, 2017, s. 4.

Pierwszym etapem, praktycznie powtarzającym się dla wszystkich systemów cyberochrony czy systemów zarządzania ryzykiem cybernetycznym, jest identyfikacja zagrożeń. Jest to istotny element, gdyż ryzyko cybernetyczne jest specyficzne dla konkretnej firmy, statku czy operacji. Oceniając ryzyko, organizacje powinny wziąć pod uwagę wszelkie szczególne aspekty swojej działalności, które mogą zwiększyć ich podatność na incydenty cybernetyczne.

W *Wytycznych...* zwraca się także uwagę na czynnik ludzki, jako powtarzalny i główny element, stanowiący w pewnym sensie luki w cyberprzestrzeni. Może to być niezamierzone i spowodowane błędem ludzkim podczas obsługi i zarządzania systemami IT i OT lub nieprzestrzeganiem ustalonych procedur.

Istnieje jednak także możliwość, że działania te mogą być złośliwe i są celową próbą zniszczenia firmy i statku przez niezadowolonego pracownika.

Kolejną istotą kwestię stanowi identyfikacja słabych punktów. Zaleca się, aby firma przeprowadziła ocenę potencjalnych zagrożeń, które mogą wystąpić. Po tym powinna nastąpić ocena systemów i procedur pokładowych w celu określenia ich odporności na bieżący poziom zagrożeń. Rezultatem powinna być strategia skupiona wokół kluczowych ryzyk. Oczywiście systemy samodzielne/odizolowane będą mniej podatne na zewnętrzne cyberataki w porównaniu z systemami podłączonymi do niekontrolowanych sieci lub bezpośrednio do Internetu. Dlatego też należy zadbać o świadomość zagrożeń w tym drugim przypadku. Systemy te składają się z potencjalnie podatnego na uszkodzenia sprzętu, który także należy poddać przeglądowi podczas oceny.

Nowoczesne technologie mogą zwiększyć podatność statków, zwłaszcza jeśli istnieją niezabezpieczone sieci i niekontrolowany dostęp do Internetu. Ponadto personel na lądzie i na pokładzie może nie wiedzieć, w jaki sposób niektórzy producenci sprzętu utrzymują zdalny dostęp do wyposażenia pokładowego i jego systemu sieciowego. Dostęp ten powinien również być brany pod uwagę jako ważna część oceny ryzyka.

Jeżeli chodzi o ocenę ryzyka cybernetycznego to powinna rozpocząć się ona na wyższym szczeblu zarządzania w przedsiębiorstwie, a nie od razu być przekazywana do realizacji oficerowi ochrony statku lub szefowi działu IT.

Jako podstawa do oceny ryzyka (głównie do zagrożeń cybernetycznych na pokładzie statków) mogą służyć poniższe pytania[25]:

- Jakie aktywa są zagrożone?
- Jaki jest potencjalny wpływ incydentu cybernetycznego?
- Kto ponosi ostateczną odpowiedzialność za zarządzanie ryzykiem cybernetycznym?
- Czy systemy OT i ich środowisko pracy są chronione przed zagrożeniami płynącymi z Internetu?
- Czy istnieje zdalny dostęp do systemów OT, a jeśli tak, to w jaki sposób jest monitorowany i chroniony?
- Czy systemy informatyczne są chronione i czy zdalny dostęp jest monitorowany i zarządzany?
- Jakie najlepsze praktyki zarządzania ryzykiem cybernetycznym są stosowane?
- Jaki jest poziom wyszkolenia personelu obsługującego systemy IT i OT?

[25] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, *The Guidelines on Cyber Security Onboard Ships*, ver. 3., 2017, s. 16.

Natomiast przy ocenie wpływu poszczególnych zagrożeń cybernetycznych można wykorzystać model poufności, integralności i dostępności (CIA) opierający się na trzech poniższych elementach[26]:

- nieuprawniony dostęp i ujawnienie informacji lub danych o statku, załodze, ładunku i pasażerach,
- utrata integralności, która doprowadziłaby do transformacji lub utraty danych wpływających na bezpieczną i efektywną eksploatację i administrację statkiem,
- utrata dostępności z powodu usunięcia informacji i danych i/lub zakłócenie usług lub funkcjonowania systemów statków.

Potencjalne skutki mogą być związane z bezpieczeństwem, operacją, środowiskiem, finansami, reputacją itp. Obecnie istnieje kilka metodologii oceny ryzyka, zawierających określone kryteria i techniki, które mogą pomóc w określeniu skali wpływu cyberataku, w tabeli nr 2 przedstawiono jedną z nich.

Tabela 2. Poziomy w modelu CIA

Potencjalny wpływ	**Charakterystyka**	**Skutki w praktyce**
niski	Można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała ograniczony negatywny wpływ na firmę i statek, aktywa organizacji lub osoby	Naruszenie ochrony może: (1) spowodować pogorszenie funkcjonowania statku, kiedy organizacja jest w stanie wykonywać swoje podstawowe funkcje, ale skuteczność tych funkcji jest zauważalnie ograniczona; (2) spowodować niewielkie szkody w majątku organizacji; (3) spowodować niewielkie straty finansowe; lub (4) spowodować niewielkie obrażenia osób fizycznych.
umiarkowany	Można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała istotny negatywny wpływ na przedsiębiorstwo i statek, aktywa lub osoby	Naruszenie ochrony może: (1) spowodować znaczące pogorszenie funkcjonowania statku, kiedy organizacja jest w stanie wykonywać swoje podstawowe funkcje, ale skuteczność tych funkcji jest znacznie ograniczona; (2) spowodować znaczne szkody w majątku organizacyjnym; (3) spowodować znaczną stratę finansową; lub (4) spowodować znaczną szkodę dla osób,

[26] Federal Information Processing Standards, *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, s. 2.

		która nie wiąże się z utratą życia ani poważnymi obrażeniami zagrażającymi życiu.
wysoki	Można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała poważny lub katastrofalny negatywny wpływ na działalność przedsiębiorstwa i statku, aktywa, środowisko lub osoby	Naruszenie ochrony może: (1) spowodować poważne pogorszenie lub brak możliwości eksploatacji statku, kiedy organizacja nie jest w stanie wykonywać jednej lub więcej swoich podstawowych funkcji; (2) spowodować poważne szkody w środowisku i/lub majątku organizacyjnym; (3) spowodować poważne straty finansowe; lub (4) spowodować poważne lub katastrofalne szkody dla osób, które mogą skutkować utratą życia lub poważnymi obrażeniami zagrażającymi życiu.

źródło: Federal Information Processing Standards, Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, s. 6.

Kolejnym etapem jest ustanowienie środków ochrony i wykrywania. Efektem oceny ryzyka przedsiębiorstwa i późniejszej strategii cyberbezpieczeństwa powinno być zmniejszenie ryzyka, na tyle, na ile jest to wykonalne. Na poziomie technicznym obejmowałoby to podjęcie niezbędnych działań w celu ustanowienia i utrzymania uzgodnionego poziomu cyberbezpieczeństwa. Niezwykle ważne jest to, aby określić sposoby zarządzania cyberbezpieczeństwem na pokładzie i przekazać obowiązki kapitanowi i określonym członkom załogi.

Środki ochrony przed zagrożeniami cybernetycznymi mogą mieć charakter techniczny lub proceduralny, z kontrolami technicznymi wdrażanymi w celu egzekwowania kontroli proceduralnych lub charakteryzować się podejściem kombinowanym z zastosowaniem odpowiednich środków zapewniających najbardziej skuteczny poziom ochrony.

Typowo techniczny charakter ma centrum bezpieczeństwa internetowego (CIS, ang. *Centre for Internet Security*), zawierające wskazówki dotyczące środków, które można zastosować w celu wyeliminowania luk w zabezpieczeniach cybernetycznych. Przedsięwzięcia zabezpieczające znajdują się na liście krytycznych środków kontroli bezpieczeństwa (CSC, ang. C*ritical Security Controls*), które są uszeregowane pod względem ważności i sprawdzane, czy zapewniają właściwą ocenę i doskonalenie firmowych zabezpieczeń. CSC obejmują

aspekty techniczne i proceduralne[27]. Poniższe przykłady CSC zostały wybrane jako szczególnie istotne dla jednostek pływających[28]:

- ograniczenie i kontrola portów sieciowych, protokołów i usług,
- konfiguracja urządzeń sieciowych, takich jak zapory, routery i przełączniki,
- bezpieczeństwo fizyczne,
- wykrywanie, blokowanie i alerty,
- łączność satelitarna i radiowa,
- bezprzewodowa kontrola dostępu,
- wykrywanie złośliwego oprogramowania,
- bezpieczna konfiguracja sprzętu i oprogramowania,
- ochrona poczty i przeglądarki internetowej,
- możliwość odzyskiwania danych,
- bezpieczeństwo aplikacji (zarządzanie poprawkami).

Z kolei kontrole proceduralne koncentrują się na tym, w jaki sposób członkowie załogi korzystają z systemów pokładowych. Plany i procedury, które zawierają wrażliwe informacje, powinny być traktowane jako poufne i obsługiwane zgodnie z polityką firmy. Przykładami działań proceduralnych mogą być następujące[29]:

- szkolenie i świadomość,
- dostęp dla zwiedzających,
- aktualizacje i konserwacja oprogramowania,
- aktualizacje narzędzi antywirusowych i anty-malware,
- zdalny dostęp,
- korzystanie z uprawnień administratora,
- korzystanie z nośników danych,
- utylizacja sprzętu, w tym usuwanie danych,
- uzyskanie wsparcia z lądu i z planów awaryjnych.

Następnym etapem zarządzania ryzykiem jest ustalenie planów awaryjnych. Z punktu widzenia cyberbezpieczeństwa jednostki pływającej ważne jest, aby zrozumieć istotę każdego incydentu cybernetycznego i odpowiednio ustalić priorytety reagowania. Każdy cyberatak należy ocenić w kontekście jego wpływu na operacje, aktywa itp.

W większości przypadków, z wyjątkiem nielicznych systemów np. systemów planowania i zarządzania ładunkiem, utrata systemów IT na pokładzie,

[27] CIS, *Critical Security Controls for Effective Cyber Security*, www.cisecurity.org/critical-controls.cfm, dostępny 18.11.2020 r.
[28] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, *The Guidelines on Cyber Security Onboard Ships*, ver. 3., 2017, s. 25-28.
[29] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, *The Guidelines on Cyber Security Onboard Ships*, ver. 3., 2017, s. 29-33.

w tym naruszenie danych poufnych, będzie stanowiło problem z ciągłością działania z biznesowego punktu widzenia, natomiast nie powinno mieć negatywnego wpływu na bezpieczeństwo eksploatacji statku. Inaczej wygląda kwestia utraty systemów OT, w tym przypadku może to mieć istotny i natychmiastowy wpływ na bezpieczną eksploatację statku. Gdyby incydent cybernetyczny spowodował utratę lub nieprawidłowe działanie systemów OT, konieczne byłoby podjęcie skutecznych działań w celu zapewnienia natychmiastowego bezpieczeństwa załodze, jednostce, ładunkom i środowisku morskiemu. Dlatego też załogi powinny być regularnie szkolone w zakresie planów reagowania. Działania, określone w tych planach, powinny być regularnie ćwiczone przez załogi statków, kierownictwo i personel wsparcia IT, podobnie jak w przypadku rutynowych ćwiczeń w zakresie reagowania na inne zagrożenia. Zewnętrzni dostawcy systemów pokładowych również powinni być uwzględnieni i zobowiązani do uczestniczenia w tych ćwiczeniach i tworzeniu planów awaryjnych.

Należy także zwrócić uwagę na połączenia między systemami brzegowymi i systemami OT, które mogą być istotne w szerokim zakresie zastosowań, może to być np. monitorowanie wydajności, konserwacja predykcyjna czy zdalne wsparcie. Wspólne dla tych systemów jest to, że nie są one absolutnie niezbędne do bezpiecznej eksploatacji statku. Stanowią jednak potencjalny element ataku, pozwalający uzyskać dostęp do systemów OT. Dlatego ważne jest, aby ocenić, kiedy i w jakich okolicznościach połączenia te są dozwolone. Należy także ustanowić plany określające, kiedy systemy OT powinny być czasowo oddzielone od połączenia z siecią lądową. Przerwanie tej łączności z pewnością może utrudnić atakującemu manipulowanie systemami krytycznymi dla bezpieczeństwa jednostki lub przejęcie bezpośredniej kontroli nad takim systemem, a także pozwolić uniknąć rozprzestrzeniania się złośliwego oprogramowania między poszczególnymi segmentami sieci. Z tego punktu widzenia ważne jest, aby sieć była zaprojektowana w taki sposób, aby można było szybko fizycznie oddzielić jej poszczególne elementy, usuwając np. pojedynczy kabel sieciowy (oznaczony określonym kolorem) lub modyfikować zaporę sieciową.

Ostatni element zaplanowanej polityki zarządzania bezpieczeństwem cybernetycznym zawiera sposoby reakcji na poszczególne incydenty i metody przywrócenia zainfekowanych systemów do stanu sprzed ataku.

Ważne jest, aby zrozumieć, że skutki incydentów cybernetycznych co do zasady nie znikają same. Jeśli na przykład system ECDIS został zainfekowany złośliwym oprogramowaniem, to uruchomienie zapasowego ECDIS może spowodować kolejny incydent cybernetyczny. Dlatego też sposób czyszczenia i przywracania zainfekowanych systemów powinien być wcześniej zaplanowany i przygotowany.

Plany odtwarzania systemów po awarii muszą być integralną częścią każdego planu cyberbezpieczeństwa morskiego. Obejmuje to przechowywanie danych cybernetycznych do celów kryminalistycznych, a także przywracanie

i ochronę systemów, szczególnie systemów OT. Plany te powinny być również regularnie sprawdzane i aktualizowane, zarówno w morzu, jak i na lądzie. Także wszelka wiedza na temat wcześniej zidentyfikowanych incydentów cybernetycznych, powinna zostać wykorzystana do ulepszenia planów reagowania na wszystkich jednostkach danego armatora.

Jeżeli chodzi o reakcję, to jeżeli ma być ona skuteczna, powinna składać się z co najmniej następujących kroków[30]:

1. Ocena wstępna. Aby zapewnić odpowiednią reakcję, zespół reagowania powinien dowiedzieć się o tym:
   - jak doszło do incydentu,
   - które systemy IT i/lub OT zostały dotknięte i w jaki sposób,
   - w jakim zakresie wpływa on na dane handlowe i/lub operacyjne,
   - jakie zagrożenia dla IT i OT są nadal realne.
2. Odzyskanie systemów i danych. Po wstępnej ocenie incydentu cybernetycznego systemy i dane IT i OT powinny zostać wyczyszczone, odzyskane i przywrócone, w miarę możliwości, do stanu operacyjnego.
3. Zbadanie incydentu. Aby zrozumieć przyczyny i konsekwencje incydentu cybernetycznego, firma powinna przeprowadzić dochodzenie, w razie potrzeby zatrudniając zewnętrznego eksperta. Informacje z dochodzenia będą odgrywać znaczącą rolę w zapobieganiu kolejnym atakom.
4. Zapobieganie ponownym incydentom. Biorąc pod uwagę wynik wyżej wymienionego dochodzenia, należy rozważyć podjęcie działań w celu usunięcia wszelkich nieprawidłowości w zakresie technicznych i/lub proceduralnych środków ochrony, zgodnie z procedurami firmy dotyczącymi wdrażania działań naprawczych.

Gdy incydent cybernetyczny jest złożony, na przykład, jeżeli systemy IT i/lub OT nie mogą zostać przywrócone do normalnego działania, może być konieczne zainicjowanie planu naprawczego wraz z pokładowymi planami awaryjnymi.

W takim przypadku zespół reagowania powinien być w stanie udzielić statkowi porad dotyczących:

- tego czy systemy IT lub OT powinny być wyłączone lub nadal funkcjonować w celu ochrony danych,
- tego czy należy przerwać określone połączenia komunikacyjne statku z brzegiem,
- właściwego wykorzystania zaawansowanych narzędzi dostarczonych w preinstalowanym oprogramowaniu zabezpieczającym,
- zakresu, w jakim incydent naruszył systemy IT lub OT, który wychodzi poza możliwości istniejących planów naprawczych.

[30] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, *The Guidelines on Cyber Security Onboard Ships*, ver. 3., 2017, s. 36.

Co ważne plany naprawy powinny być dostępne w wersji papierowej zarówno na pokładzie, jak i na lądzie. Celem tych planów jest wsparcie odtwarzania systemów i danych niezbędnych do przywrócenia IT i OT do stanu operacyjnego. Żeby zapewnić bezpieczeństwo załogi, w planie należy nadać priorytet dla eksploatacji i nawigacji statku. Istotne również jest to, żeby plany te były zrozumiałe dla personelu odpowiedzialnego za cyberbezpieczeństwo. a ich szczegółowość i złożoność zależała od rodzaju statku oraz systemów IT, OT i innych zainstalowanych na pokładzie.

System zarządzania cyberryzykiem wg IMO

W bardzo podobny sposób do ram zarządzania ryzykiem cybernetycznym podchodzi IMO, bazując na ramach określonych przez NIST (ang. *The National Institute of Standards and Technology, U.S. Depart-ment of Commerce*), przy czym podkreśla się, że wpisujące się w te ramy elementy funkcjonalne nie mają charakteru sekwencyjnego. W praktyce wszystkie powinny być współbieżne i stałe, należą do nich[31]:

1. Identyfikacja: zdefiniowanie ról i obowiązków personelu w zakresie zarządzania ryzykiem cybernetycznym oraz zidentyfikowanie systemów, aktywów, danych i zdolności, które w przypadku zakłócenia stwarzają ryzyko operacyjne dla statków.
2. Ochrona: wdrożenie procesów i środków kontroli ryzyka oraz planów awaryjnych w celu ochrony przed zdarzeniem cybernetycznym i zapewnienia ciągłości operacji żeglugowych.
3. Wykrywanie. opracowanie i wdrożenie działań niezbędnych do szybkiego wykrycia zdarzenia cybernetycznego.
4. Reagowanie: opracowanie i wdrożenie działań i planów mających na celu zapewnienie odporności i przywrócenie systemów niezbędnych do operacji lub usług żeglugowych, które zostały zakłócone w wyniku zdarzenia cybernetycznego.
5. Przywracanie: określenie środków tworzenia kopii zapasowych i przywracania systemów cybernetycznych niezbędnych do operacji żeglugowych, na które miało wpływ zdarzenie cybernetyczne.

Budowa systemu zarządzania ryzykiem cybernetycznym według organizacji Mission Secure, który będzie zgodny z wymaganiami wspomnianej wcześniej rezolucji IMO i kodeksu ISM, wymaga wykonania trzech kroków[32].

[31] IMO, *Guidelines on maritime cyber risk management*, MSC-FAL.1/Circ.3, 5 July 2017, Aneks, s. 3 oraz https://www.nist.gov/cyberframework/framework, dostępny 19.11.2020 r.

[32] Mission Secure, *IMO 2021: Three Steps to Ensure IMO/ISM Cybersecurity Compliance*, https://www.missionsecure.com/blog/imo-2021-three-steps-to-ensure-imo-cybersecurity-compliance, dostępny 19.11.2020 r.

Pierwszym z nich jest ocena zagrożeń. Podkreślić należy połączony charakter statkowych systemów OT i IT oraz ich podatność na cyberataki, można tutaj wymienić m.in. systemy sterowania napędem i maszynami, systemy kontroli mocy, systemy łączności, systemy mostkowe; systemy kontroli dostępu; systemy obsługi i zarządzania ładunkiem; sieci publiczne; systemy obsługi i zarządzania pasażerami oraz systemy administracyjne i socjalne dla załogi. Różne informacje i dane są wymieniane między tymi systemami, dlatego też muszą być one oceniane w aspekcie wszelkich potencjalnych zagrożeń cybernetycznych. Każda nagła awaria spowodowana cyberatakiem może powodować określone implikacje dla wszystkich, połączonych ze sobą systemów.

Ocenie odporności na cyberzagrożenia powinny również zostać poddane wszystkie procesy zachodzące na jednostce, bez względu na źródło tych zagrożeń. Nie ma tu znaczenia czy są one wynikiem działań zamierzonych, przypadkowych czy błędów ludzkich. Dlatego też należy wziąć pod uwagę wszelkie niedociągnięcia projektowe, eksploatacyjne, integracyjne lub konserwacyjne, które mogą potencjalnie wpłynąć na bezpieczeństwo i cyberbezpieczeństwo, a także przeanalizować wszelkie potencjalne luki lub niewłaściwe procedury, których przestrzega załoga i strona trzecia, a które wchodzą w interakcje z systemami statku. Kolejny raz zwraca się także uwagę na czynnik ludzki, który jest bardzo istotny i z tego też względu jest nieodłącznym elementem oceny cyberryzyka. Świadomość zagrożeń cybernetycznych i szkolenie załogi ma kluczowe znaczenie dla cyberbezpieczeństwa statków. Niezbędna jest pewność, że członkowie załóg i osoby odpowiedzialne za cyberbezpieczeństwo utrzymują wymagany poziom dyscypliny i przestrzegają ustalonych procedur.

Po dokonaniu odpowiedniej oceny wszelkich potencjalnych cyberzagrożeń w odniesieniu do ludzi, procesów, procedur i technologii, należy uwzględnić politykę bezpieczeństwa cybernetycznego na wszystkich poziomach zarządzania, na pokładach i na lądzie oraz opracować system stałych przeglądów, inspekcji i wewnętrznych audytów cyberbezpieczeństwa.

Drugim krokiem jest projekt bezpiecznej morskiej architektury cybernetycznej. Zgodnie z wytycznymi zawartymi w Kodeksie ISM i Przewodniku IMO organizacje morskie są zachęcane do projektowania, ustanawiania lub włączania zarządzania ryzykiem cybernetycznym do swojego systemu zarządzania bezpieczeństwem. Organizacje, reprezentujące branżę morską, będą miały różne potrzeby i różne poziomy dojrzałości, jeśli chodzi o zakres sieci OT na statku i systemów związanych z cyberprzestrzenią, stąd też będą miały także inne podejście do sposobów zabezpieczania ich morskich architektur cybernetycznych.

Organizacje morskie mogą zaprojektować bezpieczną morską architekturę cybernetyczną na kilka sposobów.

Jednym z podejść, które jest akceptowane przez IMO, jest porównanie aktualnej kompleksowej oceny ryzyka cybernetycznego z pożądanym przez organizację systemem zarządzania ryzykiem cybernetycznym. Tym sposobem można

wyeliminować wszelkie zidentyfikowane luki, aby osiągnąć cele zarządzania cyberryzykiem i umożliwić najbardziej efektywne wykorzystanie zasobów.

Można także opracować swoją politykę bezpieczeństwa cybernetycznego, obejmującą elementy ram bezpieczeństwa cybernetycznego określone przez NIST (ang. *The National Institute of Standards and Technology, U.S. Department of Commerce*). Pomogą one zapewnić właściwe praktyki w zakresie cyberbezpieczeństwa na statkach. Polityka bezpieczeństwa cybernetycznego powinna obejmować kompleksową ocenę wszystkich zidentyfikowanych zagrożeń cybernetycznych w odniesieniu do statków, personelu i środowiska, a także ciągłe doskonalenie zarządzania ryzykiem cybernetycznym.

IMO sugeruje również aktualizację systemu zarządzania bezpieczeństwem (SMS) w celu uwzględnienia ram zarządzania cyberzagrożeniami morskimi i włączenia dokumentacji ryzyka cybernetycznego, która zawiera szczegółowe informacje na temat elementów krytycznych, które mogą niekorzystnie wpłynąć na funkcjonowanie statku, jeśli zostaną naruszone, role i obowiązki kluczowych pracowników ds. cyberbezpieczeństwa, procedury działań naprawczych i zapobiegania kolejnym incydentom; plany reagowania na incydenty, procedury tworzenia i utrzymywania kopii zapasowych oraz procedury zgłaszania incydentów cybernetycznych.

Ostatni, trzeci krok związany jest z ochroną statków i operacji morskich, co jest głównym celem rezolucji IMO. Funkcjonalne elementy ram bezpieczeństwa cybernetycznego, określone przez NIST, muszą być spójną częścią polityki morskiego cyberbezpieczeństwa. Pozwoli to wykonać następujące czynności[33]:

a) zidentyfikować krytyczne systemy cybernetyczne oraz ruch sieciowy przepływający przez statkowe systemy IT i OT,
b) ochraniać:
   - urządzenia krytyczne, aktywa i dane, dzięki segmentacji sieci i ciągłemu monitorowaniu oraz walidacji,
   - ruch sieciowy przed nieautoryzowaną lub nieznaną aktywnością,
   - dostęp do sieci,
   - zasoby i systemy z zaawansowanymi mechanizmami szyfrowania,
c) wykryć:
   - krytyczne urządzenia, zasoby lub dane dzięki monitorowaniu w czasie rzeczywistym,
   - nieautoryzowany lub nieznany ruch sieciowy i/lub urządzenia,
   - nietypowe zdarzenia,
   - walidację danych za pomocą sygnałów analogowych i cyfrowych,

[33] Mission Secure, *IMO 2021: Three Steps to Ensure IMO/ISM Cybersecurity Compliance*, https://www.missionsecure.com/blog/imo-2021-three-steps-to-ensure-imo-cybersecurity-compliance, dostępny 19.11.2020 r.

- potencjalne cyberataki z powiadomieniami lub alertami w czasie rzeczywistym,

d) odpowiedzieć i odzyskać:
   - krytyczne urządzenia, zasoby lub dane dzięki monitorowaniu w czasie rzeczywistym,
   - powiadomienia lub alerty w czasie rzeczywistym kierowane do kluczowego personelu,
   - zautomatyzowane i/lub manualne działania naprawcze.

WNIOSKI

Tytułem krótkiego podsumowania można sformułować następujące syntetyczne wnioski:

1. Cyberbezpieczeństwo staje się coraz ważniejszym tematem, ponieważ obecne mechanizmy blokowania zagrożeń i zapobiegania są coraz mniej skuteczne w przypadku zaawansowanych ataków. Wyzwaniem dla bezpieczeństwa cybernetycznego jest zapewnienie adaptacyjnego procesu ochrony, integrującego funkcje predykcyjne, zapobiegawcze, detekcyjne i reagowania[34]. W ramach arsenału bezpieczeństwa cybernetycznego zaawansowane technologie ochrony przed zagrożeniami stają się coraz ważniejsze w przeciwdziałaniu wyrafinowanym atakom i stają się elementem szerszej strategii cyberobrony.
2. Statki autonomiczne będą stanowić nowe wyzwanie dla strategii cyberobrony. Chociaż sztuczna inteligencja będzie kluczowym czynnikiem umożliwiającym autonomiczne operacje, a także zajmie centralne miejsce w łagodzeniu cyberzagrożeń, będzie także potencjalnym narzędziem wykorzystywanym przez przyszłych hakerów.
3. Wraz z rozwojem systemów łączności i komunikacji, udostępniania danych i systemów autonomicznych progresowi będą także podlegać zagrożenia cybernetyczne. Potrzeba zapewnienia zdalnego dostępu do infrastruktury i statków może zwiększać ryzyko poważnych zakłóceń w międzynarodowej żegludze i operacjach morskich z powodu różnych działań o charakterze politycznym, przestępczym lub terrorystycznym.
4. Rozwój technologii i oprogramowania wprowadził nowe sposoby zarządzania jednostkami pływającymi. Obecnie istnieją platformy, które można kontrolować w dowolnym miejscu na świecie za pomocą internetowych narzędzi sterowania. Wprawdzie znacznie zwiększa to łatwość

[34] N. MacDonald, P. Firstbrook, *Designing an Adaptive Security Architecture for Protection from Advanced Attacks*, https://www.gartner.com/en/documents/2665515, dostępny 25.11.2020 r.

zarządzania tymi systemami, ale czyni je w istotny sposób zależnymi od informacji cybernetycznych, które stają się kluczowymi elementami zapewniającymi powodzenie wykonywanych operacji. To połączenie internetowe może stanowić dla hakerów okno do pozyskiwania informacji, a nawet przejęcia kontroli nad platformami.

5. Obecnie większość morskich polis ubezpieczeniowych zawiera klauzulę wykluczenia ataków cybernetycznych (CL380 10/03)[35]. To stawia cyberataki poza zakresem większości polis ubezpieczeniowych. Powoduje to sytuację, w której każda firma, nie zapewniając odpowiedniego poziomu bezpieczeństwa cybernetycznego, jest narażona na poważne ryzyko finansowe i utratę swojej reputacji.
6. W przyszłości rozwiązania w zakresie bezpieczeństwa cybernetycznego będą wymagały adaptacyjnych architektur bezpieczeństwa, które będą koncentrować się na bezpieczeństwie niezbędnym do obsługi systemów cyfrowych, rozwiązań IoT i AI, gdzie będzie to szczególnie trudne[36].
7. W miarę jak statki morskie i infrastruktura stają się coraz bardziej inteligentne i niezależne od ludzi, więcej procesów z nimi związanych będzie narażonych na ryzyko, które do tej pory było typowe dla innych sektorów. Biorąc pod uwagę wysoce zaawansowany charakter systemów autonomicznych, zasadnicze znaczenie będzie miało wprowadzenie solidnych środków zapewniających właściwy poziom bezpieczeństwa cybernetycznego jednostkom autonomicznym.
8. Należy mieć cały czas na uwadze dojrzałość cyfrową branży morskiej. Statki coraz częściej korzystają z systemów opartych na cyfryzacji, integracji i automatyzacji i związane z tym ryzyko i zagrożenia muszą być odpowiednio uwzględnione.
9. Rosnące zaufanie cyfrowe zapewniło ogromną wydajność i korzyści operacyjne, ale otworzyło również puszkę Pandory z cyberzagrożeniami – to ta druga strona obok niepodważalnych korzyści, można ją określić mianem rzeczywistości ryzyka, którą właściciele i operatorzy jednostek pływających muszą zrozumieć.
10. Jak wyraźnie pokazują incydenty Maersk, COSCO, Austal i inne, cyberprzestępczość stanowi rosnące zagrożenie dla firm żeglugowych. Nieautoryzowany dostęp lub złośliwe ataki na systemy i sieci statków mogą mieć poważne konsekwencje, stąd też zapewnienie bezpieczeństwa eksploatacji tych systemów powinno być priorytetem numer jeden.

[35] https://www.kennedyslaw.com/thought-leadership/article/cyber-exclusion-clauses-are-they-fit-for-purpose, dostępny 26.11.2020 r.

[36] S. Searle, B. Burke, D. Cearley, M. Walker, *Top 10 Strategic Technology Trends for 2017: A Gartner Trend Insight Report*, https://www.gartner.com/en/documents/3645332, dostępny 26.11.2020 r.

11. W rzeczywistości, w miarę jak nowoczesne statki stają się coraz bardziej autonomiczne, zautomatyzowane i coraz bardziej zależne od systemów sterowania opartych na oprogramowaniu, zarządzanie cyberbezpieczeństwem staje się także krytyczne z punktu widzenia biznesowego, to nie tylko utrzymanie bezpieczeństwa samych jednostek pływających.
12. Należy zdawać sobie sprawę, że obecny świat żeglugi morskiej jest bardziej skomplikowany niż kiedyś. Praktycznie nie jest możliwe poradzenie sobie z cyberzagrożeniami i lukami w zabezpieczeniach, tak jak w przypadku wgniecenia lub dziury w kadłubie, co można w miarę szybko naprawić i na tym zakończyć. Cyberataki wymierzonę są w branżę w trybie 24/7. Bezpieczne poruszanie się w tej nowej rzeczywistości zagrożeń wymaga „wszystkich rąk na pokładzie". Nie ma jednego sposobu na zwalczanie cyberzagrożeń. Jest to współpraca obejmująca ludzi oraz środki techniczne i proceduralne.
13. Segmentacja sieci pomaga zmniejszyć zakres ataku i jest bardzo przydatną koncepcją architektoniczną strategii cyberbezpieczeństwa. Stąd też zaleca się, żeby systemy OT i IT były podzielone na segmenty, co pozwala ograniczyć zakres oddziaływania cyberataku i powstrzymanie jego rozprzestrzeniania się na inne krytyczne elementy statku.
14. Warto pamiętać także o tym, że hakerzy nie dyskryminują - uderzają w duże i małe organizacje, z dużymi zasobami cyberbezpieczeństwa lub bez nich.

BIBLIOGRAFIA

[1] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC, *The Guidelines on Cyber Security Onboard Ships*, ver. 3., 2017.

[2] Blenkey N., *Cybersecurity: Attacks on OT systems are on the increase*, https://www.marinelog.com/news/cybersecurity-attacks-on-ot-systems-are-on-the-increase.

[3] Bolbota V., Theotokatosa G., Boulougourisa E., Vassalosa D., *A novel cyber-risk assessment meth-od for ship systems*, „Safety Science" Nr 131 (2020) 104908.

[4] Bureau Veritas, *Guidelines for Autonomous Shipping*, Guidance Note NI 641 DT R00 E, Paris 2017.

[5] CIS, *Critical Security Controls for Effective Cyber Security*, www.cisecurity.org/critical-controls.cfm.

[6] D'mello A., *IEC 62443: How to achieve the highest levels of industrial security*, https://www.iotglobalnetwork.com/iotdir/2020/04/16/iec-62443-how-to-achieve-the-highest-levels-of-industrial-security-24420.

[7] Federal Information Processing Standards, *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900.

[8] Fruhlinger J., *Petya ransomware and NotPetya malware: What you need to know now*, https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

[9] Greenberg A., *A Guide to LockerGoga, the Ransomware Crippling Industrial Firms*, https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms.

[10] Greenberg A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[11] IMO, *Guidelines on maritime cyber risk management*, MSC-FAL.1/Circ.3, 5 July 2017, Aneks.

[12] Lopez E., *COSCO restores service 5 days after cyberattack*, https://www.supplychaindive.com/news/COSCO-cyberattack-restores-service/528897.

[13] Lopez E., *Ransomware attack hits COSCO in US*, https://www.supplychaindive.com/news/COSCO-US-ransomware-attack/528557.

[14] MacDonald N., Firstbrook P., *Designing an Adaptive Security Architecture for Protection from Advanced Attacks*, https://www.gartner.com/en/documents/2665515.

[15] Maritime Logistics Professional, *Total Shipping Losses Are Declining, But Challenges Persist – Report*, https://www.maritimeprofessional.com/news/total-shipping-losses-declining-challenges-360154.

[16] Mission Secure, *IMO 2021: Three Steps to Ensure IMO/ISM Cybersecurity Compliance*, https://www.missionsecure.com/blog/imo-2021-three-steps-to-ensure-imo-cybersecurity-compliance.

[17] Mission Secure, *Maritime Security Challenges: The Physical Impact of Maritime Cyber Threats*, https://www.missionsecure.com/blog/the-physical-impact-of-maritime-cyberthreats.

[18] Paris C., *China's Cosco Shipping Hit by Cyberattack in U.S.*, https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557.

[19] Ragan S., *SamSam explained: Everything you need to know about this opportunistic group of threat actors*, https://www.csoonline.com/article/3263777/samsam-explained-everything-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html.

[20] Said K., Agamy M., *The impact of cybersecurity on the future of Autonomous ships*, International Journal of Recent Research in Interdisciplinary Sciences (IJRRIS), Vol. 6, Issue 2, Month: April - June 2019.

[21] Searle S., Burke B., Cearley D., Walker M., *Top 10 Strategic Technology Trends for 2017: A Gartner Trend Insight Report*, https://www.gartner.com/en/documents/3645332.Autor (nazwisko, inicjał), *Tytuł*, wydawca, miejsce i rok wydania.

[22] Staśkiewicz J., *System Zarządzania Bezpieczeństwem Informacji wg ISO 27001*, https://opensecurity.pl/bezpieczenstwo-informacji-wg-iso-27001.

[23] Suiche M., *Petya.2017 is a wiper not a ransomware*, https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b.

[24] Tomter L., Gundersen M., *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*, https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043.

[25] Warrick J., Nakashima E., *Officials: Israel linked to a disruptive cyberattack on Iranian port facility*, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[26] https://safety4sea.com/guidelines-on-maritime-cyber-risk-management.

[27] https://searchsecurity.techtarget.com/definition/cybersecurity.

[28] https://sklep.pkn.pl/pn-en-iso-iec-27001-2017-06p.html.

[29] https://www.iec.ch/cybersecurity/?ref=extfooter.

[30] https://www.kennedyslaw.com/thought-leadership/article/cyber-exclusion-clauses-are-they-fit-for-purpose.

[31] https://www.nist.gov/cyberframework/framework.

[32] https://www.ocimf.org/sire/about-tmsa.

[33] https://www.sertica.com/tmsa/#gref.

SELECTED ASPECTS OF CYBERSECURITY OF MARITIME AUTONOMOUS SURFACE SHIPS

ABSTRACT

The article deals with cybersecurity of maritime autonomous surface ships. Selected cyber attacks that took place in the maritime sector were characterized. The objectives, sequence and effects of cyber attacks, as well as legal regulations in the field of maritime cybersecurity were discussed. However, most attention has been paid to how to prevent cyber threats and to shape a proper maritime cybersecurity policy.