Kibernetička sigurnost na brodu

Zadro, Karlo

SVEUČILIŠTE U SPLITU
POMORSKI FAKULTET

KARLO ZADRO

KIBERNETIČKA SIGURNOST NA BRODU

ZAVRŠNI RAD

SPLIT, 2022.

SVEUČILIŠTE U SPLITU
POMORSKI FAKULTET

STUDIJ: POMORSKE ELEKTROTEHNIČKE I INFORMATIČKE TEHNOLOGIJE

KIBERNETIČKA SIGURNOST NA BRODU

ZAVRŠNI RAD

MENTOR: **STUDENT:**

Izv. prof. dr. sc. Anita Gudelj **Karlo Zadro (MB: 272492)**

SPLIT, 2022.

SAŽETAK

Brzi razvoj digitalne tehnologije donosi promjene u svjetskoj pomorskoj industriji. Suvremene tehnologije poput oblaka, velikih podataka, pametnih uređaja, interneta stvari i virtualne stvarnosti omogućile su e-navigaciju, pametne luke, bespilotna vođena vozila na terminalima i automatizirana plovila. S jedne strane, ove su tehnologije postale ključne i korisne u smislu učinkovitog rada, smanjenja emisije ugljika, sigurnosti i zaštite broda, posade, tereta te morskog okoliša. S druge strane, povećana digitalizacija predstavlja prijetnju od kibernetičkih napada koji mogu biti različitog tipa, od neovlaštenog pristupa podacima do zlonamjernih napada na brodske sustave i mreže. Potencijalni učinak takvih zlonamjernih radnji može imati katastrofalne posljedice za osoblje na brodu i na obali, putnike i za okoliš. U ovom radu identificirane su ranjivosti koji čine brod podložnim kibernetičkim prijetnjama. Također, iznesen je pregled najznačajnijih kibernetičkih incidenata u brodarstvu. Svrha rada je podizanje svijesti o kibernetičkim rizicima broda kao i o potrebnoj edukacije o novom obliku sigurnosne prijetnje koja zahvaća pomorsku industriju..

Ključne riječi: *kibernetička sigurnost, prijetnje, brodski sustavi, ranjivost*

ABSTRACT

Nowadays, the rapid development of digital technology poses changes in the face of the global maritime industry. Modern technologies such as clouds, big data, smart devices, the internet of things and virtual reality enabled e-navigations, smart ports, unmanned guided vehicles on terminals and automated vessels. On one side, these technologies have become crucial and beneficial in terms of efficient operations, reducing carbon emissions, safety and protection of a ship, crew, cargo and the marine environment. On the other, the increased digitalisation causes cyber threats which resulted different attacks, in the range from unauthorized data access to malicious attacks on shipboard systems and networks. The potential impact of such malicious actions can have significant consequences for staff on board and ashore, passengers, as well as, on the environment. In this paper the threats that make a ship vulnerable to cyber-threats were identified. Also, the overview of the most significant cyber incidents in shipping was presented. The purpose of this paper is to raise awareness of cyber

risks of the ship as well as the necessity of education about a new form of security threat affecting the maritime industry.

Keywords: *cybersecurity, cyber threats, ship's systems, vulnerabilities*

SADRŽAJ

1. UVOD

Kibernetičke prijetnje za pomorski sektor predstavljaju sve veću opasnost iako brodovi izgledaju kao neuobičajene mete kibernetičkih napada. U cilju bolje učinkovitosti i produktivnosti brodovi sve više koriste sustave upravljanja i nadzora koji se oslanjaju na digitalizaciju, integraciju i automatizaciju. Informacijska tehnologija (engl. Information Technology, IT) i operativna tehnologija (engl. *Operational Technology*, OT) ili industrijskih upravljačkih sustavi (engl. *Industrial Control Systems,* ICS) na brodovima međusobno su umreženi i povezani s Internetom, što nosi rizik od neovlaštenog pristupa ili zlonamjernih napada na brodske sustave i mreže. Podatci koje razmjenjuju brod i obalni ured postaju najčešća meta kibernetičkih napada jer se ne koristi enkripcija [12]. Rizici ne ovise samo o sustavima i procesima nego i o ljudskom faktoru [7].

Prema istraživanju koje je 2020. godine provelo Finskog udruženja brodara, a objavljeno od strane Baltičkog i Međunarodnog pomorskog vijeća (engl. *Baltic and International Maritime Council – BIMCO*) i Safety at Sea [2], 38% ispitanika je navelo da kibernetičke napade vide kao visok rizik za pomorski sektor. Rezultati su pokazali porast kibernetičkih napada na pomorske organizacije, od 21% više kibernetički napadi u 2016. do 31% u 2020. godini. Najveći problem u borbi s kibernetičkim prijetnjama predstavlja razvoj tehnologije jer potencijalni napadači koriste sofisticiranije sustave pa ih je samim time teže identificirati. Ipak pravovremenim sigurnosnim smjernicama, razvojem strategija i planova moguće je brzo i učinkovito odgovoriti na kibernetičke prijetnje.

Cilj završnog rada je prikazati kibernetičke prijetnje kao ozbiljan problem pomorskom prometu, ukazati na ranjivost brodskih sustav te istaknuti smjernice za što bolju zaštitu i sigurnost od kibernetičkih prijetnji. Svrha rada je podizanje svijesti o kibernetičkim rizicima broda kao i o potrebnoj edukacije o novom obliku sigurnosne prijetnje koja zahvaća pomorsku industriju.

Završni rad podijeljen je na sedam poglavlja. U uvodnom poglavlju definiran je cilj i svrha istraživanja rada. U drugom poglavlju opisan je pojam digitalizacije te njene prednosti i izazovi za pomorski sektor. U trećem poglavlju su opisane različite kibernetičke prijetnji koje mogu predstavljati prijetnje pomorskom prometu te su opisane kategorije kibernetičkih napada. U četvrtom poglavlju prikazani su različiti izvori i motivi kibernetičkih prijetnji na sigurnost brodskog sustava. Također, prikazani su i primjeri kibernetičkih napada na brodove i luke iz kojih bi se trebalo učiti kako poboljšati kibernetičku sigurnost broda. U petom poglavlju

opisane su smjernice/mjere kao odgovor na kibernetičke prijetnje. Sedmi dio je zaključak u kojemu su prezentirana zaključna razmatranja.

2. DIGITALIZACIJA U POMORSTVU

Pomorstvo danas ima važnu ulogu u svjetskom gospodarstvu i gotovo 80% svjetske trgovine obavlja se morem. Gotovo 50.000 brodova i milijun pomoraca aktivno sudjeluje u ovoj svjetskoj trgovini [6]. Uz ovu ekspanziju trgovine, s pojavom "velikih podataka" (engl. *Big data*) i međusobno povezanih tehnologija, posljednjih 25 godina pomorski sektor prolazi kroz digitalnu revoluciju. U svijetu brodarstva stalna je tendencija povećanja veličine brodova i smanjenja broja članova posade. Učinkovito upravljanje takvim sve većim brodovima zahtijeva primjenu i korištenje različitih informacijskih tehnologija (IT), kako na brodu tako i na kopnu.

2.1. DIGITALIZACIJA

Nove digitalne tehnologije kao što su Internet stvari (engl. *Internet of Things*, IoT), veliki podatci (engl. *Big Data*), oblaci (engl. *Clouds*) promijenile su poslovanje i tradicionalnu poslovnu strategiju mnogih tvrtki pa tako i brodarskih. Moderne tehnologije su omogućile modularnost, distribuirano, više-funkcionalno i globalne poslovanje koje je neovisno o vremenu i prostoru. Omogućile su nove poslovne logike i nove poslovne modele za stvaranje ekonomske i društvene vrijednosti. Pojava digitalizacije sve više zadire u brojne poslovne i industrijske sustave. Može se reći da se digitalizacija odnosi na tehničke procese, odnosno integraciju digitalnih tehnologija u svakodnevni život. Iz aspekta informacijskih tehnologija digitalizacija opisuje analogne i digitalne podatke koji se pretvaraju u digitalni format, na primjer, programiranjem ili komuniciranjem fizičkih proizvoda [2]. Osnovni cilj digitalizacije je automatizacija poslovnih procesa poslovanja, kao i obrada informacija kako bi se postigla učinkovitosti i produktivnosti.

Digitalizacija u pomorstvu postaje sve prisutnija zbog sljedećih poboljšanja performansi računalnih sustava.

- Računalna snaga – računala su danas brza, mogu izvoditi milijune naredbi, matematičkih izračuna i algoritme što dovodi do stalnog protoka i obrade informacija.
- Pohrana podataka – razvoj memorija, hardvera i računalnih oblaka pridonijeli su razvoju dostupnih i moćnih rješenja za pohranu i rukovanje podatcima.
- Povezanost – veći broj priključaka na brodovima omogućava bolju povezanost što koristi pomorskoj industriji u prikupljanju i/ili pružanju podataka u stvarnom vremenu o performansama stotina brodova koji su miljama daleko od obale.

- Senzori – omogućavaju prikupljanje podataka u stvarnom vremenu o komponentama i podsustavima broda, kao što su podatci o emisiji štetnih plinova, temperaturi tereta, lokaciji, podatci o vremenu, oceanskim strujama, kao i status propelera motora koji povećava učinkovitost održavanja i sigurnosti.

Digitalizacija se trenutno primjenjuje na osam različitih digitalnih područja, a to su [2]:

- virtualna stvarnost (engl. *Virtual reality, VR*)
- umjetna inteligencija (engl. *Artificial intelligence, AI*)
- autonomna vozila i robotika
- računalstvo u oblaku (engl. *Cloud computing*)
- veliki podaci (engl. *Big Data*)
- 3D tehnologija modeliranja i tiskanja
- proširena i potpomognuta virtualna stvarnost
- Internet stvari (engl. *Internet of Things, IoT*)
- 5G mreže.

Kao primjer korištenja računalstva u oblaku može se navesti brodarska kompanija UASC koja je migrirala na sustav za naručivanje bunkera putem računalstva u oblaku. Klasičan način naručivanja bunkera bio je skup, pa su predstavnici UASC-a napravili korak naprijed, potpisavši ugovor sa *Shiptech* kompanijom kako bi stvorili platformu za naručivanje bunkera u oblaku. Migriranje na novi sustav omogućuje UASC-u praćenje tržišnih cijena, bolju komunikaciju s dobavljačima, poboljšanje praćenja performansi broda i planiranje bunkeriranja cijele flote [1].

Pojava digitalizacije i utjecaj koji je takav oblik transformacije izazvao danas značajno utječe u brojnim poslovnim procesima velikih svjetskih industrija poput telekomunikacijske, zdravstva, bankarstva, automobilske industrije i dr. Digitalna transformacija omogućila je nove inovacijske prakse, poboljšani dizajn i različite nove poslovne modele, a sukladno tome stvaranje nove vrijednosti. Poslovna je infrastruktura postala digitalna s povećanim međusobnim povezivanjem proizvoda, procesa i usluga.

U brojnim različitim industrijama i sektorima, pojava i utjecaj digitalnih tehnologija, kao kombinacije računalne znanosti, informacija, komunikacije i tehnologije povezivanja, u osnovi mijenja poslovne procese, strategiju, mogućnosti i dr. [8].

2.1.1. IT i OT SUSTAVI BRODA

Danas su brodovi sve složeniji sustavi i ovise o primjeni digitalnih i komunikacijskih tehnologija za obavljanje svojih funkcija. Važno je razlikovati tradicionalne informacijske tehnologije (IT) od operativne tehnologije (OT). To ne znači da su to dva potpuno odvojena sustava. Naprotiv, sve veći je trend da se OT i IT sustavi integrirani i povezani u jedan cjelovit sustav.

Osnovna razlika između ova dva sustava je da OT sustavi kontroliraju fizički svijet, a IT sustavi upravljaju podacima. OT se odnosi na hardver i softver koji upravljaju plovilima, ali i kontrolira fizičke uređaje i procese. Informacijska tehnologija predstavlja spregu mikroelektronike, računala, telekomunikacija i računalnih programa koji omogućavaju unos, obradu, pohranu i distribuciju podataka.

IT sustav broda čine tradicionalne tehnologije kao što su:

- radne stanice, prijenosna računala i mobiteli
- elektronička pošta
- Internet, intranet, dijeljenje datoteka
- poslovni i financijski sustavi
- poslovna analitika
- upravljanje narudžbama.

OT sustavi su obično manje poznati od IT sustava i često njima upravljaju dobavljači. Primjeri takvih sustava su:

- Elektronički prikaz navigacijskih karata i informacijskih sustava (engl. *Electronics Chart Display and Information System, ECDIS*)
- Zapisivač o putovanju brodova (engl. *Voyage Data Recorder, VDR*),
- Uređaj za otkrivanje položaja (engl. *Emergency Position Indicating Radio Beacon, EPIRB*)
- GPS (engl. *Global Positioning System*)
- Komunikacije (Satcom, Fleet Broadband, 3G/5G, Wifi)
- Upravljanje napajanjem
- Upravljanje teretom
- Senzori, PLC-ovi, pumpe, hidraulika, dizalice, itd.

Relevantni brodski sustavi potrebni za sigurnost plovidbe, opskrbu električnom energijom i upravljanje teretom sve se više digitaliziraju i povezuju s Internetom za obavljanje širokog raspona legitimnih funkcija, a ti sustavi česta su prijetnja kibernetičkih napada. Neke od funkcija koje ti sustavi obavljaju su [7]:

- praćenje rada motora
- servis i upravljanje rezervnim dijelovima
- ukrcaj i iskrcaj, rukovanje, upravljanje dizalicom i pumpama i dr.
- praćenje performansi broda.

Rizici IT i OT sustava razlikuju se po tome što rizici IT sustava uglavnom ugrožavaju na financije i ugled organizacije, a rizici OT sustavi mogu ugroziti sigurnost posade na brodu ili osoblja na kopnu, tereta ili uzrokovati štetu za pomorski okoliš te zaustavit operacije broda. OT sustavi se spominju kao predstavnici *Internet stvari* (engl. *Internet of Things*, IoT). U takvim slučajevima, mora biti osigurano da je sučelje dovoljno zaštićeno vatrozidom i da potencijalne ranjivosti u OT sustavima ne uzrokuju i ranjivost IT sustava. Ovo je važno jer nije uvijek moguće osigurati odgovarajuću razinu zaštite u OT sustavima. U tablici 1. prikazane su osnovne funkcije IT i OT sustava, a njihovo razumijevanje je bitno kako bi se shvatila kibernetička sigurnost.

Tablica 1: Funkcije IT i OT sustava [8, 9]

Kategorija	**IT sustavi**	**OT sustavi**
Funkcija	Upravljanje podacima	Kontrolirati fizički svijet
	Povjerljivost i integritet podataka je najvažnije	Sigurnost je najvažnija, a zatim zaštita procesa
Rizici	Utjecaji rizika mogu uzrokovati kašnjenje: broda carinjenje, početak utovara/ istovar, te trgovački i poslovne operacije	Učinci rizika su neusklađenost propisa, kao i šteta za osoblje na brodu, okoliš, opreme i/ili tereta
	Tolerancija grešaka može biti manje važna	Tolerancija grešaka je bitna, čak trenutnog zastoja možda neće biti prihvatljiv

2.2. PREDNOSTI I IZAZOVI DIGITALIZACIJE U POMORSTVU

Postepenim prelaska s tradicionalnih operacijskih platformi prema novim IT rješenjima, brodarska industrije kreće u svijet digitalizacije. Brojne su prednosti digitalizacije, ali i izazovi s kojima se pomorski sektor suočava.

U pogledu brojnih IT rješenja, digitalizacija je značajno poboljšala isplativost poslovanja. Danas na brodu postoje ogromne količine podataka koji se generiraju iz različitih izvora. Mnogi sustavi na brodu su dizajnirani za prikupljanje i prezentiranje podataka tvrtki, tj. posadi, različitim dobavljačima i proizvođačima kao pomoć u donošenju odluka tijekom svakodnevnog rada broda. U tu svrhu koriste se senzori koji prikupljaju različite podataka uključujući lokaciju, podatke o vremenu i oceanskim strujama, kao i status propelera motora i tereta. Prikupljeni "real time" podatci, kao i povijesni podatci, omogućuju optimizaciju rad brodskih sustava, predviđanje održavanja, preciznije praćenje potrošnje energije i različitih emisija plinova, uvid i praćenje statusa plovila, nadzor tereta. Pojednostavljene su brojne operacije u smislu protoka informacija i poboljšanog planiranja resursa koje je usko povezano s manjim kašnjenjem, bržom obradom velikih podataka, racionalizacijom operacija, transparentnošću podataka, smanjenjem troškova razmjene informacija i izvršavanja transakcija i dr. [10].

Brza evolucija u korištenju i oslanjanju na informacijske i komunikacije tehnologije, kao i napredak u automatizaciji i integraciji različitih elektroničkih sustava koji podržavaju funkcije upravljanja, optimiranja i poslovne aplikacije, povećava važnost rješavanja svih mogućih skriveni izazovi. Prijelaz na digitalnu i automatiziranu razmjena informacija stvara nove zahtjeve za provjeru autentičnosti autora dokumenta, očuvanje integriteta poruka kao i povjerljivost kada je to potrebno. Problemi s kvalitetom velikih podataka, povjerenje kao i implementacija sigurnost propisa samo su neki od izazova koje sa sobom nosi četvrta industrijska revolucija. Rješavanje sigurnosnih izazova koje proizlaze iz digitalnih tehnologija ozbiljan je aspekt koji vlade, tvrtke i ostali dionici trebaju uzeti u obzir. Poznato je da sigurnost i zaštita već dugo vremena predstavlja problem u pomorskoj industriji. Implementacijom IT i mrežnim povezivanjem brodova, kontejnera, luka, sve većom upotrebom velikih podataka, pametnih brodova i Internet stvari povećava se količina informacija dostupna kibernetičkim napadačima. To stvara potrebu za snažnijom pristupom kibernetičkoj sigurnosti kojoj je glavni cilj zaštititi neovlaštene treće strane od pristupa brodskim podacima putem postojećih sučelja i mrežne povezanosti. Primjena postojećih sigurnosnih smjernica i izmjene relevantnih zakona često su veliki izazov.

Izazov predstavljaju i brojna regulatorna pitanja. Prekomorska dostava je u mnogim aspektima visoko regulirano međunarodno tržište. S novim, izazovnim poslovnim modelima i s novim tehnologijama i konceptima za rješavanje posebnih zadataka, regulatorna pitanja često postaju važna. Tipična pitanja i nedoumice uključuju pitanja poput hoće li uvođenje određene tehnologije ili poslovnog modela biti dopušteno, koje promjene poslovnih modela ili tehnologija mogu biti potrebne za usklađivanje s postojećim propisima i dr. Pomorski sektor suočava se sa sve strožim zahtjevima reguliranim od strane Europske Unije, Međunarodne pomorske organizacije i drugih međunarodnih organizacija i vladinih tijela [11].

Vlasništvo osjetljivih podataka postao je dodatan izazov kod IT platformi. Podaci su postali sve relevantniji za pružanje usluga kao npr. u slučaju praćenja, planiranja ruta, usluga predviđanja, održavanja, planiranja resursa i drugih dodatnih usluga. Osim toga, različiti dionici često imaju interes ne otkrivati posebne podatke drugim stranama u sektoru. Istodobno, vlasništvo nad podacima često nije jasno definirano. Prema tome, za velike usluge i poslovne modele podataka te za podatke za koje kompanija ima veliki interes za povjerljivost, temeljita procjena tokova podataka često je ključni čimbenik. Odgovornost je postala značajno veća. Prenošenjem sve više poslova na automatizirane IT sustave, odgovarajuća raspodjela rizika i odgovornosti između različitih uključenih strana postala je sve važnija. Uz spomenute prednosti, izazove i prepreke u implementaciji novih IT rješenja, postoje još i brojne druge prednosti i nedostaci, a neke će se tek otkriti i pojaviti sve širom pojavom digitalizacije. Na slici 1 sažeto je prikazano nekoliko temeljnih izazova.

Slika 1. Izazovi u primjeni IT tehnologija u pomorstvu

3. KIBERNETIČKA SIGURNOST

Rizik od kibernetičkih napada eksponencijalno se proširio krajem dvadesetog stoljeća, dolaskom interneta, korištenjem sustava računalnih mreža i pojavom digitalizacije kao osnove poslovanja [5]. Sve većom primjenom sustava temeljenih na IT tehnologijama u raznim svjetskim industrijama javila se potreba za zaštitom tih sustava s aspekta sigurnosti i očuvanju njihova integriteta

Kibernetička sigurnost se bavi zaštitom IT i OT sustava te zaštitom podataka od neovlaštenog pristupa, manipulacije i krađe. Pokriva rizike od gubitka dostupnosti ili integriteta važnih podataka i OT-a. Kibernetičko sigurnosni incidentni mogu se pojaviti kao rezultat [8,7]:

- incidenta koji utječe na dostupnost i integritet OT-a - na primjer, oštećenje podataka digitalnih pomorskih karti sadržane u elektroničkom prikazu karte (engl. *Electronic Chart Display and Information System, ECDIS*)
- greške tijekom procesa održavanja softvera ili ugradnje novog hardvera - nisu svi članovi posade obučeni za upravljanje s operativnom opremom instaliranom na brodu u slučaju poremećaja ili čak katastrofe
- gubitka ili manipulacije nad podacima vanjskih senzora koji su kritičnih za rad broda.

Iako su uzroci incidenta različiti, učinkovit odgovor temelji se na edukaciji, osposobljenosti i razvijenoj svijesti o potrebnim odgovarajućim protokolima i postupcima kompanije. Razvojem informacijskih tehnologija u pomorskoj logistici takvi će se problemi sve češće javljati ako se unaprijed ne poduzmu sigurnosne mjere za njihovo sprječavanje.

3.1. TERMINOLOGIJA I DEFINICIJE

U nastavku će se definirat osnovna terminologija potrebna za razumijevanje kibernetičke sigurnosti.

Kibernetika (engl. Cyber) je znanost o procesima upravljanja, reguliranja, dobivanja, pohranjivanja, pretvorbe i prijenosa informacija u sustavima.

Kibernetička prijetnja (engl. Cyber Threat) se može definirati kao napor usmjeren na pristup sustavu, izvlačenje podataka iz sustava, manipulaciju ili oštećenje integriteta, povjerljivosti, sigurnosti i dostupnosti podataka, aplikacija i političkih sustava bez zakonitog dopuštenja. Prijetnja je potencijalni uzrok kibernetičkog incidenta koji koristi ranjivost kibernetičke sigurnosti i uzrokuje štetu sustavima i organizacijama.

Kibernetički napad (engl. *Cyber attack*) je bilo koja vrsta ofenzivnog manevra putem kibernetičkog prostora, usmjeren na informacijsko-komunikacijske i industrijsko upravljačke sustave u svrhu ometanja, onemogućavanja, uništavanja ili zlonamjerne kontrole računalnog infrastrukture, ili uništavanja integriteta podataka ili krađe kontroliranih informacija [8].

Kibernetička sigurnost se može definirati kao skup preventivnih mjera i postupaka koji se koriste za zaštitu podataka od krađe, kompromitiranja ili napada. Zahtijeva razumijevanje potencijalnih informacijskih prijetnji, kao što su virusi i drugi zlonamjerni kod. Strategije kibernetičke sigurnosti uključuju upravljanje identitetom, upravljanje rizikom i upravljanje incidentima. Prema Međunarodnoj telekomunikacijskoj uniji (engl. *International Telecommunications Union. ITU*) kibernetička sigurnost je skup alata, politika, sigurnosnih koncepata, mjera, smjernica, metoda upravljanja rizicima, radnji, obuka, primjera dobrih praksi i tehnologija koje se mogu koristiti za zaštitu sustava, mreže, programa i podataka od digitalnih napada **Error! Reference source not found.**.

Kibernetički incident: Korištenje informacijskog sustava ili mreže sa posljedicom stvarne ili potencijalne štete na informacijskom sustavu, mreži ili informacijama koje se u njima nalaze [13].

Ranjivost: Slabost ili nedostatak u dizajnu, implementaciji ili radu sustava koji može smanjiti sigurnost informacija sustava.

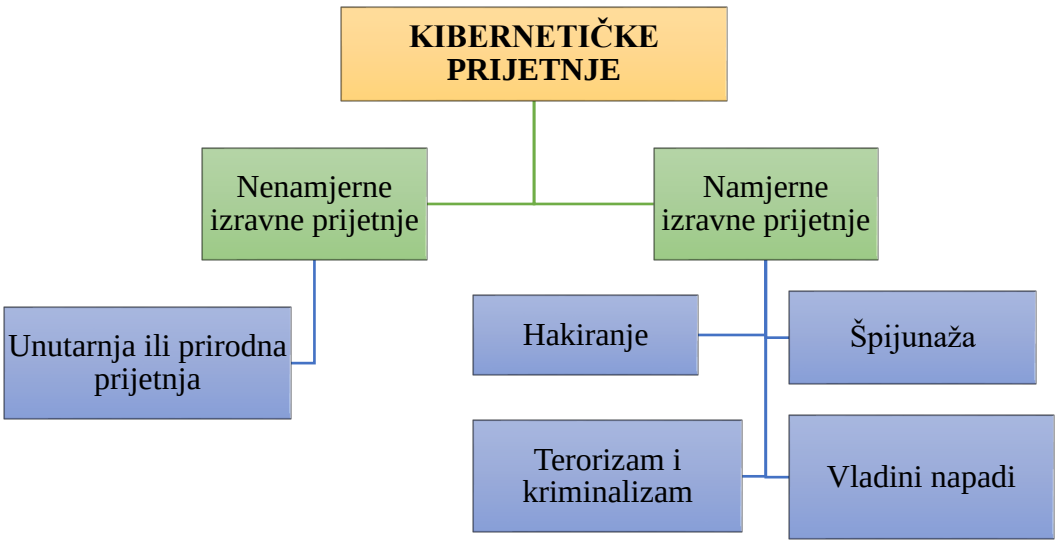
Zlonamjerni program (engl. *Malware*) je generički izraz za niz zlonamjernih programa koji mogu zaraziti računalne sustave i utjecati na njihov rad. Sukladno tome, virus se može definirati kao skriveni, samo replicirajući dio računalnog programa koji zlonamjerno oštećuje i manipulira radom računalnog programa ili sustava [8].

Rizik se definira kao situacija koja uključuje izlaganje opasnosti, uz mogućnost da se dogodi neugodna ili nepoželjna situacija. Danas je kibernetički rizik postao toliko važan da utječe na bilo koju od uobičajenih aktivnosti, a zbog sve bržeg tehnološkog razvoja, slabosti i rizici šire se puno brže.

3.2. VRSTE KIBERNETIČKIH PRIJETNJI

Slika 2 prikazuje vrste kibernetičke prijetnje koje mogu biti:

- namjerne izravne prijetnje
- nenamjerne izravne prijetnje.



Slika 2. Osnovne vrste kibernetičkih prijetnji

Namjerne izravne prijetnje su kako se i iz naziva može zaključiti svjesno izazvane, a dijele se na [5]:

- Hakiranje: Ovu grupu čine pojedinci, kojima je glavna akcija *online* napad s ciljem pristupa sustavu, te krađe osjetljivih informacija i podataka za korištenje u zlonamjerne svrhe.
- Špijunaže: Organizirani su za obavljanje radnji špijunaže s glavnim ciljem dobivanja pristupa povjerljivim informacijama, uništavanju podataka i krađe intelektualnog vlasništva kako bi ih iskoristili za konkurentsku prednost ili ometali poslovanje.
- Vlada: U pomorskoj industriji mnoge su zemlje uključene u kibernetičke napade. Njihova je svrha dobiti pristup državnim tajnama, visokoosjetljivim informacijama, komercijalnim informacijama i vrijednim dokumentima, koji će se koristiti u namjeri izravnog utjecaja na drugu državu ili instituciju od velike važnosti za jedan narod, te ovim činom stvoriti nacionalnu destabilizaciju ili kaos ili steći ekonomsku prednost i informacijsku kontrolu.
- Terorizam: Terorističke skupine mogu koristiti elektroničke i računalne medije kao novi modus operandi za izvođenje svojih terorističkih činova protiv drugih skupina, naroda i kompanija, dobivanjem pristupa i prekidanjem operativnog sustava za ideološke, vjerske ili političke interese ili svrhe.
- Kriminalci: Pojedinci ili kriminalne organizacije koriste kibernetičke napade na međusobno povezane sustave i mreže s namjerom obavljanja kriminalnih aktivnosti, uglavnom usmjerenih na prijevaru, iznude ili krađu intelektualnog vlasništva. Poznato

je da ovi kriminalci, kada dobiju pristup različitim sustavima, mogu kontrolirati operativne sustave kako bi olakšali trgovinu drogom, oružjem i krijumčarenim novcem te ostvarili ekonomsku korist ili prodali vrijedne informacije drugome.

Nenamjerne izravne prijetnje odnose se na interne prijetnje unutar kompanije ili prirodne prijetnje. To mogu biti pogreške zaposlenika ili pružatelja usluga. Zaposlenici kompanije mogu ugroziti sustave pomorske industrije nemarom, neznanjem ili samo ljudskom pogreškom, slučajnim otvaranjem zlonamjernih elektroničkih poruka, korištenjem zaraženih prijenosnih medija ili pristupanjem lažnim *web* stranicama i društvenim mrežama. Ove nenamjerne radnje izlažu osjetljive brodske sustave ili podatke prijetnjama, stvarajući tako dodatni rizik. Prepoznato je da ova vrsta prijetnje proizlazi iz nedostatka obuke i svijesti brodskog osoblja na kibernetičke napade. Obuka i svijest trebali bi biti prilagođeni ovisno o tome na kojem brodskom sustavu pojedinac radi i koliko je taj sustav izložen kibernetičkim napadima [14].

Prirodne prijetnje se mogu opisati kao greške u sustavu, programu ili aplikaciji koje proizlaze iz loše instalacije ili proizvodnje, a koja ne pruža sigurnosne opcije koje su potrebne za očuvanje sigurnosti sustava [8]. Pripadajući hardver ili softver koji proizvođač više ne ažurira, neće primati buduće nadogradnje za rješavanje potencijalnih ranjivosti. Iz tog razloga, korištenje hardvera i softvera koji više nije podržan od strane kompanjie treba pažljivo procijeniti kao dio procjene kibernetičkog rizika [14].

Za razliku od drugih područja sigurnosti gdje postoje dokazi o napadima i gdje je potrebno izvješćivanje o incidentima, kibernetička sigurnost postaje izazovnija zbog nepostojanja bilo kakvih konačnih informacija o incidentima i njihovom utjecaju. Dok se ne pribave ti dokazi, razmjer i učestalost napada i dalje će biti nepoznati. Iskustva iz drugih poslovnih sektora poput financijskih institucija, javnih uprava i zračnog prometa pokazala su da uspješni kibernetički napadi mogu rezultirati značajnim gubitkom usluga, imovine, pa čak i ugroziti ljudske živote. Brodarska industrija također bi trebala proaktivno raditi na razumijevanju i ublažavanju kibernetičkih prijetnji.

3.3. KATEGORIJE KIBERNETIČKIH NAPADA

Općenito, postoje dvije kategorije kibernetičkih napada:

- nasumični napadi (engl. *untargeted attacks*) gdje napadač nema određenu metu, već napadač putem mreže postavlja zamke kojima hvata svoje žrtve.

- ciljani napadi (engl. *targeted attacks*) gdje su sustavi, programi ili podaci kompanije ili broda ciljana meta zlonamjernog djelovanja.

Nasumični napadi će vjerojatno koristiti alate i tehnike dostupne na Internetu koji se mogu koristiti za lociranje, otkrivanje i iskorištavanje ranjivosti sustava. Neki od najčešće korištenih tehnika su [8]:

- ***Zlonamjerni programi:*** Dizajnirani su za pristup ili oštećenje softvera i/ili hardvera računala bez znanja vlasnika. Postoje različite vrste zlonamjernog programa, uključujući trojanske viruse, ransomware, špijunski softver, viruse i crve.
- ***Društveni inženjering:*** Tehnike koje koriste potencijalni kibernetički napadači kako bi prevarili pojedince da prekrše sigurnosne procedure i naveli ih na otkrivanje osjetljivih podataka npr. broj bankovnog računa), normalno, ali ne isključivo, putem interakcije preko društvenih medija.
- ***Krađa identiteta*** (engl. *Phishing*): Slanje elektroničkih poruka velikom broju potencijalnih ciljeva tražeći određene osjetljive ili povjerljive informacije. Takva poruka također može zahtijevati da osoba posjeti lažnu *web* stranicu koristeći hipervezu koja je uključenu u poruci.
- Uspostavljanje lažne *web* stranice ili ugrožavanje originalne *web* stranice radi iskorištavanja posjetitelja.
- ***Skeniranje***: Nasumičan napad na velike dijelove interneta.
- ***Prijetnje kroz IoT uređaje:*** IoT uređaji, poput industrijskih senzora, ostaju glavna meta zlonamjernih napada jer rijetko imaju potrebnu zaštitu. Hakeri pokušavaju preuzeti kontrolu nad uređajem i neovlašteno pristupiti podacima koje uređaj prikuplja.

Ciljani napadi mogu biti sofisticiraniji i koristiti alate i tehnike posebno napravljene za ciljanje kompanije ili brodova. Primjeri čestih alata i tehnika koji se mogu koristiti u ovim napadima [8,15]:

- *Spear Phishing*: Poput *Phishinga*, ali pojedinci su ciljani osobnim e-porukama, često sadržavajući zlonamjerni program ili veze koje automatski preuzimaju zlonamjerni program
- napad putem zlonamjernog programa (*Malware*), bilo kakav oblik virusa, trojana ili crva. Cilj takvih programa može biti specifičan ili sveobuhvatan, ali najčešće sa namjerom dobivanja pristupa informacijama bez znanja vlasnika

- *Ransomware*: Vrsta *Malware* programa dizajnirana funkcijom enkripcije podataka uređaja. Sve informacija sistema postaju neupotrebljive dok se ne ispune uvjeti novčane isplate za dekodiranje
- MITM (engl. *Man in the Middle*): potajno prenošenje ili izmjena podataka između dvije strane koje vjeruju da međusobno izravno komuniciraju ne znajući da komunikacija biva preko posrednika
- napad uzastopnim pokušavanjem (engl. *Brute force*): Napad kojim se pokušavaju mnoge lozinke s nadom da će se na kraju točno pogoditi. Napadač sustavno provjerava sve moguće lozinke dok ne pronađe ispravnu
- napadi uskraćivanjem resursa (engl. *Denial of service - DoS)*: Onemogućuje pristup informacijama legitimnim i ovlaštenim korisnicim, obično preplavljivanjem mreže podacima. Distribuirani napad uskraćivanja usluge (engl. *Distributed denial of service, DDoS*) preuzima kontrolu nad više računala i/ili poslužitelja za provedbu DoS napada
- napad lanca nabave *(*engl. *Supply chain attack)*: Napad na kompaniju ili brod kompromitirajući opremu, programe ili prateće usluge koje se isporučuju kompaniji ili brodu.

Porast *Spear Phishingu* napada zabilježen je 2019. godine u Americi [16]. To je primjer ciljanog napada. Incident je potaknuo američku obalnu stražu da izda niz obavijesti, savjeta i smjernica. Upozorili su da se e-poruke za koje se tvrdi da dolaze od nadzornog tijela američke lučke uprave (engl. *U.S. Port State Control authority*) šalju brodovima i šire zlonamjerni program kroz brodske sustave koji tako mogu ugroziti brodsku mrežu. Istraga je otkrila da iako je zlonamjerni program značajno degradirao funkcionalnost računalnog sustava na brodu, to nije utjecalo na bitne upravljačke brodske sustave. Dodatno, što možda i nije iznenađujuće, primijetili su da je brod, radeći bez učinkovitih mjera kibernetičke sigurnosti, izlagao kritične kontrolne sustave broda značajnim ranjivostima. Iako su ovakvi incidenti pravi razlog za zabrinutost, češće je u pomorskom području zlonamjerni program unesen slučajno ili nepažnjom u brodske sustave od strane ljudi [17].

Kibernetički napadi se također mogu sinkronizirati s kopnenim manevrima i koristiti kako bi se prouzročila veća šteta. Točno tempirani kibernetički napad mogao bi onesposobiti sposobnost komunikacije i ometati koordiniran odgovor [18].

Kontinuirani porast kibernetičkih napada, zajedno sa sigurnosnim prekršajima koji su ti napadi prouzročili, javila se potrebna za dodatnim ulaganjem u kibernetičku sigurnost. Ljudski

čimbenik igra temeljnu ulogu u učinkovitosti napada kao značajan element ranjivosti za kompanije.

Prema istraživanjima provedenim u 2016. od strane *HIS Fairplay* u suradnji s Baltičkim i Međunarodnim pomorskim vijećem (engl. *Baltic and International Maritime Council - BIMCO*), zlonamjerni program (*Malware*) predstavlja 77% svih pomorskih kibernetičkih napada [5]. Prema tome, razvoj kibernetičke sigurnosti i implementacija sigurnosnih strategija za rješavanje kibernetičkih prijetnji i rizika, zajedno s davanjem prioriteta internom djelovanju i promicanjem svijesti o sigurnosti i obuci ljudskih resursa, od vitalnog je značaja za sigurno poslovanje kompanije.

4. KIBERNETIČKA SIGURNOST NA BRODU

Kibernetička sigurnost pomorstva je odabir politika, smjernica, sigurnosnih kontrola, obuke, dobre prakse i tehnologija koje se koriste za zaštitu pomorskih organizacija, njihovog okruženja i njihovih plovila.

Međunarodna pomorska organizacija (*engl. International Maritime Organistion*, IMO) u svojim smjernicama za upravljanje pomorskim kibernetičkim rizikom, Guidelines on Maritime Cyber Risk Management (MSC-FAL.1-Circ.3) [17], definira kibernetički rizik kao:

"...pomorski kibernetički rizik odnosi se na stupanj ugroženosti tehnologije okolnostima ili događajem, što može rezultirati operativnim, sigurnosnim ili zaštitnim ugrožavanjem kao posljedica oštećenja, gubitka ili kompromitiranja informacija ili sustava."

Nadalje poglavlje 1.2.2 Međunarodnog kodeksa upravljanja sigurnošću, International Safety Management (ISM) Code, navodi [19]:

"*...Sigurnosni menadžment kompanije trebao bi, između ostalog[...] omogućiti sigurnu praksu i radno okruženje na brodu[...] procijeniti sve identificirane rizike za svoje brodove, osoblje i okoliš i utvrditi odgovarajuće zaštitne mjere[...] kontinuirano poboljšavati sigurnosni menadžment osoblja na obali i brodovima, uključujući pripremu za hitne slučajeve vezane za sigurnost i zaštitu okoliša*…"

4.1. ZAŠTO JE VAŽNA KIBERNETIČKA SIGURNOST NA BRODU?

Mnogi brodovi još uvijek koriste stare sustave i tehnologiju koje nisu namijenjene za spajanje na Internet. Takvi brodski sistemi i mreže su kombinacija informacijskih tehnologija (IT) i operacionalnih tehnologija (OT). Specifičnije, kod arhaične IT tehnologije ne postoji opcija ažuriranja jer većini kompanija koje pružaju IT usluge nije u interesu održavati takve sustave i kao takvi su veći kibernetički rizik od novije tehnologije. Primjerice, operativni sustav Windows XP se još uvijek koristi na brodovima iako nema opciju ažuriranja [24].

IT i OT koriste se za navigaciju, komunikaciju, inženjering, upravljanje tereomt, balast, sigurnost, kontrolu okoliša i za mnoge druge svrhe. IT i OT na brodovima povezuju se i integriraju, sve češće putem interneta. To donosi veći rizik od neovlaštenog pristupa ili zlonamjernih napada na brodske sustave i mreže. Za naglasiti je da neovlašten pristup IT može omogućiti pristup OT sustavima i obrnuto. Ove sustave koriste posada, putnici i ostali dionici pomorskog sektora, najčešće bez ikakve kontrole. Rizici također mogu nastati zbog osoblja koje

pristupa sustavima na brodu, na primjer uvođenjem zlonamjernog programa putem prijenosnog medija [21].

Stoga je ključno da se kibernetička sigurnost pravilno primjenjuje. Odgovorno ponašanje štiti brod, posadu i teret od potencijalnih kibernetičkih prijetnji i napada. Povjerljivost, integritet i dostupnost podataka imperativ su za sve dionike pomorskog prijevoza zbog ogromne količine osjetljivih informacija i novca koji su uključeni u svaku aktivnost [9].

4.2. MOTIVACIJA KIBERNETIČKIH PRIJETNJI I NAPADA

Pomorski sektor je sve češća meta organiziranog kriminala. Pojedine pomorske organizacije i kompanije su prijavile u posljednjih par godina ciljane kibernetičke napade. Trend koji je kroz posljednjih par godina alarmantno rastući.

Prema izvješću agencije Europske unije za kibernetičku sigurnost [31], napad putem ransomwarea je jedna od 10 najvećih prijetnji organizacijama širom svijeta, uključujući i pomorske organizacije. Ova vrsta prijetnje može biti usmjerena i na tradicionalne organizacijske IT sustave kao i kritične IT i OT sustave broda i tako ugroziti sigurnost plovila, posade i morskog okoliša. Primjer takvog napada je ometanja i lažiranja GPS sustava pri tome je ugrožena sigurnost plovidbe [29].

Uobičajeni profil aktera prijetnji je [12]:

- Kibernetički kriminalci - organizirane kriminalne grupe koje posjeduju potrebna sredstva i znanje za provođenje ciljanih kibernetičkih napada.
- Komercijalni konkurenti - konkurencija koja nastoji doći do povjerljivih podataka ili poslovnih tajni.
- Nezadovoljni zaposlenici i kupci su česti akteri s motivom osvete.
- Aktivisti koji često djeluju na temelju osobne ideologije.
- Teroristi - ekstremističke skupine koje koriste kibernetičke napada u svrhu zastrašivanja, prisile ili ometanja mete kako bi postigli političke promjene, izazvali strah ili napravili fizičke štete.
- Država i sponzorirani akteri – grupe koje sponzorira vlada kako bi pristupili mrežama i sustavima drugih vlada ili industrija kako bi se ukrali, promijenili, oštetili ili izbrisali podatke.

Motivi kibernetičkih aktera da prijetnje provedu u napad na pomorsko okruženje i brod, prema istraživanju provedenom od strane Finskog udruženja brodara [3], mogu se sažeti u sljedeće kategorije:

- Politički, ideološki, tehnički i vojni motivi: akteri prijetnji kao što su aktivisti i države obično su motivirani političkim, ideološkim i vojnim ciljevima.
- Financijska dobit: Financijska motivacija je najčešći motiv za kibernetičke kriminalce, a ponekad i za komercijalne konkurente. Ovakvi akteri obično ne mare za određenu organizaciju nego samo žele što prije unovčiti ukradene informacije i podatke. Žrtve su, iako ne isključivo, organizacije visokog profila i loše kibernetičke sigurnosti.
- Zloglasnost ili reputacija: Pojedini akteri prijetnji motivirani su ugledom, slavom i pažnjom koju žele steći. Žrtve su organizacije visokog profila i loše kibernetičke sigurnosti.
- Osveta: Osveta je čest motiv među nezadovoljnim zaposlenicima s dovoljno znanja o sustavima, mrežama i obranama organizacije.
- Preklapanje motiva: U mnogim slučajevima postoji preklapanje motiva za aktera. Često je motiv za napad i osveta i financijska dobit.

Posljednjih godina financijski motivirani napadi su najčešći napadi i često su popraćeni organiziranim kriminalom kao glavnim oblikom prijetnje.

4.3. RANJIVOST BRODSKIH SUSTAVA

Ranjivi dijelovi sustava su hardver, softver, komunikacije, podaci, procesi i ljudi. Identifikacija uzroka ranjivosti je ključna za zaštitu sustava i sprečavanje napada. Digitalizacija brodova znači i veći broj priključaka, što posljedično povećava raspon kibernetičkih prijetnji. Nadalje, moderna informacijska oprema se može smatrati potencijalno visoko rizična sa stajališta informacijske sigurnosti jer mogu sadržavati veliku količine podataka koji se lako mogu izgubiti ili ukrasti.

Neki od uobičajenih uzroka kibernetičke ranjivosti brodskih sustava su [12]:

- Zastarjeli operacijski sustav: Zbog visokih troškova, brodari često odugovlače kad je riječ o nadogradnju svojih operativnih sustava. Ne ažurirani operativni sustav je laka meta zlonamjernih programa koji upada u mrežu broda. Microsoft Windows ili Linux operativni sustavi su, zbog jednostavnosti i kompatibilnosti, uobičajeni na brodskim računalima i kao takvi su plijen zlonamjernog softvera koji koriste njihove poznate ranjive točke.
- Uporaba neautoriziranih programa
- Zastarjeli ili nedostajući antivirusni program na klijentskim i poslužiteljskim računalima

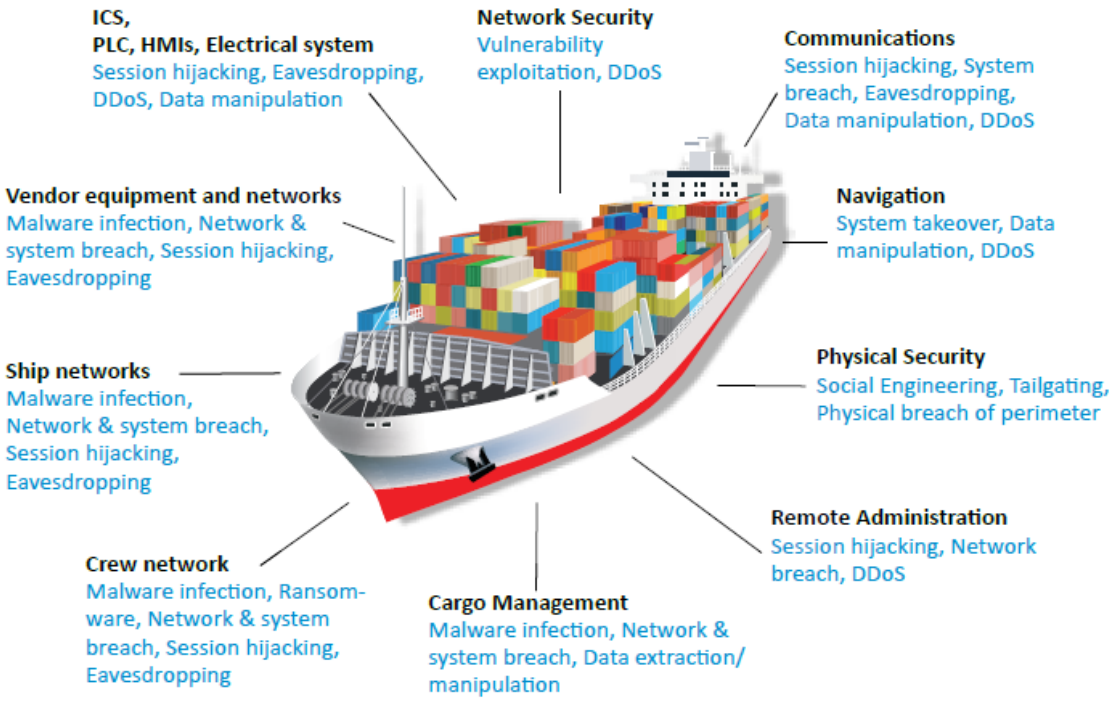
- Svaki zastarjeli uređaj ili onaj koji se ne koristi, a koji je povezana na OT mrežu broda česta je meta hakera. Ovi nesigurni uređaji su hakerima ulaz u brodsku mrežu te napadaju kritične i komunikacijske sustave.
- Brodska računalna mreža: Na brodovima računalna mreža je možda nezaštićena, nije dizajnirana tako da je otporna na kibernetičke napade. ili mreža nije segmentirana. Kao takva, mreža predstavlja rizik za brodske sustave kojima će napadač pristupiti putem nesigurnih veza i onda može nadzirati, ometati ili čak preuzeti kontrolu nad kritičnom opremom.
- Niska razina kontrole pristupa: Preslaba ili nepostojeća lozinka koja pruža pristup ili kontrolu nad upravljanjem sustava ili mrežom, korisnici s administrativnim ovlastima.
- Neažurni i slabi protokoli upravljanja mrežom koji se koriste bez enkripcije i tako omogućuju pristup lozinkama i nelegalno povezivanje s poslužiteljem.
- Nedostatak enkripcije i dvofaktornosti Ovjera: S porastom broja bežičnih pristupnih točaka na brodu lako se izgubi kontrola nad njima (kako su povezane i što je s povezano). Često nisu konfigurirane na odgovarajući način pa je razmjena poruka bez enkripcije i cijeli mrežni promet je onda ranjiv na presretanje i neovlašteno praćenje poruka. Pristup vašim bežičnim pristupnim točkama trebao bi biti ograničen na ovlaštene uređaje i osiguran snažnom enkripcijom.
- Nepostojan nadzor sustava u slučaju abnormalnog ponašanja: Iako mnoge tvrtke prikupljaju podatke o aktivnostima i ponašanju brodskih sustava, ne postoji osoblje koje je dovoljno obučeno/osposobljeno za provjeru tog sustava na abnormalne aktivnosti procedura ili planovi za izvanredne situacije.
- Sigurnosna kritična oprema ili sustavi koji su uvijek povezani s obalom: Komunikacija i izmjena poruka između ovih sustava je često bez enkripcije. Prenosi se čisti tekst koji je laka meta napadača koji mogu ukrasti ili izmijeniti podatke i tako preuzeti kontrolu nad sustavom.
- Nedostatak kontrole pristupa brodskim resursima za suradnike i davatelje usluga: Posljedica ovakvog nemara može biti gubitak podataka, propadanje opreme, ugrožavanje posade broda i okoliša.
- Pomorci obično koriste prijenosne diskove (USB memorije), pametne telefone i druge mobilne uređaje za prijenos podataka, koji mogu biti uzrok ranjivosti ako se priključe na brodski računalni sustav i mrežu.

Organizacijski uzroci leže u nepostojećim ili loše definiranim procesima. Ljudski uzroci su u greškama i propustima te neznanju. Pomorci često otvaraju elektroničku poštu od nepoznatog pošiljatelja ne znajući da sadrži potencijalno maliciozan sadržaj. Uzrok ranjivost može biti u nesavjesnom djelovanju pojedinca kada putem društvenih mreža dijeli podatke o kompaniji, brodu, posadi ili o poslu.

Prema IMO-u, 2017. najranjiviji brodski sustavi su [1]:

- Navigacijski most: Uz sve veću upotrebu elektroničke navigacijske opreme, ovi su sustavi podložniji kibernetičkom riziku, jer mnogi od njih komuniciraju s poslužiteljima na kopnu.
- Sustavi za rukovanje teretom: Sustavi koji se koriste za ukrcaj i iskrcaj tereta i njegovo upravljanje i kontrolu mogu biti ranjivi na kibernetičke napade jer su integrirani u brodske elektroničke podatkovne sustave.
- Sustavi upravljanja pogonom, strojevima i snagom: Budući da programi kontroliraju fizičke aktivnosti broda, mogu postati mete kibernetičkog napada i ugroziti kontrolu broda, posebno kada su povezani sa sustavima za daljinskim praćenjem stanja i integrirani s navigacijskim sustavima .
- Administrativni sustavi: Sustavi koji se koriste za upravljanje imovinom, ukrcajem, uobičajeni sustavi za obradu podataka o putnicima. Uređaji poput ručnih tableta, skenera i drugih prosljeđuju podatke koji se prikupljaju na poslužitelja koji može biti meta napada.
- Komunikacijski sustavi: Internet ili satelitski komunikacijski sustavi mogu povećati ranjivost brodskih sustava. Iako davatelji usluga imaju svoju obranu od kibernetičkih prijetnji, dobra praksa je ne oslanjati se samo na te mjere zaštite.

Na slici 3. prikazan su brodski sustavi i njihove ranjivosti u odnosu prema ciljanim kibernetičkim napadima. Gotovo svaki brodski sustav može bit napadnut i to sa više načina.



Slika 3. Povezani brodski sustavi podložni kibernetičkom napadu [3]

4.4. PRIMJERI IDENTIFICIRANIH NAPADA NA BRODOVE I LUKE

Točan broj pomorskih kibernetički napada nije poznat i može se smatrati da je mnogo veći od prijavljenih jer su napadi često neprimjetni ili kompanije ne žele objavljivati takve informacije kako ne bi ugrozile svoje poslovanje ili narušili povjerenje svojih klijenata. U novije vrijeme niz napada rezultirao je kršenjem podataka, sustava i opreme, kao i ozbiljnim financijskim gubicima. Ovisno o vrsti napada, posljedice variraju od lakših do umjerenih, primjerice u slučaju krađe podataka, dok se u slučaju preuzimanja kontrole nad cijelim brodskim sustavom, posljedice mogu biti katastrofalne [7]. Velike pošiljke tereta obično putuju tjednima preko oceana prije nego što stignu na svoje konačno odredište, što ih čini vrlo ranjivim na kibernetičke napade jer postoji dovoljno vremena da se uklone dokazi o napadu [1].

Nekoliko tvrtki koje pružaju sigurnost na brodovima koji plove kroz područje visokog rizika (*engl. High Risk Area - HRA*) bilo je podvrgnuto hakerskim napadima još 2011. Pirati su uspješno pristupili osjetljivim podacima o kretanju broda, njihovom teretu i osiguranju. Koristeći to, mogli su planirati svoje daljnje radnje i zatražiti otkupninu. Svi ti napadi imali su isti scenarij, zlonamjerni programi korišteni su za snimanje svakog pritiska na tipkovnicu i slanje podataka dalje prema e-porukama pirata [26].

Luka Antwerpen u Belgiji bila je pod hakerskim napadima koje su počinili sofisticirani krijumčari droge u razdoblju od 2011. do 2013. Koristeći zlonamjerne programe hakeri su

uspješno otkrivali gdje se nalaze kontejneri s narkoticima. Poslije su slali vlastite vozače da pokupe robu prije nego što dođe pravi vlasnik. Lučke vlasti su shvatile da se nešto događa netom nakon što su cijeli kontejneri počeli nestajati iz luka [27].

Unatoč činjenici da je glavna svrha AIS-a povećanje sigurnosti, lakša identifikacija i komunikacija na moru, sustav ima mnogo nedostataka, posebno u pogledu kibernetičke sigurnosti jer je potpuno kibernetički nezaštićen. Provedeni su testovi kako bi se potvrdili takvi problemi, tijekom kojih su generirani lažni AIS simboli na raznim mjestima diljem svijeta. Posljedice koje mogu proizaći iz zlouporabe AIS-a su ogromne.

Grupa studenata uspješno je otkrila slabosti i nesavršenosti GPS sustava 2013. kada su hakirali GPS signal na privatnoj jahti i distribuirali lažne podatke o položaju prema navigacijskoj opremi. Kako je pilot na stazi bio aktivan, pokrenuta je automatska korekcija kursa kako bi se jahta vratila na rutu. Ometanje GPS signala može uzrokovati velike probleme za navigaciju i pozicioniranje, kako na obali tako i na moru. Kako je GPS pod kontrolom SAD-a, predstavnici Bijele kuće uputili su upozorenje Sjevernoj Koreji, zbog snažnog ometanja u gradu Seulu. U to vrijeme širenje jakih radio valova uzrokovalo je mnogo problema zrakoplovima koji su letjeli iznad pogođenog područja [29].

U 2014. hakeri su koristili zlonamjerni program kako bi isključili naftnu platformu i potpuno je onemogućili na period od 19 dana što je uzrokovalo ogromne financijske posljedice i pokazalo ranjivosti sustava [21].

U lipnju 2017. najveći kontejnerski operater na svijetu *Maersk* pretrpio je veliki kibernetički napad. Zlonamjerni program *NotPetya* napravio je veliku štetu, i nužna je bila ponovna instalacija više od 4.000 poslužitelja i 45.000 računala. Tvrtka je bila prisiljena transportirati, utovariti i isprazniti kontejnere bez IT podrške 10 dana [23].

U ljeto 2017. godine kompanije *Svitzer* bila je žrtva krađe podataka, preko 5000 e-poruka s osobnim podacima preusmjereno je na vanjske adrese. Ugroženo je više od 400 djelatnika. Problem je zapažen 10 mjeseci nakon što je izveden napad, a zatim otklonjen u roku od 5 sati. Istraga je potvrdila da su poruke preusmjerene na vanjske adrese, ali kada su poštanski sandučići postali puni, e-poruke su se vraćale kao nedostavljene [30].

Gigantska tvrtka COSCO bila je žrtva zlonamjernog programa *NotPetya* u srpnju 2018. Tijekom napada onemogućeni su komunikacijski kanali, prvo u luci Long Beach, a potom i na cijelom teritoriju SAD-a [23].

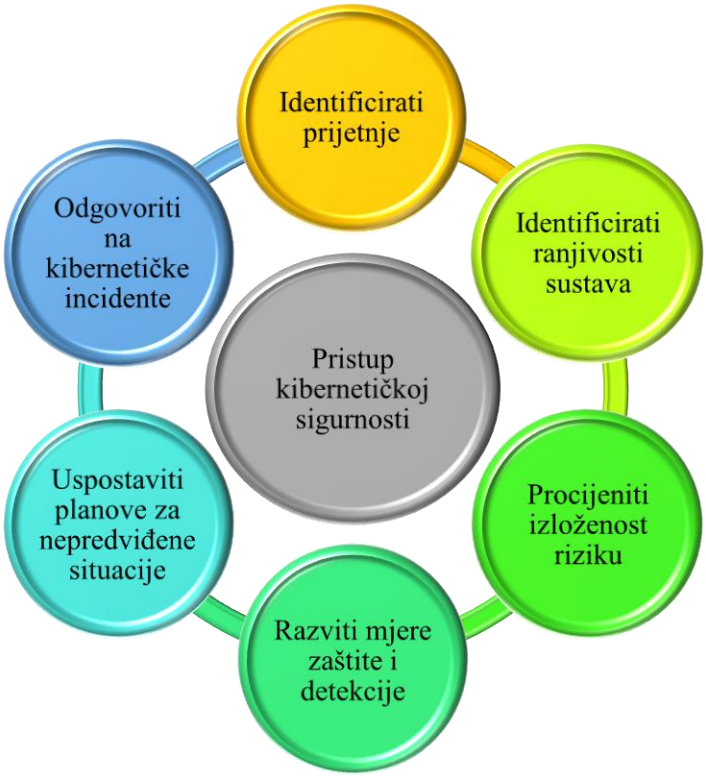
Najveća međunarodna brodska linija, Mediterranean Shipping Company, 2021. godine je imala prekid rada u podatkovnim centrima u Ženevi, Švicarska što je utjecalo na dostupnost nekih IT alata i web-mjesta [29].

5. PREPOPRUKE O MJERAMA KIBERNETIČKE SIGURNOSTI

Menadžment kibernetičke sigurnosti trebao bi [7]:

- definirati uloge i odgovornosti korisnika, ključnog osoblja i menadžmenta na kopnu i na brodu
- identificirati sustave, imovinu, podatke koji bi, ako se provale, mogli predstavljati prijetnju operacijama i sigurnosti broda
- provesti tehničke i proceduralne mjere za zaštitu od kibernetičkih incidenata i osigurati kontinuitet poslovanja
- provoditi aktivnosti za pripremu i reagiranje na kibernetičke incidente.

Neki aspekti upravljanja kibernetičkim rizikom mogu uključivati komercijalno osjetljive ili povjerljive informacije. Organizacije bi stoga trebale razmotriti zaštitu ovih informacija na odgovarajući način i koliko god je to moguće, ne uključuju osjetljive informacije u svoje poruke. Na slici 4. prikazan je pristup kibernetičkoj sigurnosti na temelju *Smjernica za upravljanje kibernetičkim rizicima* [12].



Slika 4. Pristup kibernetičkoj sigurnosti

Prikupljanjem informacija o potencijalnim prijetnjama i ranjivostima brodskog sustava, procjenom rizika napada brodskih sustava koji su potencijalna meta napadača, može se izgraditi konkretni pristup kibernetičkoj sigurnosti. Smjernice i/ili preporuke o mjerama kibernetička sigurnost odnose se na [6]:

- edukaciju zaposlenika
- sigurnost sustava i podataka
- arhitekturu mreže.

5.1. EDUKACIJA ZAPOSLENIKA

Nesavjesno osoblje je jedan od glavnih razloga povećanih kibernetičkih incidenata [7]. IMO smjernice (MSC-FAL.1 / Circ.3) naglašavaju da učinkovito upravljanje kibernetičkim rizikom trebalo bi započeti razvijanjem i osiguravanjem odgovarajućih razina svijest o kibernetičkom riziku na svim razinama organizacije. Svi zaposlenici, od višeg menadžmenta do posade bi trebali znati što znači kibernetička sigurnost i što mogu učiniti kako bi osigurali da njihovo kibernetičko okruženje bude sigurno. To se može postići obukom, tečajevima i webinarima, kao i internom komunikacijom s odgovornima za kibernetičku sigurnost u organizaciji.

Trenutno ne postoji obvezna obuka za kibernetičku sigurnost pomoraca prema Međunarodnoj konvenciji o standardima osposobljavanja, certificiranja i stražarstva pomoraca (STCW). Međutim, postoje zahtjevi u ISM kodeksu da osoblje treba biti kvalificirano za svoje zadatke [22]. Preporuka je da svi zaposlenici, i na brodu i na kopnu, prođu osnovni tečaj o kibernetičkoj sigurnosti što je podržano procedurama za upravljanje kibernetičkim rizicima organizacije. Svi članovi posade i osoblje broda trebali bi

- prepoznati prijetnje i kako odgovoriti na njih
- znati pokrenuti skeniranja virusa na svim datotekama i prijenosnim pogonima koji pristupaju brodskim računalima
- biti savjesni i otvarati samo e-pošte i privitak pošiljatelja koji su poznati i kojima se vjeruje
- prijaviti neobična ponašanja sustava
- znati što učiniti ako važni IT/OT sustavi ne rade
- znati gdje i kako dobiti pomoć.

Kibernetička sigurnost nije samo pitanje osoblja na brodu i kopnu nego i svih strana koji su uključeni u brodske sustave kao proizvođače i pružatelji usluga te i njih treba uključiti u edukaciju.

Posada broda mora imati jasne i koncizne postupke koji definiraju kako treba upravljati kibernetičkom sigurnošću broda. Treba se izraditi sljedeće procedure:

- Procedura o korištenju sustava i usluga na brodu
- Procedura upravljanja vanjskim medijima
- Procedura kako ažurirati i upravljati sustavima plovila
- Procedura o korištenju osobnih uređaja, mreže posade i interneta
- Procedura za daljinski pristup dobavljača
- Procedura za upravljanje incidentima kibernetičke sigurnosti
- Procedura o osposobljavanju članova posade za kibernetičku sigurnost.

5.2. SIGURNOST SUSTAVA I PODATAKA

Kako bi se osigurala kibernetička sigurnost broda i/ili ublažile posljedice kibernetičkih napada potrebno je osigurati sigurnost i pouzdanost podataka i procesa. Preporuke koje bi trebale osigurati sigurnost podataka i procesa su:

- Obnavljanje/oporavak podataka i/ili sustava: Programski alati za sigurnosno kopiranje trebaju biti dostupni kako bi se osiguralo da se sustav i podatci mogu oporaviti nakon kibernetičkog incidenta. Redovne sigurnosne kopije treba pohraniti na vanjski medij, namijenjen za tu svrhu, a ne spremati u poslovnoj mreži. U slučaju incidenta, sigurnosna kopija spremljena na zaraženo računalo bit će izgubljeno ili šifrirana kao i svaka druga datoteka.
- Sustavi koji imaju visoke zahtjeve za dostupnost podataka treba učiniti otpornim na napade. OT sustavi koji su od vitalnog značaja za sigurnu plovidbu i rad broda, treba imati sustave pričuvne pohrane podataka (backup) kako bi se brzo i sigurno vratile navigacijske i operativne mogućnosti broda nakon kibernetičkog napada.
- Kritični sustavi i uređaji broda ne bi smjeli biti dostupni putem Interneta. Većina pružatelja usluga nudi privatni IP adresni prostor kako bi spriječilo hakere da dođu do OT sustava na brodu putem interneta. Moguće je provjeriti jesu li uređaji broda javno dostupni tako da se unose IP adrese u preglednik i provjeri usmjerava li to do web sučelje uređaja.

- Ažuriranje administratorske lozinku na kritičnim sustavima i uređajima u OT mreži broda. Hakeri mogu brzo identificirati i pristupiti sustavima povezanim s internetom koji koriste zadane lozinke. to je imperativ promijeniti zadane lozinke proizvođača i ograničiti pristup kritičnim sustavima broda.
- Uspostavljanje sustava upravljanja korisničkim računima i ograničenje broja računa koji imaju pristup kritičnim sustavima broda. Implementacija procedure o sigurnoj lozinki može smanjiti rizik od kibernetičkog incidenta.
- Popis dopuštenih softvera
- Sigurnost aplikacijskog softvera: Instaliranim programima treba osigurati sigurnosna ažuriranja i održavanje sigurnosne konfiguracije hardvera. Ova ažuriranja ili zakrpe treba primijeniti ispravno i na vrijeme kako bi se osiguralo da se svi nedostaci u sustavu otklone prije nego što to iskoriste kibernetički napadači.
- Sigurni USB portovi na svim brodskim sustavima: Potrebno je zaključavanje/onemogućavanje USB pristupa kako bi se spriječio ulazak zlonamjernog programa u sustave broda. Ako se kritični sustavi mogu ažurirati samo pomoću USB, potrebno je takve USB ključeve čuvati na sigurnom mjestu.

Nadalje, važna je identifikacija nastanka incidenta kako bi spriječili širenje ili ga čak blokirali čim se identificira. Praćenjem i otkrivanjem anomalija i incidenata unutar sustava, tvrtka je u mogućnosti aktivirati mehanizme za ublažavanje kibernetičkih napada i odgovoriti na napad.

5.3. ARHIKTEKTURA MREŽE

Pri stvaranju optimizirane mrežne topologije koncept koji povećava otpornost mreže je segmentiranjem komponente. Mrežna segregacija je alat koji se koristi za podjelu mreže na manje dijelove kao pod mreže ili mrežni segmenti. Glavna svrha segregacije je ograničiti pristup mreži koji grupa korisnika ili bilo koji određeni uređaj može imati. Ovakva obrana je politika osiguranja informacija kojoj je namjera zaštititi u slučaju neuspjeha sigurnosne mjere ili ranjivosti iskorištene ljudskom ili mehaničkom pogreškom.

Tradicionalno, mreže na brodu bile su dizajnirane kao "ravne". Ravna mreža je dizajn računalne mreže s ciljem smanjenja troškova, održavanja i administracija. Ravne mreže smanjuju broj usmjerivača i prekidača računalne mreže spajanjem uređaja na jedan umjesto, a

ne više prekidača. Međutim, ravne mreže dolaze sa sigurnosnim rizicima jer nemaju međugranične pregrade koje se koriste za segmentiranje informacija mreže.

Provedbom segregacije mreže dizajnirani model mreže ima sposobnost osiguranja individualne zone vatrozidom i listama pristupa kontrole (*engl. Access control list*, ACL), koji pružaju kontrolu filtriranja unutar mreže i koji se regularno koriste kao sigurnosni mrežni parametri.

Važniji sustavi mreže koji trebaju bolju zaštitu bi se trebali nalazit što dublje unutar mrežne topologije. Važni ili kritični sustavi na brodu su uglavnom oni koji doprinose pogonu i navigaciji sustava. Uvođenjem zaštita poput vatrozida u svakoj zoni pristup automatskim sistemima unutar mreže može zahtijevati prolazak kroz više oblika prepreka. Vatrozidovi sadrže sigurnosna pravila koja upravljaju IP adresama koja smiju ili ne pristupati svakoj zoni. Procjenu rizika treba provoditi pojedinačno za svaku tvrtku kako bi se definirale jedinstvene potrebe za kritičnom zaštitom sustava.

Iako vatrozidi mogu biti vrlo korisni u zaštiti mreže oni mogu biti prekomjerno implementirani. Vatrozidovi koji nisu pažljivo konfigurirani mogu ograničiti ne samo sumnjivi već i legitiman promet i izazvati opasne posljedice za sustave. Ova ograničenja mogu spriječiti produktivnost, pa čak i potaknuti korisnike da pokušaju upotrijebiti backdoor kako bi mogli produktivnije raditi svoj posao. Nadalje, softverski bazirani vatrozidi imaju dodatnu neugodnost smanjenja ukupne izvedbe uređaja jer koriste snagu procesora i RAM memoriju što je u većini brodova luksuz koji ne postoji. Vatrozidi temeljeni na hardveru ne doživljavaju isti problem, međutim, oni su znatno skuplji i zahtijevaju posebno obučeno IT osoblje da ih instalira, konfigurira i održava na brodu.

5.4. MEĐUNARODNI PROPISI I SMJERNICE

Zabrinutost u vezi s kibernetičkom sigurnošću u pomorskom sektoru posljednjih je godina sve veća, zbog čega je Međunarodna pomorska organizacija (IMO) odlučila djelovati u ovom području, provodeći propise i dajući smjernice o tome kako spriječiti i djelovati u slučaju kibernetičkih napada [1].

Međunarodna pomorska organizacija je usvojila promjene Međunarodnoj konvenciji o zaštiti ljudskih života na moru (*engl. The International Convention for the Safety of Life at Sea – SOLAS Convention*) koje su potom usvojile ISM kodeks (engl. *International Management Code for the Safe Operation of Ships and for Pollution Prevention - ISM Code*) i ISPS kodeks (engl. *International Ship and Port Facility Security Code - ISPS Code*) [22].

Od važnijih smjernica i rezolucija imamo *Opću uredbu o zaštiti podataka* (engl. *General Data Protection Regulation, GDPR*) koja je stupila na snagu u svibnju 2018. napade [1]. Odbor za pomorsku sigurnost (engl. *Maritime Safety Committee, MSC*) i *Facilitation Committee* izdali su *Smjernice za upravljanje kibernetičkim rizikom u pomorstvu* (engl. *Guidelines on maritime cyber risk management*) kao odgovor na povećani broj kibernetičkih napada.

Time su brodske kompanije, pod SOLAS konvencijom, legalno obvezane za sigurnost koja se odnosi na radio i telekomunikacijske sustave, uključujući računalne sustave i mreže.

Za naglasiti je da pomorska industrija iako svjesna kibernetičke opasnost svojih brodova je isto tako ograničena internacionalnim zakonima od djelovanja izvan već navedenih okvira. Nadležna legalna tijela ne mogu pratit brzi razvoj kibernetičkog kriminala.

6. MOGUĆE POSLJEDICE KIBERNETIČKIH NAPADA BRODA

Veličina posljedica kibernetičkih napada ovisi o prirodi samih napada, složenosti scenarija i procedurama koje je industrija već uspostavila. Neki od mogućih posljedica napada u smislu sigurnosti, okoliša i ekonomskog utjecaja opisani su u nastavku.

6.1. SIGURNOST

Postoje mnogi sustavi, vrste opreme i razne tehnologije u pomorskoj industriji i brodovima, uključujući most, upravljanje teretom, nadzor brodskog pristupa, pogonski i komunikacijski sustavi i dr. koji ovise o elektroničkim sustavima. IMO putem Međunarodne konvencije za sigurnost života na moru (SOLAS) zahtijeva nošenje AIS-a i ECDIS-a i zahtijeva posjedovanje prijamnika za globalni navigacijski satelitski sustav. Međutim, neki od sigurnosnih rizika koji su prijavljeni su upravo u sustavu navigacijske opreme, kao što su AIS, ECDIS i GPS, koji su neophodni za navigaciju i pozicioniranje brodova. Iz tog razloga, ometanje ili prekid rada na bilo kojem od ovih bitnih navigacijskih sustava jest ozbiljan problem koji može utjecati na pomorsku industriju.

6.2. OKRUŽENJE

Zagađenje okoliša još je jedan potencijalni rizik povezan s kibernetičkom sigurnošću. Svake godine u more se izlijevaju dizel, nafta, benzin i druge otrovne kemikalije. Većina nesreća uključuje tankere, teglenice, platforme i benzinske stanice. Razlozi za izlijevanje nafte uključuju sudare plovila, prizemljenje, prijenos naftnog tereta, prelijevanje spremnika goriva i dr. Izlijevanje nafte u more može imati ozbiljne posljedice, uključujući štetu divljim životinjama, staništima i ekosustavima.

U pomorskoj industriji postoje mnogi rizici za okoliš, kao što su ispuštanje balastnih voda, kanalizacija i emisija plinova. Sva oprema ili uređaji na brodu koji reguliraju utovar, istovar i emisije, kontrolirani su elektroničkim sustavima, a ako je plovilo kibernetički napadnuto, sva ta oprema je ranjiva i može se koristiti za izvođenje kaznenih djela ili određene štete, što znači potencijalni rizik za okoliš i zdravlje ljudi. Osim toga, zaraze zlonamjernim programom dogodile su se na nekoliko *offshore* platformi posljednjih godina. Prema *Houston Chronicleu*, kibernetički napadači sa znanjem o naftnim platformama, rafinerijama, cjevovodima i tehnološkim sustavima mogu distribuirati zlonamjerni program u tim strukturama, što predstavlja katastrofalan scenarij i visoku razinu rizika za ljude i okoliš [31].

Pomorska industrija mora biti svjesna razornih učinaka koje kibernetički napadi mogu imati na brodarske kompanije, brodove, luke i pomorsku administraciju s katastrofalnim utjecajima na okoliš i posljedicama koje mogu rezultirati prekidom poslovanja, financijskim gubicima i učincima na ugled. Kako bi se sveli na najmanju moguću mjeru mogući negativni ishodi u smislu štete po okoliš, bitno je razviti i provesti robusne mjere i radnje kibernetičke sigurnosti [31].

6.3. EKONOMSKI UTJECAJ

Informacijska tehnologija jedan je od najvažnijih čimbenika u modernom poslovanju, ako poslovne informacije i sustavi nisu na odgovarajući način osigurani, sustav, podaci i informacije su podložni kibernetičkim napadima. Podaci i povjerljive informacije koje se kontinuirano razmjenjuju u pomorskom sektoru privlačni su kibernetičkim napadačima. Osim toga, posebni ekonomski rizici uključuju prekid poslovanja, oporavak informacija, popravak opreme i instalaciju sustava. Potrebne radnje za izbjegavanje budućih kibernetičkih incidenata označavaju značajno ulaganje u sustave kibernetičke sigurnosti za kompanije [5].

Danas gotovo sve kompanije koriste mreže, Internet i međusobno povezane sustave kao glavno sredstvo za poslovanje. Sve se radi *online*. Međutim, sve te operacije i aktivnosti mogu se nadzirati i ometati. U tom slučaju potrebna je zaštita od kibernetičkih napada kako bi se smanjile moguće ekonomske posljedice koje mogu izravno ili neizravno utjecati na pojedince, organizacije i društvo [5].

Druga relevantna ekonomska posljedica kibernetičkih napada je gubitak intelektualnog vlasništva, što je jedna od najvećih prijetnji poslovanju. Kompanije ulažu u sustave kibernetičke sigurnosti kako bi spriječile gubitak intelektualnog vlasništva. To znači da su mnoge kompanije značajno investirale u nove sustave i tehnologiju [31].

Kako bi se smanjile posljedice i potencijalni napadi potrebno je provesti procjenu rizika kako bi se razumjela prijetnja i razina rizika te izloženost i ranjivost svakog sustava i dijela opreme.

7. ZAKLJUČAK

Brodarska industrija kreće u svijet digitalizacije. Svakim danom tehnologija napreduje, a time i opasnost od kibernetičkih napada sve više raste. Brod je za kibernetički kriminal idealna meta budući da je putem računalnih sustava najlakše pristupiti infrastrukturi i posadi broda. Kako je sigurnost posade, putnika i ostalih osoba koje sudjeluju u pomorskom prometu ljudi najveći prioritet, potrebno je stalno raditi na razvijanju novih programa koji će se kvalitetno i efikasno suprotstaviti svakom obliku napada.

Kibernetičke prijetnje, brodovi, lučki terminali i drugi pomorski sustavi razvijaju se istovremeno, a negativni učinci kibernetičkih napada evidentni su ne samo na brodu, već i u mnogo širem sektoru uključujući brodarske kompanije, lučke terminale, sustave međupovezivanja itd.

Ključno je imati na umu da kibernetički napad na bilo koji brodski sustav može značajno utjecati na sigurnost pomorske plovidbe i navigacije, a potencijalni rizik napada brodskih sustava može imati katastrofalne posljedice za okoliš i zdravlje i sigurnost ljudi, sigurnost imovine i tereta na brodu. Sustavi na brodu koji reguliraju utovar, istovar tereta te emisije plinova kontrolirani su elektroničkim sustavima, a napadom na te sustave mogu se preuzetu podatci i/ili kontrola nad tim sustavima pa posljedično se može ispustiti velika količiae štetnih tekućina u more.

Pomorske organizacije i brodari trebali bi provesti plan procjene rizika kako bi se shvatila kibernetička prijetnja i razina rizika te identificirala ranjivost brodskih podsustava i opreme. Potrebno je da organizacije razviju procedure i strategiju oporavka nakon napada kako bi postigli kibernetičku sigurnosti koju propisuje IMO.

Osim toga, članovi brodske posade i osoblje na kopnu predstavljaju sve veću kibernetičku prijetnju i rizik od napada jer se često događa da posada na brodu, s minimalnim ili nikakvim znanjem o ovoj pojavi, otvara e-poštu od nepoznatog pošiljatelja, otvara poveznice u prilogu, šalje povjerljive informacije putem društvenih mreža ili ih pohranjuju na web mjestima, odnosno u oblacima. Na taj način sustav je izložen prijetnjama i otvoren za napad. Prema tome, potrebno je podići svijest o tome i pojačati razinu osposobljenosti posade i osoblja na kopnu o potencijalnim kibernetičkim prijetnjama i rizicima.

LITERATURA

[1] Alcaide, I.J.; Llave, G.L.: *Critical infrastructures cybersecurity and the maritime sector*, Transportation Research Procedia, 2020, Izd. 45, str. 547–554, URL: https://doi.org/10.1016/j.trpro.2020.03.058, (26.11.2021.)

[2] Bican, P.M.; Brem, A.: *Digital Business Model, Digital Transformation, Digital Entrepreneurship: Is There A Sustainable "Digital"?,* Sustainability, 2020, br. 12 (13), 5239. URL: 10.3390/su12135239, (25.11.2021.)

[3] Finish Maritime Cybersecurity Maturity – Maritime Cybersecurity Report, 2021, URL: https://www.huoltovarmuuskeskus.fi/files/d60cfd87d66aa5321cfc9e48dc76f8b5789603b3/maritime-cybersecurity-report.pdf, (15.02.2020)

[4] Ginter, A.: *Strengthen Your Cyber Security. Take a number of steps to achieve a comprenhensive and robust plan*, Chemical Processing, 2010, URL: https://www.chemicalprocessing.com/articles/2010/088/, (27.11.2021.)

[5] Jorgensen, R. N.: *Cyber Security Survey Shows More Action Is Needed In The Industry*, 2018, URL: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey, (15.02.2020)

[6] Lagouvardou, S.: *Maritime Cyber Security: concepts, problems and models*, Master Thesis, Technical University of Denmark, 2019, URL: https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/Lagouvardou_MScThesis_FINAL.pdf, (15.02.2020)

[7] Mraković, I.; Vojinović, R.: *Maritime Cyber Security Analysis – How to Reduce Threats?*, Transactions on Maritime Science, 2019, Izd. 8, br. 01, str. 132-139, URL: https://doi.org/10.7225/toms.v08.n01.013, (27.11.2021.)

[8] Nadeem, A.; Abedin, B.; Cerpa, N.; Chew, E.: *Digital Transformation & Digital Business Strategy in Electronic Commerce - The Role of Organizational Capabilities*, Journal of Theoretical and Applied Electronic Commerce Research, 2018, br. 13 (2). URL: 10.4067/S0718-18762018000200101, (26.11.2021.)

[9] Silgado, D. M.: *Cyber-attacks: a digital threat reality affecting the maritime industry*, The Maritime Commons: Digital Repository of the World Maritime University, Panama, 2018. URL: https://commons.wmu.se/all_dissertations/663/, (22.11.2021.)

[10] Silgado, D. M.: *Cyber-attacks: a digital threat reality affecting the maritime industry*, The Maritime Commons: Digital Repository of the World Maritime University, Panama, 2018. URL: https://commons.wmu.se/all_dissertations/663/, (22.11.2021.)

[11] Solesvik, M.Z.; Gausdal, A.H.; Czachorowski, K.V.: *Applying Blockchain Technology : Evidence from Norwegian Companies*, MDPI Sustainability, 2018, br. 10 (6). URL: https://doi.org/10.3390/su10061985, (26.11.2021.)

[12] The Guidelines on Cyber Security Onboard Ships, BIMCO Publications, 2021. URL: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships, (22.11.2021.)

[13] Yu, H. M.: *Decentralized Cyber Forces: Cyber Functions At The Operational And Tactical Levels*, Canadian Forces College, Canada, 2018.

[14] The importance of cybersecurity in the maritime industry, URL: https://marine-digital.com/article_importance_of_cybersecurity, (20.11.2021.)

[15] Tijan, E.; Jović, M.; Aksentijević, S.; Pucihar, A.: *Digital transformation in the maritime transport sector*, Technological Forecasting & Social Change, 2021, Izd. 170. URL: https://doi.org/10.1016/j.techfore.2021.120879, (25.11.2021.)

[16] 2020 'State of the Phish' - Security Awarness Training, Email Reporting More Critical as Targeted Attacks Slike. URL: https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical, (15.02.2020)

[17] Computer security resource center – cyber incident, URL: https://csrc.nist.gov/glossary/term/cyber_incident, (15.02.2022)

[18] Cyber Security: 6 common cyber risks affecting maritime industry, URL: https://safety4sea.com/cm-6-common-cyber-risks-affecting-maritime-industry/, (24.11.2021.)

[19] Cyber Security: Maritime Meets Cyber Security, URL: https://www.maritime-executive.com/blog/maritime-meets-cyber-security, (23.11.2021.)

[20] DBIR – 2021 Dana Breach Investigation Report, URL: https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/, (28.11.2021)

[21] Global shipping fleet exposed to hacking threat, Reuter, 2014, URL: https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423, (28.11.2021.)

[22] ISM CODE – Latest Updates, URL: https://safety4sea.com/cm-ism-code-latest-updates/, (15.02.2020)

[23] Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack, Bleeping Computer, 2018, URL: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/, (29.11.2021.)

[24] Microsoft – Windows XP Support Has Ended, 2014, URL: https://support.microsoft.com/en-us/windows/windows-xp-support-has-ended-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e, (15.02.2020)

[25] Network Outage Resolved - MSC Statement & FAQ, URL: https://www.msc.com/che/news/2020-april/network-outage-resolved, (7.12.2021.)

[26] Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry - Wave of cyber-attacks, 2012, URL: https://safety4sea.com/pirates-exploiting-cybersecurity-weaknesses-in-maritime-industry, (28.11.2021.)

[27] Police warning after drug traffickers' cyber-attack, BBC News, 2013, URL: http://www.bbc.co.uk/news/world-europe-24539417, (28.11.2021.)

[28] Seven cybersecurity trends for 2020, 2020. URL: https://safety4sea.com/seven-cybersecurity-trends-for-2020/, (24.11.2021.)

[29] State Department issues notice on North Korean jamming, URL: http://gpsworld.com/state-department-issues-notice-on-north-korean-jamming, (28.11.2021.)

[30] Svitzer employee details stolen in data breach affecting almost half of its Australian employees, ABC News, URL: https://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600, (28.11.2021.)

[31] Threat Landscape Report, Vol 1, CERT-EU, 2021, URL: https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

POPIS SLIKA

POPIS TABLICA

POPIS KRATICA

ACL (engl. *Access control list)*	liste pristupa kontrole
AI (engl. *Artificial intelligence*)	umjetna inteligencija
AIS	automatski identifikacijski sustav
BIMCO (engl. B*altic and International Maritime Council*)	Baltičko i Međunarodno pomorsko vijeća
DDoS (engl. *Distributed denial of service*)	distribuirani napad uskraćivanja usluge
DoS (engl. *Denial of service – DoS*)	uskraćivanje resursa
ECDIS (engl. *Chart Display and Information System*)	Elektronički prikaz navigacijskih karata i informacijskih sustava
EPIRB (engl. *Emergency Position Indicating Radio Beacon*)	uređaj za otkrivanje položaja
GDPR (engl. *General Data Protection Regulation*)	opća uredba o zaštiti podataka
HRA (engl. *High Risk Area*)	područje visokog rizika
ICS (engl. *Industrial Control System*)	industrijsko kontrolirani sustavi
IMO (engl. *International Maritime Organistion)*	Međunarodna pomorska organizacija
IoT (engl. *Internet of Things*)	Internet stvari
ISM (engl. *International Safety Management*)	Međunarodnog kodeksa upravljanja sigurnošću
ISPS (engl. I*nternational Ship and Port Facility Security Code*)	Međunarodni pravilnik o sigurnosnoj zaštiti brodova i luka
IT (engl. *Information Technologies*)	informacijske tehnologije
ITU (engl. *International Telecommunications Union*)	Međunarodna telekomunikacijska unija
MITM (engl. *Man in the Middle*)	osoba u pozadini
MSC (engl. *Maritime Safety Committee*)	Odbor za pomorsku sigurnost
OT (engl.*Operational Technologies)*	operativne tehnologije
SOLAS (engl. *International Convention for the Safety of Life at Sea*),	Međunarodna konvencija o zaštiti ljudskih života na moru
SSP (engl. *Ship security plan*)	Plan sigurnosti broda
VDR (engl. *Voyage Data Recorder*)	zapisivač o putovanju brodova
VR (engl. *Virtual reality*)	virtualna stvarnost