Kibernetička sigurnost u pomorskom sektoru

Sikimić, Roko

SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET U SPLITU

ROKO SIKIMIĆ

KIBERNETIČKA SIGURNOST U POMORSKOM SEKTORU

ZAVRŠNI RAD

SPLIT, 2022.

SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET U SPLITU

STUDIJ: PEIT

KIBERNETIČKA SIGURNOST U POMORSKOM SEKTORU

ZAVRŠNI RAD

MENTOR:

dr. sc. Anita Gudelj

STUDENT:

Roko Sikimić

(MB:0171277868)

SPLIT, 2022.

SAŽETAK

Cilj ovog završnog rada je prikazati stanje kibernetičke sigurnosti u pomorskom sektoru, izazove s kojim se suočava, ranjivosti kibernetičkih sustava, te strategija za poboljšanje. Fokus rada je na autonomnim i pametnim pomorskim sustavima. Pri izradi rada korištene su smjernice Međunarodne pomorske organizacije (eng. *International Maritime Organization, IMO*), te smjernice poduzeća i udruženja specijaliziranih za kibernetičku sigurnost. Analizirani su kibernetički i drugi česti napadi, poput socijalnog inženjeringa, "watering hole" i DDoS napada. Također su analizirane karakteristike, ranjivosti i slučajevi napada na razne brodske sustave, među kojima su važniji navigacijski, komunikacijski i pametni sustavi. Na kraju rada su analizirani incidenti, tj. slučajevi napada na pomorski sektor, koji uključuju sve od navedenih kibernetičkih napada. Za svaki napad, tehniku manipulacije i zlonamjernu tehnologiju postoje protumjere i sigurnosne strategije. Proučavanjem ovog rada, moguće je spojiti teoriju i lekcije naučene na napadima u prošlosti, da bih se izbjegli incidenti u budućnosti i postigao što manji rizik, uz što veću kibernetičku sigurnost.

Ključne riječi: *kibernetička sigurnost, izazovi, ranjivosti, strategije, autonomni sustavi, kibernetički napadi*

ABSTRACT

The goal of this thesis is to show the state of cybersecurity in the maritime sector, the challenges it faces, the vulnerabilities of cyber systems and the strategies for improvement. The focus is on autonomous and smart maritime systems. IMO guidelines were used, along with guidelines from companies and associations specialized in cybersecurity. Cybernetic and other common attacks were analyzed, including social engineering, watering hole and DDoS attacks. Characteristics, vulnerabilities and attacks on various ship systems were also analyzed, among which navigational, communication and smart systems are more important. At the end of this thesis, incidents, that is, attack cases on the maritime sector were analyzed. The cases include all the listed cybernetic attacks. For every attack, manipulation technique and malicious technology, there are countermeasures and security strategies. By studying this thesis, it is possible to connect the theory with lessons learned on past attacks, to avoid incidents in the future and accomplish the smallest possible risk factor, with as high cybersecurity as possible.

Keywords: *cybersecurity, challenges, vulnerabilites, strategies, autonomous systems, cyberattacks*

SADRŽAJ

1. UVOD

Pomorski prijevoz je ključan za ekonomsku održivost mnogih država svijeta. Porast globalne populacije, poboljšanje životnog standarda te ukidanje zabrane trgovanja, doprinose sve većem oslanjanju na transportnu industriju. Za tržišta koja zahtijevaju održiv razvoj, niske cijene, efikasnost i, od nedavno sve važnije, ekonomski prihvatljive operacije, pomorski sektor je zaslužan za prijevoz 90% svih dobara [10]. Moderni razvoji u područjima Internet stvari tehnologije (eng. *Internet of Things, IoT*), "Big Data" i umjetne inteligencije (eng. *Artificial Intelligence, AI*) omogućili su tranziciju u više digitalizirane pomorske infrastrukture, što je stvorilo potrebu za ispitivanjima u polju internet tehnologija. Nadalje, povezanost i ovisnost o pametnim uređajima je uzrokovala porast kibernetičkih zločina poput društvenog inženjeringa, krađe identiteta, te "spam" e-mailova. Zaštita integriteta automatiziranih i autonomnih sustava, te informacijskih tehnologija (eng. *Information Technology, IT*) i industrijskih tehnologija (operativnih) sustava (eng. *Operational Technology, OT*), koji su sastavan dio pomorskih infrastruktura, je nužna. Pomorstvo se sve više oslanja na digitalna rješenja za izvršavanje svakodnevnih zadaća, te će digitalizacija transformirati industriju.

Pomorski sektor je uvijek bio spor, u usporedbi s globalnim razvojem tehnologije, budući da svaki izum i uređaj mora biti odobren sa strane IMO-a i ostalih klasifikacijskih društava. Zbog sporijeg razvoja sektora, značajan broj pomoraca i ostalih zaposlenika u sektoru je ostao needuciran o informatičkoj i kibernetičkoj sigurnosti. Napadači preko svijeta iskorištavaju needucirane pojedince, koji predstavljaju jednu ranjivost industrije, da bi izvršili razne vrste kibernetičkih zločina. Pomorski sustavi su najčešće dizajnirani da spriječe predvidljive probleme, poput zamora materijala radi starosti i korištenja, ali ne i da spriječe djelovanje inteligentnih igrača, tj. napadača. Ne može postojati centralno upravljanje svih kibernetičkih sustava, svaki igrač mora upravljati svojom mrežom i sustavima, te se zaštiti od svih ostalih. Potrebno je da svi kojih se tiče sigurnost broda, brodskih mreža, sustava i osoblja, razumiju opasnost kibernetičkih napada. Također je potrebno da se uči na prijašnjim napadima i razumije da industrija ne može uspješno opstati u budućnosti, bez razumijevanja prijetnji koje budućnost donosi. Kibernetička sigurnost pretežito se bavi zaštitom informacijskih, industrijskih i operacijskih sustava, uz zaštitu podataka od neovlaštenih pristupa, manipulacije i povrede.

Kibernetička sigurnost se ugrubo može podijeliti na dvije grane: struktura i sigurnost brodske mreže, te ljudski faktor. Ovi aspekti biti će proučeni u ovom radu. Klasificirati i analizirati će se napadi u pomorskom sektoru. Opisat će se optimalne strategije za poboljšanje postojećih sigurnosnih mjera i planova za hitne slučajeve. Obradit će se rizične i učestale kibernetičke prijetnje pomorstvu. Podjela prijetnji će obuhvatiti sve od prijetnja posadi i ostalom osoblju, do prijetnji navigacijskim, autonomnim i drugim brodskim i lučkim sustavima. U 2. poglavlju bit će obrađeni najčešći i najopasniji kibernetički napadi u sektoru, te strategije koje se mogu koristiti protiv njih. U 3. poglavlju obradit će se kibernetička sigurnost i napadi na brodske navigacijske sustave, uz njihove prednosti i nedostatke, te potrebne sigurnosne mjere. U 4. poglavlju, bit će obrađeni autonomni i pametni sustavi. Obrada će se sastojati od kibernetičke sigurnosti i napada na daljinski upravljana plovila i potpuno autonomna plovila, uz pametne luke i obradu procesa digitalizacije. U 5. poglavlju, prije zaključka ovog rada, analizirat će se primjeri incidenata u sektoru. Analiza će rezultirati vrijednim zaključcima i metodama, u svrhu poboljšavanja kibernetičke sigurnosti u pomorskom sektoru.

2. KIBERNETIČKI NAPADI

Kibernetički napadi se generalno smatraju događajima u kojima napadači ciljaju kibernetičke, digitalne ili fizičke mete. Kibernetički sustavi su definirani kao sustavi koji integriraju računala s fizičkim komponentama, te su sve više prisutni u svim aspektima ljudskih života, gdje se razvijaju sve sofisticiraniji senzori, instrumenti, mreže i ugrađena računala [10]. Prijetnja kibernetičkih napada je razumljiva kada se uzme u obzir situacija ili scenarij u kojem kiberteroristi uzimaju kontrolu nad autonomnim vozilima u luci i koriste ih u svrhu napada lučkog osoblja ili oštećivanja lučke opreme. Još opasniji bi bio slučaj u kojem napadač preuzima pristup nad sustavima brodske navigacije, propulzije ili sustava balasta. Ukoliko bi brod bio namjerno nasukan na kritičnoj lokaciji, porast brodskih troškova, radi odgađanja i preusmjeravanja, bi bio ogroman, bez da se uzmu u obzir troškovi popravljanja oštećenih objekata.

Ako napadač preuzme kontrolu nad senzorima, mjerilima ili sustavima koji sadrže potencijalno opasne materijale, može doći do izlijevanja, eksplozija ili drugih nepoželjnih situacija. U konačnici, svi kibernetički napadi imaju fizičku metu, bilo to direktnim ili indirektnim napadom. Motivacija i ciljevi napadača, te njihove vještine i metode napada, mogu veoma varirati, kao što je prikazano u Slici 1. Nadalje, moguće je da se napadom na jedan brod ugrozi veći broj brodova, ako napadač zarazi brod mrežnim virusom. Da bi se ovo spriječilo, potrebno je zaraženi brod staviti pod karantenu, da bi se spriječilo spajanje na lučku mrežu, te time i samo širenje virusa. Stručnjaci kibernetičke sigurnosti se slažu u tome da je potrebno izolirati "bolesne" brodove i ostale objekte pomorskog sektora, od "zdravih". U nastavku su opisane vrste napada.

Tablica 1. Motivacija i ciljevi napadača [8]

Skupina	Motivacija
Slučajni napadači	• bez zlonamjernih motiva, ali također uzrokuju nenamjernu štetu kroz lošu sreću, nedostatak znanja ili brige. Čest primjer je umetanje zaraženih uređaja u brodske IT ili OT sustave.
Aktivisti (uključujući nezadovoljne zaposlenike)	• osveta • poremećaj poslovanja • medijska pozornost • oštećenje ugleda.
Kriminalci	• financijski dobitak • komercijalna špijunaža • industrijska špijunaža.
Oportunisti	• izazov • dobitak ugleda • financijski dobitak.
Države Državno sponzorirane organizacije Teroristi	• politički ili ideološki dobitak. Na primjer, (ne)kontrolirani poremećaj gospodarstava i kritičnih državnih infrastruktura • špijunaža • financijski dobitak • komercijalna špijunaža • industrijska špijunaža • komercijalni dobitak.

2.1. NAPAD USKRAĆIVANJA USLUGA

Jednom kada ciljani uređaj postane zaražen zlonamjernim softverom, on postane "bot", kojeg napadač može iskorištavati. Taj uređaj može postati dio jedne veće mreže "botova". S većom mrežom uređaja koji se mogu koristiti u razne svrhe, napadač ima resurse s kojima može izvršiti opasan napad. Te mreže "botova" ili "botnet" mogu se iskoristiti da bi se preopteretio ciljani server ili mreža, pomoću slanja prekomjerne količine podataka. Ovo je poznato kao DDoS napad, tj. raspodijeljeni napad uskraćivanjem resursa (eng. *Distributed Denial of Service, DDoS*). Sami "botovi" često nisu mete, te korisnici tih uređaja često nisu svjesni da su zaraženi zlonamjernim softverom i upravo zato su efikasan alat za DDoS napad. Neki od načina pomoću kojih se mogu smanjiti rizici ovakvih napada su da se isključe nepotrebni servisi koji su pokrenuti na uređaju i uspostavljanje kvalitetnih pravila pri korištenju vatrozida, te održavanje softvera i hardvera ažuriranima [10].

2.2. SOCIJALNI INŽENJERING

Sa svakim tehničkim uređajem, korisnici su uvijek najslabija karika u lancu sigurnosti. Ljudske akcije predstavljaju "rupu" u sigurnosti sustava, koja nikada ne može biti potpuno zakrpljena. Napad iznutra predstavlja najveću prijetnju sigurnosti, a najgori scenarij je slučaj u kojem unutrašnji napadač nije svjestan da je on taj, tj. da je korišten u takve svrhe. Socijalni inženjering je vještina manipuliranja jednom osobom ili grupom ljudi, u svrhu dobivanja podataka ili usluge, koju inače ne bih dobili. Na primjer, većina ljudi neće dati svoju lozinku, ako su pitani direktno, ali će ju najčešće dati ako ih pita netko tko izgleda vjerodostojno, kao tehničar za podršku ili mrežni administrator. Socijalni inženjering se može podijeliti u dvije skupine, na temelju ljudi ili na temelju računala [10].

Inženjering na temelju ljudi se bazira na interakciji između ljudi, bilo to preko razgovora, e-mailova ili drugih načina preko kojih ljudi mogu komunicirati. Ove tehnike obično zahtijevaju fizički pristup ciljanoj lokaciji, koji se na primjer, može probati dobiti na sljedeći način. Napadač dođe do ciljane lokacije i tvrdi da je ostavio svoju identifikacijsku karticu kod kuće, te pita osobu s odgovarajućim autoritetom da im dopusti ulazak. Načini za prikupljanje podataka mogu biti jednostavni, poput traženja po kontejnerima. Pregledavajući odbačene papire i dokumentaciju moguće je pronaći lozinke, kontaktne podatke zaposlenika ili podatke o mreži firme.

Također je moguće da napadač zauzme ulogu važećeg korisnika, poput osobe za tehničku podršku, te uvjeri zaposlenika da mu da pristup službenom računalu firme. Napadač bi također mogao kontaktirati IT podršku, tvrdeći da je korisnik firme, te zatražiti resetiranje lozinke. Nadalje, moguće je dobiti podatke na način da napadač vidi korisnika kada se logira, bilo da promatra korisnika preko njegovih ramena ili sa veće udaljenosti, pomoću dalekozora. Prisluškivanje također može otkriti vrijedne podatke. Jedna poznata tehnika je obrnuti socijalni inženjering, gdje napadač manipulira metom u svrhu da meta kontaktira napadača. Na ovaj način meta više vjeruje napadaču, uspoređeno s situacijom gdje napadač kontaktira metu. Na primjer, napadač pošalje mail skupini korisnika, upozoravajući ih o mrežnim poteškoćama sutradan, te priloži broj tehničke podrške u slučaju da im se dogode spomenute poteškoće. Sljedeći dan, napadač obavi jednostavan DDoS napad na mrežu mete i čeka da ga korisnici nazovu. Tada ih zatraži podatke za prijavu, tj. korisničko ime ili e-mail mete i lozinku, tako da može razriješiti problem i time dobije pristup podacima firme.

Socijalni inženjering se izvodi pomoću računala ili drugih uređaja za obradu podataka. Ovi napadi mogu uključivati specijalno izrađene skočne prozore, koji mogu biti specifično izrađeni da privuku pozornost određene mete, ako su dostupni podaci o zanimacijama, hobijima i slično, odabrane mete. Ovi prozori služe da navedu korisnika da klikne na njih, te pristupi lažnim web stranicama i lažnim mobilnim porukama, pomoću kojih se može prikupiti velik broj podataka, ako meta "zagrize" i unese podatke. Društvene mreže se također mogu iskoristiti u svrhu skupljanja podataka, da bi lažne poruke izgledale što sofisticiranije i vjerodostojnije [10].

2.3. PHISHING I SPEAR PHISHING NAPAD

"Phishing", što dolazi iz iskrivljenog oblika engleske riječi za pecanje ("fishing") podrazumijeva vrstu napada pri kojem se koriste e-mailovi, izrađeni da izgledaju pravilno. Ovi e-mailovi se sastoje od poveznica na lažne stranice ili za preuzimanje zlonamjernog sadržaja. E-mailovi mogu izgledati kao da su poslani sa strane neke banke, kreditne firme ili drugih legitimnih kompanija. U slučaju da korisnik klikne na poveznice, napadač dobiva sve podatke koje korisnik unese na lažnoj stranici. Ovakvi e-mailovi mogu biti stručno napravljeni, te i iskusni korisnici mogu biti prevareni.

Najbolja tehnika zaštite protiv phishing e-mailova je educirati korisnike kako ih prepoznati. Nabrojat će se nekoliko primjera kako se lažni e-mailovi mogu prepoznati:

- Sadržaj – čak i kada e-mail izgleda kao da ga je poslao netko poznat meti, ali sadržaj izgleda "van mjesta" ili je nešto čudno, sumnjivo oko sadržaja, potrebno je biti oprezan.
- Poruka – odmah se može prepoznati da se radi o lažnom e-mailu, ako e-mail nije specifično adresiran meti, ali sadrži poruku poput "Poštovani člane".
- Mobilni/Telefonski broj – ako e-mail sadrži broj mobitela ili telefona, potrebno je provjeriti ispravnost broja, ako meta u pitanju planira nazvati broj, što bi bilo bolje izbjeći.
- Pravopis i gramatika – e-mailovi od legitimnih poduzeća su uvijek napisani s pravilnim riječima i pravopisom.
- Hiperveze – potrebno je provjeriti poveznice prije nego se klikne na njih. Kada pokazivač miša lebdi iznad poveznice, pojavi se naziv web-stranice, na koju poveznica vodi.

Spear phishing napadi su naprednija, te opasnija vrsta phishing napada u industriji. U ovim slučajevima, napadač je sakupio podatke o žrtvi pomoću drugih metoda socijalnog inženjeringa. Osnovna ideja ostaje ista, napadač šalje e-mail koji sadrži poveznice na lažne stranice. Međutim, u ovom slučaju meta je pozdravljena s njihovim pravim imenom. E-mail sadrži ispravne podatke o meti, radi čega meta manje sumnja na ispravnost e-maila. Phishing napadi se ne obavljaju uvijek uz pomoć e-mailova. Društvene mreže su postale bitna platforma za izvršavanje ovakvih napada. Slučajevi poput lažnih poveznica na Facebook-u i drugim stranicama za komuniciranje nisu više rijetkost. Ove metode dozvoljavaju napadaču da sakupi podatke o meti, u svrhu izvršavanja spear phishing napada [10].

2.4. WATERING HOLE NAPAD

Watering hole napad, koji dolazi iz engleske riječi za pojilo, se bazira na iskorištavanju sigurnosnih rupa web-stranica. Napadač "zarazi" web-stranice koje određena grupa korisnika posjećuje, te ih time kompromitira.

Cilj je zaraziti računalo mete i dobiti mrežni pristup na lokaciji zaposlenja mete. Ovi napadi se većinom fokusiraju na legitimne, popularne web-stranice. Napadač prvo profilira svoju metu, koja je najčešće zaposlenik velikih poduzeća, grupa za ljudska prava ili državnih ureda, da bih ocijenio kakvu vrstu web-stranica meta posjećuje. Nadalje, napadač traži ranjivosti u spomenutim web-stranicama, te "ubrizgava" zlonamjerne JavaScript ili HTML programske kodove (eng. *HyperText Markup Language, HTML*). Ovi kodovi preusmjeravaju metu na zasebnu web-stranicu, na kojoj se zlonamjerni softver nalazi. Takva kompromitirana web-stranica je tada spremna da "zarazi" metu s zlonamjernim softverom, kada meta pristupi stranici. Watering hole napadi nisu česti, ali predstavljaju poprilično prijetnju, pošto ih je teško detektirati. Uobičajeno se koriste pri ciljanju visoko osiguranih organizacija, pomoću manje osiguranih zaposlenika, poslovnih partnera, povezanih servisa ili neosiguranih bežičnih mreža [10].

2.5. ZLONAMJERNI SOFTVER

Malware, engleska riječ za zlonamjerni softver, je u prošlosti samo bio nakupina digitalnih agenata ili jedinki, koji se sastoje od programskih kodova. Svrha im je bila zaraza uređaja i samoreplikacija, radi čega ih nije bio problem detektirati. Moderni malware može biti teško primijetiti, te je prosječno potrebno 188 dana od infekcije do detekcije. Razlog ovome je to što je malware sposoban mutirati, te može biti i ažuriran, da bih se izbjegla detekcija. Malware također može biti stvoren specifično protiv određenih pojedinaca ili organizacija. Ovaj zlonamjerni softver može biti prenesen pomoću "drive-by" preuzimanja, te na ovaj način korisnik nije svjestan da se malware preuzima, radi ranjivosti prisutne u operacijskim sustavima, web-preglednicima ili programima. Iskorištavajući ranjivosti prisutne u softveru, malware može prevariti aplikaciju, poput web-preglednika, da pokrene njegov kod. Jednom kada se računalo zarazi, malware počne osiguravati svoje preživljavanje na tom uređaju, pomoću raznih tehnika. Neke od tehnika su stvaranje "backdoora", preuzimanja "root" pristupa računalu i onesposobljivanja antivirusnog softvera.

Nakon toga, napadač može iskoristiti malware da preuzme kontrolu metinog uređaja i sakupi podatke. Međutim, ovakva komunikacija mora biti tajna, što se može realizirati pomoću enkriptirane komunikacije, cirkulacije prometa podataka ili pomoću "port hoppinga".

Tradicionalni vatrozidi koriste mrežne priključke i protokole radi identifikacije i filtriranja prometa podataka. Ova metoda nije efektivna protiv malwarea koji "skače" od jednog mrežnog priključka do drugog, dok ne pronađe otvoreni pristup, tj. vezu prema mreži. Vatrozid sljedeće generacije izvodi realističniju klasifikaciju prometa podataka, baziranu ne samo na mrežnim priključcima i protokolima, nego na kontinuiranom procesu analize programa, dekripcije, dekodiranja i heuristike. Pomoću ovih sposobnosti moguće je postepeno analizirati svaki sloj toka podataka, da bih se spoznao njegov pravi identitet. Sposobnost precizne analize nepoznatog prometa podataka, bez obzira na mrežne priključke i enkripciju, je definirajuća karakteristika vatrozida sljedeće generacije. Radi toga ima vrlo visoku vrijednost u borbi protiv naprednog zlonamjernog softvera, softverskih iskorištavanja i drugih sofisticiranih prijetnji [10].

3. KIBERNETIČKA SIGURNOST I NAVIGACIJSKI SUSTAVI

Što su sustavi više međusobno povezani, to je veći rizik, te su veće šanse da se sustavi međusobno zaraze. Brodski navigacijski sustavi se često međusobno potpomažu pri radu, te je vrlo moguće da sustav "zaražen" zlonamjernim softverom utječe na rad drugih sustava. Bilo da se radi o tome da "zaraženi" sustav prenese pogrešne podatke drugim sustavima ili da ih samo "zarazi", od velike je važnosti spriječiti napade na navigacijske sustave. Radi njihove međusobne povezanosti, posljedice mogu potencijalno biti katastrofalne. GPS i drugi globalni navigacijski satelitski sustavi (eng. *Global Navigation Satellite Systems, GNSS*) su osnovni elementi zaštite unutar pomorskog sektora. Postoji i ECDIS, koji je postao veoma bitan alat za navigaciju, obavezan za sva postojeća plovila od srpnja 2018. AIS je također obavezan za sva putnička i internacionalna plovila, preko 300 GT, od 2002. Svi ovi sustavi su podložni napadima, te je potrebno razumjeti kako funkcioniraju i kako smanjiti rizik, da ne dođe do zlouporabe.

3.1. GLOBALNI POZICIJSKI SUSTAV

Globalni pozicijski sustav (eng. *Global Positioning System, GPS*) je osnovan alat za određivanje položaja broda na otvorenom moru. On daje podatke o položaju mnogo navigacijskih sustava, što je potrebno za njihov pravilan rad. GPS signale nije teško nadjačati, pošto su relativno slabi i neenkriptirani. 2013. tim sa Sveučilišta u Texasu, u Austinu, proveo je test s ciljem zamjene GPS signala broda. Uspjeli su zamijeniti signal, s lažnim signalom, pomoću uređaja od 2000 dolara, tako da navigacijska oprema očitava da je brod skrenuo 3 stupnja s kursa [19]. Isti tim je radio na protumjerama ovakvih napada, te je osmislio zaštitni uređaj koji prikazuje zamjenu signala, s kratkim kašnjenjem. Pravi signal dolazi od različitih satelita, iz različitih smjerova, dok lažni signal najčešće dolazi iz samo jednog izvora. Namjerni napadi na GPS, te zamjene signala, uzrokovali su da oprema krivo prijavi ili izgubi lokaciju broda ili drugih brodova. U lipnju 2017., dogodio se veliki incident zamjene GPS signala u Crnom moru. Ciljani su brodovi ruske luke Novorossiysk, te je navigacijska oprema očitala da im se položaj pomakao 40 kilometara, na jedan ruski aerodrom.

Nuspojava zamjene signala je bila utjecaj na AIS navigacijske sustave, radi čega su sustavi prijavljivali posadi da se nalaze na aerodromu, zajedno s desetak drugih brodova. Za ovaj incident se smatra da je rezultat ruske vježbe elektroničkog ratovanja [6]. Ovakvi incidenti se nastavljaju.

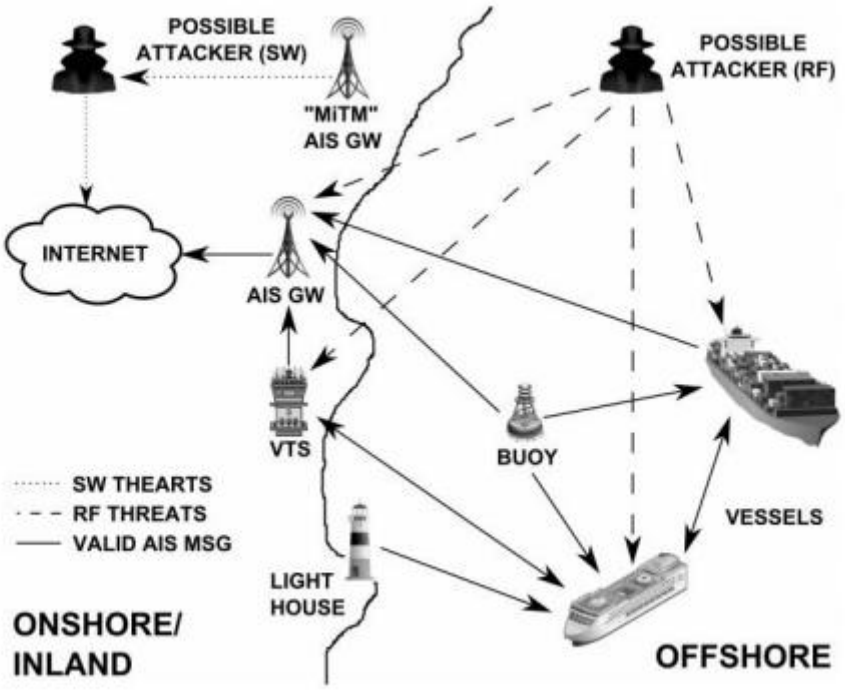
3.2. ELEKTRONIČKI PRIKAZ KARATA I INFORMACIJSKI SUSTAV

Elektronički prikaz karata i informacijski sustav (eng. *Electronic Chart Display and Information System, ECDIS*) je obavezan navigacijski alat koji u stvarnom vremenu daje geografske podatke ključne za rad brod. Reguliran sa strane IMO-a kao zamjena za papirnate nautičke grafove, ovaj sustav olakšava planiranje putovanja, pošto zahtijeva manje truda i manje vremena za izračun. ECDIS sustavi su u osnovi stolna računala, kod kojih zlonamjerna osoba s fizičkim pristupom računalu, može iskoristiti opću serijsku sabirnicu (eng. *Universal Serial Bus, USB*) za učitavanje krivih ili zastarjelih geografskih karti, pristupiti operativnom sustavu i raširiti zlonamjerni softver. Često su ovi sustavi pokrenuti s administratorskih pravima, te nisu zaštićeni lozinkama. S pozitivne strane, ECDIS najčešće nije spojen na internet, što znači da ne može biti zaražen s daljine. Nacionalni računalni centar u Manchesteru, tj. grupa NCC (eng. *National Computing Centre, NCC*) je provela istraživanje ranjivosti ECDIS-a. Ispitna okolina se sastojala od ECDIS "demo-a" jednog od većih proizvođača, s osnovnom konfiguracijom, te bez instaliranog vatrozida i antivirusnog softvera. Uspjeli su pretražiti i preuzeti sve podatke spremljene na računalu, te su mogli učitati, izbrisati i zamijeniti bilo koji podatak.
Također su pronađene druge ranjivosti.

3.3. AUTOMATSKI IDENTIFIKACIJSKI SUSTAV

Automatski identifikacijski sustav (eng. *Automatic Identification System, AIS*) je sustav za identifikaciju i pronalaženje plovila. AIS pomaže pri istraživanju nesreća i u operacijama potraga i spašavanja (eng. *Search And Rescue, SAR*), te nadopunjuje radar pri radu, koji ostaje kao glavni alat za uporabu pri izbjegavanju sudara. AIS je veoma koristan u slučajevima ograničene vidljivosti, te je učinio navigaciju sigurnijom, ali ima više sigurnosnih nedostataka. Sustav nema ugrađene mehanizme zaštite od kibernetičkih napada, što ga čini ranjivim prema vanjskim prijetnjama. 2013., firma za rješenja kibernetičke sigurnosti, TrendMicro, je prijavila više ranjivosti AIS sustava, od nedostatka verifikacije poruka, integriteta, autentifikacije, do nedostatka enkripcije [2].

Svatko s jeftinim radio prijemnikom može "prisluškivati" sustav, ovisno o udaljenosti. Napadi na AIS sustave veoma variraju, od napada gdje hakeri preuzmu podatke plovila, te promjene ključne parametre ili šalju lažne poruke, do napada gdje hakeri šalju lažne meteorološke prognoze posadi, mijenjaju točku najbližeg prilaska (eng. *Closest Point of Approach, CPA*), što veoma utječe na rutu broda. Čak i pomoću radio frekvencija se mogu napadati plovila, kopnene instalacije, te servisi za promet podataka između plovila.



Slika 1. Ispitivanje sigurnosti AIS sustava [2]

Pozitivna strana je to što se dobar broj ovih prijetnja može zaobići uspoređivajući podatke s drugim izvorima, poput radara i vizualnog promatranja. Više javnih web-stranica i "smartphone" aplikacija dopušta bilo kome da pronađe trenutačnu lokaciju bilo kojeg plovila koje odašilje svoje AIS podatke. IMO odbor za pomorsku sigurnost je upozorio na opasnosti curenja AIS podataka već 2004 [9]. Već tada su znali da objavljivanje takvih podataka na web-stranice ima potencijal za potkopavanje sigurnosti navigacije u pomorskom sektoru.

3.4. MJERE SIGURNOSTI

Svi navigacijski sustavi koji su obrađeni u poglavljima 3.1, 3.2 i 3.3, su integralni dio modernog pomorstva. Svaki sadrži pozitivne i negativne atribute, ali često na brodu negativni aspekti ovih sustava prevladavaju. Uz strateški izrađene mjere sigurnosti i kvalitetnu međuljudsku koordinaciju, može se puno postići na snižavanju rizika i opasnosti korištenja ovih sustava, nabrojati će se više primjera takvih sigurnosnih mjera:

Ovisnost o posadi:

- adekvatna i kontinuirana edukacija o kibernetičkoj sigurnosti
- razvoj politike kibernetičke sigurnosti.

Oslanjanje na tradicionalne alate:

- papirnati grafovi
- radar.

Plovila se moraju tretirati kao svaka druga mreža:

- sigurnosne revizije
- ispitivanje penetracije
- procjene fizičke sigurnosti.

Reakcija na incident:

- razvoj planova za nepredviđene slučajeve
- ispitivanja stresa
- procjena rizika.

Kibernetički rizici nisu nekontrolirani fenomen. Potrebno je imati kibernetički sustav koji je siguran, svjestan i otporan. Sustav mora imati kontrole, prioritiziranje po riziku, da bi se zaštitile ključne komponente. Potrebno je imati znanje o mogućim i rastućim rizicima, te situacijsku svijest, da bi se predvidjelo i prepoznalo štetno djelovanje. Uz to, potrebno je imati sposobnost oporavka od kibernetičkih napada i smanjivanja njihovih utjecaja, tj, posljedica.

4. AUTONOMNI I PAMETNI SUSTAVI

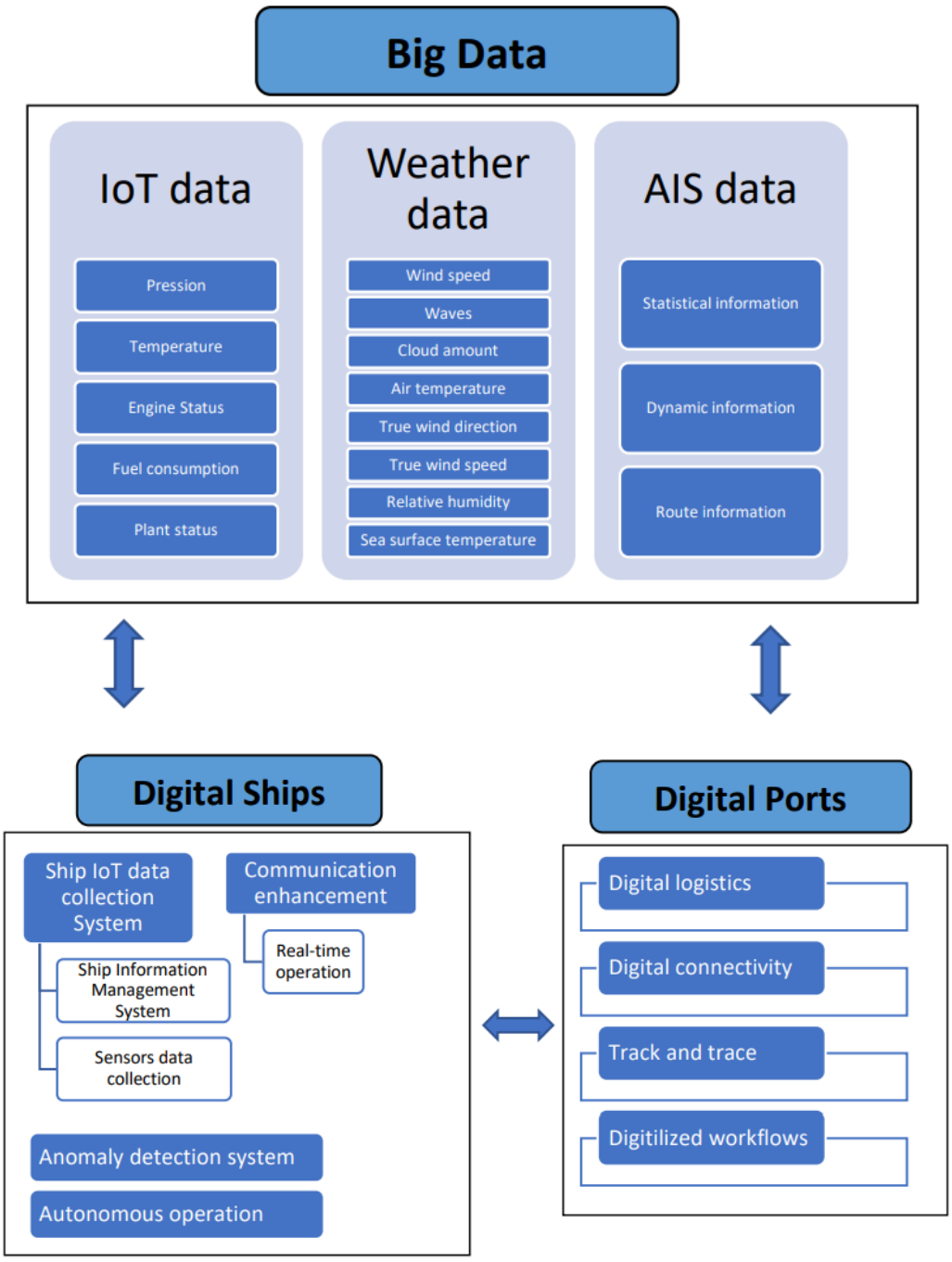
Autonomni sustavi i brodovi podrazumijevaju vrstu sustava koji su, u slučaju broda, sposobni upravljati samim sobom, tj. da umjetna inteligencija upravlja brodom. Za ovakve se brodove, te slične sustave, smatra da su budućnost pomorstva. Firma Rolls-Royce proučava mogućnosti zamjene standardnih plovila s autonomnim plovilima, u budućnosti. Također proučavaju i tehnološke, sigurnosne, zakonske i ekonomske aspekte autonomnih brodova. Tvrde da do 2035. mogu realizirati potpuno autonomno plovilo, spremno za oceansku plovidbu. S porastom korištenja automatizacije u lukama, operacijama ukrcaja/iskrcaja i u drugim pomorskim sustavima, veoma su se smanjili troškovi, te se povećala efikasnost u radu. Također nestaje mogućnost ljudskih greški, s aspekta redundancije i kontrolnih petlji.

Rastući trend u pomorskom sektoru je razvoj tzv. "pametnih luka", koje većinom koriste IoT. Pametne luke koriste mrežno spojene senzore za promatranje morskih mijena, struja, temperature, smjera i brzine vjetra, morske dubine, vidljivosti, dostupnosti pristaništa i niz drugih podataka. Sve ove podatke senzori šalju centralnoj nadzornoj ploči, gdje se podaci prosljeđuju povezanim plovilima. Ova vrsta sustava može optimizirati lučke operacije da bi se smanjilo vrijeme čekanja, vrijeme ukrcaja/iskrcaja i da bi se povećao broj plovila kojima se može efikasno upravljati, tako da uprave luki i brodara uštede značajne količine kapitala. Ovi sustavi su lakše primjenjivi na kopnu, u lukama, dok primjena na brodu, pogotovo na potpuno autonomnom brodu, sadržava veće izazove. Imati potpuno autonomno plovilo zahtijeva ogroman broj senzora koji moraju biti obrađeni računalnim sustavom, koji razumije pravila pomorskog prometa. Ideja da računalo obavlja sve navigacijske odluke, dok operater nadgleda više plovila sa udaljene kontrolne stanice, se smatra da je daleka i nerealna budućnost, ali u dolazećim desetljećima, nagli razvoj računala bih mogao ovo ostvariti.

4.1. DIGITALIZACIJA

Autonomni i pametni sustavi su ključni dio procesa digitalizacije pomorskog sektora. Postoje nepobitne prednosti sve prisutnije digitalizacije u sektoru, kao što je prikazano na Slici 3.

Poslovne prednosti koje pružaju aplikacije, pomoću kojih se može upravljati podacima, su transformacija većinski "analognih" operacija koje najčešće ovise o tradicionalnim tehnikama, u više optimizirane metode koje čine rukovanje teretom efikasnijim poslom. Također je prednost što se poboljšavanjem pomorske nabave i logističkih procesa, zrcale trendovi u mnogo drugih sektora, tj. industrija. Nadalje, digitalizacija pruža osnovu za poboljšanu efikasnost, rast, inovaciju, sigurnost i kompetitivnu prednost, dok minimalizira negativni utjecaj okoline.



Slika 2. Digitalizacija pomorske industrije [3].

Implementacija digitalizacije se oslanja na tehnologije poput "blockchaina" i "Big Data", upravljanja u stvarnom vremenu, AI-a, autonomnih vozila i robotike, mrežne povezanosti, komunikacija, virtualne realnosti (eng. *Virtual Reality, VR*) i IoT-a. Da bih se ubrzala prilagodba industrije na proces digitalizacije, potrebno je dijeliti znanje i iskustva među dioničarima prisutnima u industriji. To će rezultirati ispravnom provedbom novih metoda rada, optimizirajući korisnička sučelja i pružanje usluga.

Tri faze su predviđene da bi se postigao ovaj cilj: optimizacija, ekstenzija i transformacija, uz izazove koji uključuju sigurno financiranje, te istodobno upravljanje troškovima kibernetičke sigurnosti. "Big Data" i AI tehnologije su korištene da bih se dobila izvješća i smjernice budućih istraživanja. Ova izvješća i smjernice su stvorile mogućnost segmentiranja ili podjele procesa digitalizacije industrije. Proces je prvo podijeljen na pomorski prijevoz, lučke komunikacijske sustave i inovacije u pomorskom prijevozu. Nadalje, dijeli se na primjenu "Big Data" iz AIS-a, budući da se time može utjecati na nadzor, te ekološku i ekonomsku održivost. Proces se dalje dijeli na optimizaciju potrošnje energije, s fokusom na optimizaciju brzine, ruta i pozicioniranja dizalica. Konačno, proces se dijeli na prediktivnu analizu, iz razloga što se ona povezuje s performansama plovila, vizualnim nadzorom i drugim primjenjivim područjima. Morten Lind-Olsen, glavni izvršni ravnatelj (eng. *Chief Executive Officer, CEO*) Dualoga, poznate informatičke firme u pomorskom sektoru, uključio se u proces digitalizacije pomorskog sektora. Lind-Olsen se slaže s tezom da "Big Data" i AI nude održiva i dostižna rješenja za izazov digitalizacije pomorskog sektora, naglašavajući da će prihvaćanje IoT tehnologije pružiti poboljšanja u područjima prijevoza dobara i operacija flote [14]. AI će pomoći pri optimizaciji sigurnosti i procesa donošenja odluka.

Sve veći raspon u polju primjene robotike pridonijet će izvršavanju operacija u složenijim okolinama, te će biti integralni dio pojave bespilotnih plovila u pomorstvu. Migracija industrije na sve veće razine pametnih lučkih sustava i autonomnih plovila zahtijeva uspostavljanje novih protokola kibernetičke sigurnosti i poboljšanih metoda zaštite. Dokazi postoje da za svaku luku ili plovilo postoji rizik od kibernetičkih napada, ako ključni informacijski sustavi nisu adekvatno zaštićeni. Ovaj izazov je dalje pogoršan razvojem i korištenjem novih tehnologija, pošto one uzrokuju porast u broju mogućih ranjivosti u najbitnijim operacijskim infrastrukturama, tj. sustavima. Kao rezultat, izloženost povećanom riziku od neovlaštenih pristupa i novih vrsta kibernetičkih napada je pojačana. U budućnosti, među puno izazova koji će ostati, smatra se da će najbitniji biti razvoj plana standardizacije digitalnih usluga za autonomna plovila. Nadalje, novi standard sigurnosti, koji smanjuje broj i opseg kibernetičkih napada na autonomna plovila i pametne luke, morat će biti definiran radi ekonomske održivosti industrije.

4.2. PRIJETNJE AUTONOMNIM I PAMETNIM SUSTAVIMA

Kibernetička sigurnost je veoma bitna kod autonomnih i pametnih sustava, budući da zaštitni sklopovi nisu još ugrađeni u ove uređaje, radi čega su poznata meta mrežnih napada. Na primjer, ogromni DDoS napad na firmu Dyn, uslužitelje internetskih domena i e-maila, 2016., je uzrokovao "botnet". Automatizirana mreža za napad, koja se sastojala od više od 100,000 takvih uređaja [11]. Osim Rolls-Royce firme, organizacije poput Massterly-a, luke Long Beach-a i lučke kapetanije Singapura, uz druge, su uključene u razne inicijative i vijeća. Jedna od takvih je MUNIN inicijativa, koja se bavi istraživanjem i razvijanjem bespilotne navigacije u pomorstvu, pomoću inteligencije u mrežama (eng. *Maritime Unmanned Navigation through Intelligence in Networks, MUNIN*). Ove organizacije prate i rade na razvoju autonomnih i daljinski upravljanih plovila, te se slažu da "tehnologija koja bi uzdržala ovu razinu automatizacije je definitivno spremna, ali ono što nedostaje je dovoljno povjerenja, da ovi sustavi neće biti ugroženi mrežnim napadima" [1].

Rolls-Royce priznaje kibernetičke rizike i tvrde da bih bilo moguće preuzeti kontrolu nad plovilom, s udaljenosti, za zlonamjerne svrhe. Također znaju da postoji i mogućnost napada na AIS ili GPS sustave, kao što je spomenuto ranije u [19], [2], [9]. S ciljem minimaliziranja rizika, oni savjetuju iskorjenjivanje ranjivosti brodskih računala, te dodavanje zaštite i detekcije protiv uljeza. Sustavi moraju često biti ažurirani i podaci moraju biti enkriptirani i provjereni. Mjere su iste kao i kod standardnih plovila, budući da ipak ostaje faktor čovjeka i ljudskih greški, kada postoji udaljeni operater koji ima pristup brodskih sustavima.

4.2.1. PRIJETNJE DALJINSKI UPRAVLJANIM BRODOVIMA

Daljinski upravljani brodovi su slični potpuno autonomnim, sastoje se od ogromne mreže senzora i njima većinom upravljaju algoritmi koji interpretiraju primljene podatke, da bi implementirali preciznu navigaciju preko plovnih puteva. Proširene razine međusobne povezanosti, zauzvrat će izložiti velik broj novih prostora za napade u mrežama senzora, daljinskim kontrolama i komunikacijskim vezama između plovila i operatera koji daljinski upravljaju s obale [7]. Takvi dvosmjerni kanali su potrebni, budući da prenose struje podataka, ali su i izvor brige radi sigurnosti tih podataka, te ih je potrebno adekvatno zaštititi.

4.2.2. PRIJETNJE AUTONOMNO UPRAVLJANIM BRODOVIMA

Autonomno upravljani brodovi su manje podložni "standardnim" kibernetičkim napadima, poput onih gdje su ljudi uključeni u sami napad, npr. držanje posade taocima ili iskorištavanje komunikacijskih linkova posade radi napada na GPS sustav, te mijenjanje signala sustava. Zabrinutost radi povećanja broja kibernetičkih napada koji rezultiraju u sudarima brodova, s gubicima života, te ekološkoj šteti, postoji radi nedostataka u sustavima automatiziranih brodova. Nedostatci uključuju loše upravljanje sigurnosnim ključevima, dvosmjerne točke skladištenja i prikupljanje podataka s "oblaka". Ovi nedostaci omogućavaju napadačima uporabu raznih, novih vrsta napada.

4.3. PRIJETNJE IoT SUSTAVIMA U BRODOVIMA I LUKAMA

Napadi na IoT sustave najviše ovise o razini implementacije IoT tehnologije, u danom sustavu. Dizajn i način funkcioniranja komponenti, te samog sustava, uz protokole koje sustav koristi i područja gdje se primjenjuju, najviše određuju razinu implementacije ove tehnologije. Ranjivosti IoT sustava se mogu odrediti jedino ako se poznaju komponente sustava, međusobna ovisnost različitih komponenti, te njihove prednosti i nedostaci [5]. Napadi na IoT sustave se baziraju na iskorištavanju dijelova sustava, kako bi se dobio ovlašteni pristup, u cilju izmjene funkcioniranja sustava, krađe i kompromitiranja podataka. Potrebno je imati znanje o sustavu koje nam pomaže prepoznati potencijalne vrste napada, na koje bi sustav bio ranjiv, te primijeniti pravilnu protumjeru. Neki od mogućih vrsta napada su napadi na mrežni sloj sustava, pomoću iskorištavanja mogućih ranjivosti u protokolu mrežnog sloja. Napad na aplikacijski sloj sustava se odvija preko ranjivosti u protokolima aplikacijskog sloja, mana u dizajnu same mreže, te lošeg upravljanja pristupnim ključevima. IoT tehnologija također sadrži sigurnosne izazove radi svojih karakteristika dvosmjernog skladištenja podataka i tehnika prikupljanja podataka iz "oblaka" [18]. Jednom kada je ova tehnika pristupa i prikupljanja podataka kompromitirana, cijeli sustav je ugrožen. Jedan primjer IoT napada je LogicLoker, koji je "samo-širući ransomware crv", koji funkcionira pomoću programabilnih logičkih kontrolera (eng. *Programmable Logic Controller, PLC*).

Postoje i drugi primjeri, poput napada na sustave automatiziranih senzora spremnika ili sustave za nadzor, kontrolu i prikupljanje podataka (eng. *Supervisory Control and Data Acquisition, SCADA*), manje veličine. Ovi sustavi također koriste IoT tehnologiju, a služe za praćenje razine goriva u spremnicima, te pokretanje alarma u slučaju izlijevanja goriva [18].

5. ANALIZA PRIMJERA INCIDENATA

U ovom poglavlju analizirati će se primjeri incidenata pronađeni u smjernicama o kibernetičkoj sigurnosti od IMO-a. Ovi incidenti su anonimni, poznate su jedino okolnosti, te uzroci i posljedice incidenta. Analizom primjera incidenata u kojima je napadač na ikakav način oštetio ili ugrozio plovilo, posadu ili brodarsku tvrtku, mogu se izvući vrijedni podaci i zaključci, da bih se u budućnosti izbjegao incident u pitanju. Analizom je također moguće brže reagirati i oporaviti se od kibernetičkih incidenata, te je moguće poboljšati utjecaj i efikasnost strategija u slučaju hitnih slučajeva, tj. "contingency" planova. Moguće je doći do napretka i u drugim poljima zaštite od kibernetičkih napada, poput identifikacije prijetnji i ranjivosti, procjene rizika, razvoja sigurnosnih mjera, uspostavljanja odgovarajućih strategija i efikasnijeg djelovanja tijekom incidenata. U sljedećim podpoglavljima, analizirati će se različite vrste incidenata koji uključuju kibernetičke napade na pomorski sektor.

5.1. VIRUS OTKUPNINE

Brodovlasnik je prijavio da su poslovne mreže kompanije zaražene s virusom otkupnine ili "ransomware-om", navodno uzrokovanim privitkom e-pošte, koji je stvoren kao dio "phishing" napada. Izvor virusa su bila dva nesvjesna brodska agenta, u različitim lukama, koji su iskorišteni u svrhu širenja virusa. Virus je utjecao i na brodove, ali šteta je ograničena na poslovne mreže, dok su navigacija i brodske operacije ostali osigurani. U jednom slučaju, vlasnik je platio otkupninu, iako plaćanje nije uvijek preporučena strategija. Ovaj slučaj je važan jer prikazuje koliko je ključna kibernetička sigurnost preko cijelog pomorskog sektora, od brodara i agenata, do vjerodostojnih poslovnih partnera i proizvođača. Pokušaji pojedinaca da ojačaju svoje poduzeće od kibernetičkih napada su dobra strategija, ali često nedovoljna. Idealna strategija bi bila da svi uključeni u lanac opskrbe pomorskog sektora zajedno rade i dijele podatke međusobno, kako bi se smanjio rizik kibernetičkih napada.

5.2. NEPOZNATI ECDIS VIRUS

U novoizgrađenom teretnom brodu je pronađen virus u ECDIS sustavu, radi kojega je odgođena plovidba nekoliko dana. Brod je dizajniran za navigaciju bez papira, tj. potpuno digitaliziranu navigaciju, te nije bilo papirnatih karti i grafova na brodu. Neuspjeh ECDIS sustava je izgledao kao tehnički problem, te nije bio prepoznat kao kibernetički problem, sa strane kapetana i časnika. Tehničar proizvođačke firme je posjetio brod, te nakon dužeg vremena dijagnosticiranja problema, otkrio da su obje ECDIS mreže zaražene virusom. Virus je stavljen u karantenu i ECDIS računala su obnovljena. Izvor i način zaraze u ovom slučaju su nepoznati, a vremenski zaostaci u plovidbi i troškovi popravka su iznosili više stotina tisuća američkih dolara. Važnost ovog slučaja leži u tome da su apsolutno svi u pomorskom sektoru mete, ne samo luke i brodovi, koji su u većini slučajeva ciljani s strane napadača, nego i proizvođači brodske opreme, te je svu opremu potrebno detaljno pregledati prije korištenja.

5.3. KVAR SUSTAVA INTEGRIRANOG MOSTA

Brodu sa sustavom integriranog navigacijskog mosta dogodio se kvar skoro svih navigacijskih sustava, na moru, u području visokog prometa i smanjene vidljivosti. Posada je bila primorana koristiti samo jedan RADAR i rezervne papirnate grafove za navigaciju dva dana, dok nisu stigli u luku radi popravaka. Uzrok kvara svih ECDIS računala je dijagnosticiran kao posljedica zastarjelih operativnih sustava. Za vrijeme zadnjeg posjeta luci, tehnički predstavnik proizvođača je izvršio ažuriranje softvera navigacijske opreme. Međutim, zastarjeli operativni sustavi nisu bili sposobni pokretati novi softver i pokvarili su se. Brod je ostao u luci dok nova ECDIS računala nisu ugrađena i klasifikacijski inspektori nisu pregledali sve. Troškovi radi kašnjenja su bili veliki, te ih je morao razriješiti brodovlasnik. Važnost ovog incidenta leži u tome što naglašava kako nisu svi računalni kvarovi posljedica kibernetičkih napada i da se zastarjeli softver može pokvariti i biti uzrok opasne situacije. Detaljnije testiranje i češći pregledi softvera bi spriječili ovaj incident.

5.4. KVAR NAVIGACIJSKOG RAČUNALA

Brod je bio pilotiran kada su ECDIS računala i računala za kalkulaciju performansi plovidbe doživjela kvar. Pilot je bio na mostu. Kvarovi računala su odvukli pažnju časnicima straže, ali pilot i kapetan su uspjeli uz zajednički rad fokusirati tim na mostu, da bi se postigla sigurna navigacija pomoću vizualne identifikacije i radara. Kada su računala obnovljena, bilo je očito da su operativni sustavi zastarjeli i nepodržani potrebnim softverom. Kapetan je prijavio da su se računalni problemi ovog tipa često događali, te da su ponovljeni zahtjevi za servisiranje bili ignorirani sa strane brodovlasnika. Ovaj slučaj direktno prikazuje kolika je važnost servisiranja brodske opreme i uključenosti uprave u brodske probleme, da bih se spriječile kobnije situacije.

5.5. CRV VIRUS

Brod je bio opremljen sa sustavom upravljanja snage koji se mogao spojiti na internet, radi ažuriranja i popravljanja softvera, daljinske dijagnostike, sakupljanja podataka i daljinskog upravljanja. Brod je nedavno izrađen, ali ovaj sustav, po planu, još nije bio spojen na internet. IT odjel firme je donio odluku da će posjetiti brod i izvesti testiranja ranjivosti ovog sustava, da bi se utvrdilo da nema znakova infekcije sustava i da je sustav siguran za spajanje na internet. IT tim je otkrio "uspavanog" crv virusa, koji je sposoban aktivirati samog sebe u slučaju spajanja sustava na internet, što bi uzrokovalo drastične posljedice za brod.

Ovaj incident dobro naglašava da čak i sustavi sa zračnim razmakom mogu biti kompromitirani, te prikazuje koliko je važno imati proaktivan stav pri djelovanju s kibernetičkom sigurnošću i rizicima. Brodovlasnik je obavijestio proizvođače o otkriću virusa, te je zahtijevao procedure o eliminaciji crva. Brodovlasnik je tvrdio da je prije otkrića serviser bio na brodu, za kojeg se smatralo da je mogao uzrokovati infekciju. Crv se raširio pomoću USB-a u aktivni proces koji je sposoban izvršavati programe u memoriji. Ovaj program je dizajniran da komunicira sa svojim kontrolnim serverom, da bi dobio sljedeći niz naredbi za izvršavanje. Bio je čak sposoban stvarati datoteke i direktorije. Firma je zatražila profesionalce za kibernetičku sigurnost, da provedu forenzičku analizu i sanaciju. Saznali su da su svi serveri povezani s opremom bili zaraženi i da je virus ostao u sustavu neotkriven 875 dana. Alati za skeniranje su eliminirali virus, a analiza je pokazala da je serviser, na kojega se sumnjalo, uistinu bio izvor zaraze.

Crv je prenio zlonamjerni softver u brodske sustave pomoću USB-a, tijekom instalacije softvera. Analiza je također dokazala da je crv djelovao u memoriji sustava i aktivno "zvao" internet, sa servera. Budući da je crv učitan u memoriju, mogao je utjecati na performanse servera i sustava spojenih na internet.

5.6. NESVJESNA ZARAZA

Teretni brod je završio operacije bunkeriranja u luci. Mjernik bunkera je stigao na brod i zatražio dopuštenje da pristupi računalu u kontrolnom centru strojarnice (eng. *Engine Control Room, ECR*), radi printanja potrebnih dokumenata. Mjernik je priključio USB u računalo i nesvjesno prenio zlonamjerni softver na brodsku administrativnu mrežu. Softver nije primijećen, sve dok se kasnije nije proveo ispit kibernetičke sigurnosti na brodu i dok posada nije prijavila računalne probleme s poslovnim mrežama. Ovaj slučaj naglašava potrebu za procedurama pomoću kojih će se ograničiti ili zabraniti korištenje USB uređaja na brodu, uključujući one koji pripadaju posjetiteljima.

5.7. VIRUS OTKUPNINE NA POSLUŽITELJU APLIKACIJA

Virus otkupnine je zarazio glavnog poslužitelja aplikacija, što je uzrokovalo potpuni poremećaj IT infrastrukture. Virus je enkriptirao svaki kritični podatak na serveru i kao posljedica toga izgubljeni su osjetljivi podaci. Aplikacije potrebne za brodske administrativne operacije su bile neuporabljive. Incident se ponovio i nakon potpunog obnavljanja poslužitelja aplikacija. Uzrok infekcije je bila loša sigurnost lozinki, radi čega su napadači uspješno preuzeli kontrolu nad daljinski upravljanim servisima. IT odjel kompanije je deaktivirao nedokumentiranog korisnika, tj. napadača i postrožio mjere sigurnosti lozinki na brodskim sistemima, radi saniranja štete uzrokovane incidentom.

6. ZAKLJUČAK

Pomorstvo kao industrija napreduje sigurno, ali sporo, uspoređeno s drugim globalno zastupljenim industrijama. U procesu prilagodbe industrije na sve više digitaliziran i automatiziran svijet današnjice, ona je podložna različitim vrsta napada. Pozitivna posljedica modernih vrsta napada, poput kibernetičkih i drugih, je prilagodba i navikavanje industrije na njih. Sve više časnika širom svijeta je informatički educirano, čime se izbjegavaju male greške koje mogu snositi velike posljedice. Također, informatička educiranost časnika smanjuje rizik od svih vrsta napada koji su obrađeni u ovom radu. U 2. i 3. poglavlju se iz obrađenoga da zaključiti da napadači uspješno iskorištavaju industriju, koja još nije potpuno spremna na prijetnje koje tehnologije današnjice donose. Koliko god prednosti i funkcionalnosti imaju tehnologije današnjice i budućnosti, u koje spadaju autonomni sustavi, napredni AI, IoT, "Big Data", uz ostale, one donose sa sobom velik broj opasnosti. Nije dovoljno da samo časnici budu informatički educiraniji, potrebno je da svi uključeni u poslovanje industrije, od kopnenih branši, do plovila, budu educiraniji. Ovo obuhvaća razumijevanje vrsta napada koji se mogu dogoditi, tehnologija i sustava koji se koriste, te načina na koji se pojedinačna osoba može zaštiti. Kroz ovaj rad je prikazano u 2. i 5. poglavlju kako pojedinci mogu ugroziti čitava poduzeća, radi malih grešaka. Ako su svi educiraniji, rizici napada se drastično smanjuju, te neke vrste napada postaju veoma teške za izvršiti, budući da ovise o needuciranosti pomorca ili zaposlenika u pitanju.

Uz sve što se nabrojalo, ako su sigurnosne mjere i planovi za hitne slučajeve optimalno izrađeni preko cijele industrije, u puno boljem položaju se sama industrija nalazi u vidu spremnosti na budućnost, uz tehnologije i prijetnje koje ona donosi. Međutim, kao što je prikazano u nekim slučajevima analiziranima u 5. poglavlju, čak i uz potpunu spremnost posade i adekvatne sigurnosne mjere, moguće je da dođe do neke vrste napada, bilo da se radi o zaraženoj i neažuriranoj brodskoj opremi ili o prikrivenim napadačima. Još veće prijetnje postoje za autonomne i pametne sustave, koji su obrađeni u 4. poglavlju. Ovi sustavi su manje istraženi i primijenjeni od drugih, pošto još traje proces prilagodbe industrije na njih.

Nadalje, potrebno ih je dobro istražiti i izraditi odgovarajuće sigurnosne mjere za njih, jer su ovi sustavi osnova infrastrukture pomorske industrije sljedeće generacije. Ako ovi sustavi nisu adekvatno zaštićeni, to će rezultirati još sada nepoznatim posljedicama u budućnosti. Korištenje pametnih luka, IoT i pametnih sustava, te autonomnih i daljinski upravljanih brodova pruža mnoge prednosti, ali također stvara i mnoge prijetnje, kako poznate tako i trenutačno nepoznate. Primjenom ovih sustava u budućnosti, nestat će mnogo prijetnja prisutnih u sadašnjosti, ali će to uzrokovati stvaranje novih prijetnji. Uz analizu, diskusiju i primjenu određenih stavki obrađenih u ovom radu, moguće je spoznati teoriju i metode koje će pomoći pomorskom sektoru. Sve sa ciljem dostizanja uspješnije, stabilnije i sigurnije industrije, spremnije na budućnost i izazove koje donosi.

LITERATURA

[1] Babica, V.; Sceulovs, D.; Rustenova, E.: *Digitalization in Maritime Industry: Prospects and Pitfalls,* ICTE in Transportation and Logistics, LNITI, Springer, Berlin/Heidelberg, Germany, 2019, str. 20–27.

[2] Balduzzi, M.; Wilhoit, K.; Pasta, A.: *A Security Evaluation of AIS,* Trend Micro Research Paper, December. 2014. https://www.acsac.org/2014/program-final/oc_multifile/3/62.pdf (pristupljeno 06.03.2022).

[3] Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonović, I.; Bellekens, X.: *Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,* Information 2022, Ver.13, Izdanje 1, 2022. https://doi.org/10.3390/info13010022 (pristupljeno 10.4.2022).

[4] Deloitte.: *Cyber Security in the shipping industry,* Capital Link Cyprus Shipping Forum, 2019, https://globalmaritimehub.com/wp-content/uploads/attach_852.pdf (pristupljeno 15.04.2022).

[5] Dineva, K.; Atanasova, T.: *Security in IoT Systems,* In Proceedings of the 19th International Multidisciplinary Scientific GeoConference SGEM 2019., Volumen 19 Albena, Bulgaria, 28. June–7. July. 2019., str. 576–577.

[6] Goward, D.: *Mass GPS Spoofing Attack in Black Sea?,* The Maritime Executive. 11. July 2017. https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea, (pristupljeno 03.03.2022).

[7] Gu, Y.; Goez, J.C.; Guajardo, M.; Wallace, S.W.: *Autonomous vessels: State of the art and potential opportunities in logistics,* NHH Dept. of Business and Management Science, Discussion Paper No. 2019/6, July. 2019., str.1706–1739.

[8] ICS; IUMI; BIMCO; OCIMF; INTERTANKO; INTERCARGO; InterManager; WSC; SYBAss.: *The Guidelines on CyberSecurity onboard Ships,* IMO, Ver. 4, 2021. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf (pristupljeno 04.04.2022).

[9] IMO.: *AIS Transponders, Maritime Security-AIS Ship Data,* IMO Maritime Safety December. 2014., https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx (pristupljeno 06.03.2022).

[10] Jović, M.; Tijan, E.; Aksentijević, S.; Cišić, D.: *An Overview of Security Challenges Of Seaport IoT Systems,* In Proceedings of the 2019. 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May. 2019., str, 1349–1354.

[11] Kan, M.: *DDoS Attack on Dyn Came From 100,000 Infected Devices,* COMPUTERWORLD, 26. October. 2016. http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infecteddevices.html (pristupljeno 08.03.2022).

[12] Kessler, G.C.: *Cyber Security in the Maritime Domain*, USCG Proceedings of the Marine Safety & Security Counsil, 76(1), Proljeće 2019., https://commons.erau.edu/publication/1318 (pristupljeno 20.4.2022).

[13] Kuhn, K.: *Cyber Risk Management in the Maritime Transportation System,* Coast Guard Journal of Safety & Security at sea, Proceedings of the Marine Safety & Security Council, 75(1), U.S. Coast Guard, 5-12 2017., str. 65–69.

[14] Lind-Olsen, M.: *Digital Trends in The Maritime Industry*, Dualog, Tromso, Norway, 2019, https://www.dualog.com/blog/4-digital-trends-in-the-maritime-industry (pristupljeno 12.05.2022).

[15] Pajunen, N.: *Overview of Maritime Cybersecurity*, South-Eastern Finland University of Applied Sciences, 2017, http://www.theseus.fi/handle/10024/123045 (pristupljeno 02.05.2022).

[16] Palo Alto Networks.: *Cybersecurity for dummies,* John Wiley & Sons, Inc., 2. Izdanje, Palo Alto, California, 2016.

[17] Serpanos, D.: *The Cyber-Physical Systems Revolution*, Computer, Volumen 51(3), March. 2018., str. 70–73.

[18] Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J.: *A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services.* IEEE Commun. Surv. Tutor., Volumen 20, Izdanje 4, 12. July. 2018., str. 3453–3495.

[19] UTNews.: *Spoofing a Superyacht at Sea*, Cockrell School of Engineering, 30. July. 2013. https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea, (pristupljeno 03.03.2022.).

[20] Walker, M.: *Certified Ethical Hacker*, McGraw-Hill Osborne Media, Izdanje Har/Pa, USA, 9. April 2013.

[21] Wright, G.; Bacon, M.: *Watering hole attack*, TechTarget Search Security, 2015. URL: http://searchsecurity.techtarget.com/definition/watering-hole-attack (pristupljeno 1.4.2022).

POPIS TABLICA

POPIS SLIKA

POPIS KRATICA

AI (eng. *Artificial Intelligence*)	umjetna inteligencija
AIS (eng. *Automated Identification System*)	automatski identifikacijski sustav
CEO (eng. *Chief Executive Officer*)	glavni izvršni ravnatelj
CPA (eng. *Closest Point of Approach)*	najbliža točka pristupa
DDoS (eng. *Distributed Denial of Service*)	raspodijeljeno uskraćivanje resursa
ECDIS (eng. *Electronic Chart Display and Information System*)	elektronički prikaz karata i informacijski sustav
ECR (eng. *Engine Control Room*)	kontrolni centar strojarnice
GNSS (eng. *Global Navigation Satellite Systems)*	globalni navigacijski satelitski sustavi
GPS (eng. *Global Positioning System)*	globalni položajni sustav
GT (eng. *Gross Tonnage*)	bruto tonaža
HTML (eng. *HyperText Markup Language)*	prezentacijski jezik za izradu web stranica
IMO (eng. *International Maritime Organization*)	međunarodna pomorska organizacija
IoT (eng. *Internet of Things*)	internet stvari
IT (eng. *Information Technology)*	informacijske tehnologije
MUNIN (eng. *Maritime Unmanned Navigation through Intelligence in Networks*)	pomorska bespilotna navigacija putem inteligencije u mrežama
NCC (eng. *National Computing Centre*)	nacionalni računalni centar
OT (eng. *Operational Technology*)	operacijske tehnologije
PLC (eng. *Programmable Logic Controller*)	programabilni logički kontroler
SAR (eng. *Search and Rescue*)	potraga i spašavanje
SCADA (eng. *Supervisory Control and Data Acquisition*)	sustav za nazdor, kontrolu i prikupljanje podataka
URL (eng. *Uniform Resource Locator*)	usklađeni lokator sadržaja
USB (eng. *Universal Serial Bus*)	opća serijska sabirnica
VR (eng. *Virtual Reality*)	virtualna stvarnost