Kibernetička sigurnost u pomorstvu

Tijan, Marlena

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET

MARLENA TIJAN

KIBERNETIČKA SIGURNOST U POMORSTVU

ZAVRŠNI RAD

Rijeka, 2023.

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET

KIBERNETIČKA SIGURNOST U POMORSTVU

CYBER SECURITY IN MARITIME INDUSTRY

ZAVRŠNI RAD

Kolegij: Prometni sustavi

Mentor: doc. dr. sc. Dražen Žgaljić

Student/studentica: Marlena Tijan

Studijski smjer: Logistika i menadžment u pomorstvu i prometu

JMBAG: 0303079615

Rijeka, srpanj, 2023.

Student/studentica: Marlena Tijan

Studijski program: Logistika i menadžment u pomorstvu i prometu

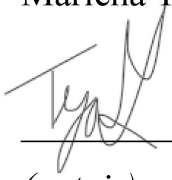
JMBAG: 0303079615

IZJAVA O SAMOSTALNOJ IZRADI ZAVRŠNOG RADA

Kojom izjavljujem da sam završni rad s naslovom Kibernetička sigurnost u pomorstvu izradila samostalno pod mentorstvom doc. dr. sc. Dražena Žgaljića U radu sam primijenila metodologiju izrade stručnog/znanstvenog rada i koristio/la literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo/la u završnom radu na uobičajen, standardan način citirao/la sam i povezao/la s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Studentica

Marlena Tijan



(potpis)

Student/studentica: Marlena Tijan

Studijski program: Logistika i menadžment u pomorstvu i prometu

JMBAG:0303079615

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Izjavljujem da kao student – autor završnog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Studentica - autor

(potpis)

SAŽETAK

S obzirom na napredak računalne tehnologije u pomorskoj industriji, primjetan je sve veći rizik od računalnih napada. Porast takvih napada zahtijeva uspostavu novih sigurnosnih standarda i pravila. Pomorska industrija privlači napadače zbog svoje uloge u trgovačkom prometu i visokih financijskih transakcija. Promjene u prijetnjama, uključujući terorističke i piratske napade, mijenjaju motivaciju napadača. Neprekidno napredovanje napadačkih tehnika dovodi u pitanje sigurnost sustava. Kako bi održala sigurnost, pomorska industrija treba ulagati u edukaciju kako bi povećala razinu informatičke pismenosti i osviještenosti o kibernetičkim prijetnjama. Iako je sigurnosni aspekt u pomorskom sektoru još uvijek u razvoju, ne smije se zanemariti.

Ključne riječi: kibernetičke prijetnje, napadi, sigurnost, ranjivost, strategije.

SUMMARY

Given the advancement of computer technology in the maritime industry, we are witnessing an increasing risk of cyber-attacks. The rise in such attacks calls for the establishment of new security standards and regulations. The maritime industry attracts attackers due to its involvement in trade activities and high-value financial transactions. Changing threats, including terrorist and pirate attacks, alter the motivation of attackers. The continuous advancement of attack techniques raises concerns about system security. To maintain security, the maritime industry needs to invest in education to enhance levels of digital literacy and awareness of cyber threats. While the security aspect in the maritime sector is still developing, it should not be overlooked.

Key words: cyber threats, attacks, safety, vulnerabilities, strategies.

1. UVOD

Razvojem računalnih tehnologija, računala su postala neizostavan dio svakodnevnog života, pružajući nam olakšanje u obavljanju različitih zadataka. Ovaj trend se također odražava i u industrijskom sektoru, gdje se računala koriste kao sredstvo za postizanje veće učinkovitosti. Internet, globalna podatkovna mreža, omogućuje nam povezivanje s udaljenim računalima i ostvarivanje komunikacije s njima.

Industrija također ima koristi od brzog razvoja računalne primjene. Uvođenjem rješenja u integrirane sustave na brodovima, pomorcima se olakšavaju svakodnevni poslovi. Automatizacija povećava razinu sigurnosti te sprječava sudare i druge događaje tijekom plovidbe. Međutim, ova veza također stvara novu prijetnju, kibernetičke napade. Koriste moderna znanja i tehnike kako bi napadali pomorsku industriju, koja je privlačna zbog svojih financijskih izgleda. Nedostatak edukacije o ovom obliku, sigurnosne prijetnje predstavlja dodatni problem.

U svrhu podizanja svijesti o ovim prijetnjama, istraživanje prati razvoj računalnih napada i njihovu primjenu. Tema ovog rada fokusira se na kibernetičke sigurnost u pomorskoj industriji, prijetnje, vrste napada te same ranjivosti tog sektora počevši te navode se određene mjere zaštite i procedure kojima se može osigurati određena razina zaštite počevši od drugog poglavlja i nastavljajući sve do zaključka.

2. KIBERNATIČKA SIGURNOST

Kibernetička sigurnost je zaštita računala, mobilnih uređaja, poslužitelja, elektroničkih sustava, podataka i mreža od zlonamjernih napada. Ovo je poznato kao informacijska sigurnost ili elektronička informacijska sigurnost. Pojam se odnosi na različite kontekste, od poslovanja do mobilnog računalstva, i može se podijeliti u nekoliko kategorija. U ovom području sigurnost je proces održavanja prihvatljive razine rizika kojem je sustav izložen. Prema ovom konceptu računalne sigurnosti, potrebno je implementirati određene zaštitne mjere kako bi se moglo obraniti od vanjskih i unutarnjih prijetnji. Informacijski i komunikacijski sektor ubrzava razvoj tehnologija, a time i količine podataka koji se njima prenose. U mnogim slučajevima, bez posebnih sigurnosnih protokola ili zaštitnih mjera, ovaj proces dovodi do povećanja potencijalnih kibernetičkih napada. Jedno od područja informacijske sigurnosti je osiguranje informacijske sigurnosti infrastruktura. Korištenjem specijaliziranog hardvera za održavanje mrežne sigurnosti, zlonamjerni se promet blokira radi zaštite određenih uređaja i softvera. Također, uspostavite način autorizacije kako bi pristup mreži imalo samo ovlašteno osoblje koje unošenjem odgovarajućeg imena i lozinke potvrđuje identitet korisnika.

2.1. RAZLIKA IZMEĐU IT I OT SUSTAVA

Kako se internet sve više koristi na sustavima i uređajima, kibernetička sigurnost postaje sve važnija tema u područjima informacijske tehnologije (IT) i operativnog inženjeringa (OT). Integracija IT i OT tehnologija i povezivanje računalnih mreža između IT i OT domena, uključujući korištenje komercijalnih informacijskih tehnologija u OT domeni, predstavljaju prijetnju sigurnosti prethodno zaštićenih OT sustava. Internetska komunikacija u IT i OT sustavima može se provoditi na dva načina: između uređaja i ljudi te između samih uređaja. ERP (Enterprise Resource Planning) koristi se za planiranje resursa poduzeća u području informacijske tehnologije (IT). MES (Manufacturing Execution Systems) predstavlja sloj između IT-a i OT-a za izvođenje proizvodnih aktivnosti. SCADA (Supervision and Data Acquisition) je računalni sustav za nadzor, prikupljanje podataka i administraciju sustava u OT području. Ova kombinacija IT-a i OT-a stvara okruženje u kojem je infrastruktura međusobno povezana, omogućujući velike protoke podataka i povećavajući broj korisnika koji komuniciraju. Međutim, nekontrolirano upravljanje i

neoperativnost ovih sustava može dovesti do tehničkih kvarova i predstavljati ozbiljnu prijetnju globalnoj sigurnosti.[1]

Stručnjaci i javnost ovim izazovima pristupaju na različite načine, a svaki prihvaća koncept kibernetičke sigurnosti. Područja industrijske upravljačke/operativne tehnologije (ICS/OT) i informacijske i komunikacijske tehnologije (ICT/IT) sve su više povezana i ovisna jedna o drugoj. Korištenje informacijske tehnologije u industriji postaje sve važnije i industrija podupire IT sektor opskrbom energijom iz različitih izvora. Ovi integracijski procesi su neizbježni i predstavljaju evoluciju poslovne prakse. Važno je pratiti IT trendove, prihvatiti nove poslovne modele i industrijske tehnologije kako bi se osigurao održivi razvoj i dugoročna konkurentnost energetskih kompanija. Razvoj sigurnosti energetskog sustava novi je izazov koji će u bliskoj budućnosti biti sve veći. Analiza postojećeg stanja i razumijevanje temeljnih načela informacijske sigurnosti u industriji provode se sukladno novim propisima. Uz sve veći broj cyber napada na ICS sustave, važno je poduzeti mjere za jačanje sigurnosti industrije. To uključuje zaštitu podataka radi održavanja njihove povjerljivosti i integriteta, osiguravanje mrežne sigurnosti radi zaštite IT mreže od zlonamjernih i ciljanih napada te zaštitu aplikacija i uređaja od prijetnji. Također je važno osigurati kontinuitet poslovanja i oporavak od katastrofe uspostavljanjem politika i procedura za ponovno uspostavljanje kontrole nad operacijama organizacije nakon katastrofalnog događaja. Kao dio programa informacijske sigurnosti, upravljanje rizikom također je ključno za sigurnost organizacije. Obuka o svijesti o sigurnosti igra važnu ulogu u osvještavanju ljudi o ranjivostima i sprječavanju slučajnog unošenja zlonamjernog softvera ili virusa u sigurne sustave.[2]

[1] Chwan-Hwa (John) Wu, J. David Irwin: „Introduction to computer networks and cybersecurity “, CRC Press, 2013.

[2] Cybersecurity for the maritime industry, https://www.maritime-cybersecurity.com/ (15. 6. 2023.)

3. UPRAVLJANJE KIBERNETIČKIM RIZICIMA

Pomorske kibernetičke prijetnje su prijetnje koje proizlaze iz sve veće upotrebe informacijskih sustava, mreža i tehnologija u pomorskom sektoru. Ove prijetnje proizlaze iz mogućnosti napada na računalne sustave, mreže i podatke vezane uz pomorske aktivnosti.

Kibernetički napadi na brodove mogu imati ozbiljne posljedice, uključujući prekid rada broda, gubitak povjerenja u sigurnost i integritet sustava te financijski gubitak. Evo nekoliko ključnih aspekata vezanih uz kibernetičke rizike u pomorstvu:

Napadi na sustave upravljanja brodovima (BMS):

BMS sustav upravlja vitalnim funkcijama plovila, uključujući navigaciju, upravljanje motorom, komunikacijske i sigurnosne sustave. Napadi na ove sustave mogu dovesti do gubitka kontrole nad brodom, sudara, kvara sigurnosnih mehanizama i mnogih drugih neočekivanih događaja.

Napadi na mreže brodova:

Kako brodovi postaju sve više povezani s vanjskim mrežama, uključujući pomorske komunikacijske mreže, satelitske veze i internet, napadi na te mreže mogu rezultirati prekidom komunikacije, presretanjem osjetljivih podataka, iskorištavanjem ranjivosti u brodskim sustavima i ovlaštenim neovlaštenim pristupom.

Fizički napadi na uređaje i sustave:

Naravno, pomorski napadi nisu ograničeni na virtualni svijet. Fizički pristup ugrađenim uređajima i sustavima može omogućiti napadačima da manipuliraju ili onesposobe kritične komponente kao što su senzori, instrumenti ili kontrolni sustavi.

Napadi na infrastrukturu pomorskih luka:

Napadi također mogu ciljati lučku infrastrukturu, uključujući sustave upravljanja lučkim operacijama, sustave inteligentnih kontejnera i upravljanje dokovima. Napadi na ove sustave mogu rezultirati prekidom teretnog prometa, gubitkom podataka, financijskim gubitkom i štetom za ugled same luke.

Socijalni inženjering i ljudski faktor:

Socijalni inženjering naširoko se koristi za manipulaciju osobljem u pomorskom sektoru i stvaranje rupa u sigurnosnom lancu. Nedostatak svijesti o kibernetičkim prijetnjama, loša

sigurnosna praksa, nedostatak obuke i nepažnja mogu dovesti do neovlaštenog pristupa sustavima i podacima. Za ublažavanje pomorskih kibernetičkih rizika važno je uspostaviti sustave upravljanja sigurnošću informacija, primijeniti najbolje prakse za zaštitu od kibernetičkih napada, obučiti osoblje o sigurnosnim prijetnjama i provoditi redovite procjene rizika. Također je važno voditi se relevantnim međunarodnim standardima i smjernicama, kao što su smjernice Međunarodne pomorske organizacije o pomorskoj kibernetičkoj sigurnosti. Upravljanje kibernetičkim rizicima u offshore liniji zahtijeva sveobuhvatan pristup informacijskoj sigurnosti i implementaciju odgovarajućih zaštitnih mjera.

Evo nekoliko koraka i strategija kako bi se omogućilo upravljanje kibernetičkim rizicima u pomorstvu:

Procjena rizika, čiji je prvi i najvažniji korak provođenje temeljite procjene rizika morskih luka, brodova i druge infrastrukture. Cilj je identificirati potencijalne prijetnje, ranjivosti i moguće posljedice samog napada kako bi se utvrdila razina rizika.

Politike i smjernice kibernetičke sigurnosti pokrivaju sve relevantne aspekte pomorskih operacija uključujući upravljanje brodovima, morske luke i komunikacijske mreže. Ove politike trebaju uključivati sigurnosne procedure, odgovornosti osoblja, sigurnosne protokole i upravljanje incidentima.

Tehničke mjere zaštite za smanjenje ranjivosti sustava i mreže. To uključuje korištenje vatrozida, antivirusnih programa, enkripcije podataka, ažuriranja softvera i hardvera te uspostavu robusnih mehanizama provjere autentičnosti i autorizacije.

Edukacija zaposlenika o kibernetičkim prijetnjama i sigurnosnim praksama bitan je dio upravljanja rizicima. Osoblje mora biti svjesno potencijalnih opasnosti, razumjeti sigurnosne postupke i biti osposobljeno za prepoznavanje i reagiranje na incidente.

Praćenje i nadzor sustava i mreža dizajniran je za otkrivanje neuobičajene aktivnosti, neovlaštenog pristupa ili drugog sumnjivog ponašanja. Alati za praćenje kao što su sustavi za otkrivanje upada i zapisnici događaja koriste se za prepoznavanje potencijalnih prijetnji u ranoj fazi.

Upravljanje incidentima uključuje definiranje uloga, postupke odgovora, obavještavanje dionika i oporavak od incidenata. Preporuča se da se provedba ovih planova redovito pregledava i prakticira kako bi svi bili spremni za hitne slučajeve.

Suradnja i partnerstva uključuju rad s relevantnim stručnjacima, organizacijama i institucijama za učinkovito upravljanje. Sudjelovanjem u međunarodnim inicijativama i razmjenom informacija o sigurnosnim prijetnjama poboljšava se sigurnost pomorskog sektora.

Upravljanje kibernetičkim rizicima u pomorskom sektoru treba stalno modernizirati i prilagođavati novim prijetnjama i tehnološkom razvoju. Redovita sigurnosna ažuriranja i usklađenost s novim smjernicama pomažu u zaštiti sustava i podataka od napada.

3.1. FAZE NAPADA

U 2019. prosječno vrijeme od proboja mreže do otkrivanja i saniranja napada bilo je 279 dana. Međutim, napad može ostati neotkriven godinama. Taj broj se povećao od 2018. godine kada je iznosio 266 dana. Vrijeme potrebno za pripremu kibernetičkog napada ovisi o motivaciji i ciljevima napadača, kao i o učinkovitosti tehničkih i proceduralnih mjera zaštite koje provodi tvrtka, uključujući one ugrađene.

Ciljani kibernetički napadi obično prolaze kroz sljedeće faze:

1) Pretraživanje/rekonstrukcija, gdje napadač koristi otvorene i javne izvore informacija, kao što su društveni mediji, za prikupljanje informacija o potencijalnim metama (kao što su tvrtke, brodovi ili članovi posade). Tehnički forumi, dokumenti i postovi mogu se koristiti za prepoznavanje tehničkih, proceduralnih i fizičkih ranjivosti. Ove informacije mogu se nadopuniti praćenjem stvarnih podataka koji ulaze i izlaze iz tvrtke ili broda.
2) Isporuka, gdje napadači ako pokušaju neovlašteno pristupiti sustavima i podacima tvrtke ili broda to mogu učiniti iznutra, unutar samog sustava, ili udaljeno putem internetske veze. Metode koje se koriste za dobivanje pristupa uključuju slanje zlonamjernih datoteka ili veza putem e-pošte osoblju tvrtke, pružanje zaraženih prijenosnih medija poput lažnih softverskih ažuriranja na brodu ili stvaranje lažnih web stranica koje prevarom prikupljaju podatke o korisničkim računima.
3) Proboj ovisi o ranjivosti koju je identificirao napadač i odabranoj metodi napada. Treba napomenuti da prekršaj ne smije rezultirati očitim promjenama u stanju objekta. Nakon kompromitacije, napadač bi mogao napraviti promjene koje utječu

na rad sustava, pristupiti, kopirati ili modificirati kritične informacije kao što su popisi tereta, popisi posade ili osjetljivi korporativni podaci.

4) Pomicanje je tehnika koja koristi već kompromitirani sustav za napad na druge sustave unutar iste mreže. U ovoj fazi, napadač može prenijeti alate, iskorištavanja i skripte u sustav kako bi podržao napade, otkrivao susjedne sustave kroz skeniranje mreže, instalirao trajne alate ili snimače tipkovnice kako bi održavao pristup sustavu te izveo nove napade na sustav.

Ove se informacije zatim mogu koristiti za omogućavanje prijevoza ilegalne robe, olakšavanje krađe, potpuno uskraćivanje poslovnih usluga i operativnih sustava, sudjelovanje u drugim kriminalnim aktivnostima kao što su hakiranje, krađa i prijevara, ometanje normalnog rada poduzeća i sustava (npr. npr. brisanje kritičnih informacija o prijavi/odjavi ili preopterećenje sustava tvrtke) i zahtjevi za otkupninom za operativne ili osobne podatke.[3]

3.2. VRSTE KIBERNETIČKIH PRIJETNJI

Postoje dvije kategorije kibernetičkih prijetnji koje mogu imati negativan utjecaj na tvrtke i brodove:

1. Neusmjereni napadi: Ovi napadi ciljaju različite tvrtke ili brodove među mnogim potencijalnim ciljevima. Alati i tehnike dostupni na internetu koriste se za pronalaženje i iskorištavanje uobičajenih ranjivosti.

Evo nekoliko primjera takvih napada:

- Malware: Zlonamjerni softver koji može pristupiti ili oštetiti računala bez znanja vlasnika. To može uključivati ransomware, trojance, spyware, crve i viruse. Ransomware kriptira podatke na sustavima i zahtijeva otkupninu za njihovo oslobađanje. Ovi napadi često iskorištavaju poznate ranjivosti i probleme u zastarjelom softveru.
- Water holing: Izrada lažnih web stranica ili kompromitiranje autentičnih web stranica kako bi se iskoristili posjetitelji.

[3] L. JENSEN: „Challenges in Maritime Cyber-Resilience“, Technology Innovation Management Review, 2015.

- Skeniranje: Pretraživanje velikog dijela interneta kako bi se pronašle ranjivosti koje se mogu iskoristiti.
- Typosquatting: Korištenje lažnih ili preusmjerenih URL-ova temeljenih na pogreškama koje korisnici često rade pri unosu web adresa.

2. Usmjereni napadi: Ovi napadi ciljaju određene tvrtke ili brodove kao mete ili kao jednu od mnogih meta. Koriste se alati i tehnike posebno razvijeni za određene organizacije.

   Evo nekoliko primjera takvih napada:

- Društveno inženjerstvo: Manipulacija ljudi kako bi prekršili sigurnosne postupke putem interakcije putem društvenih medija.
- Brute force: Napadi koji testiraju mnoge lozinke u nadi da će pronaći ispravnu.
- Pokušaji prijave s ukradenim pristupnim podacima ili često korištenim lozinkama.
- Napadi uskraćivanja usluge: Sprječavanje legitimnih korisnika pristupa informacijama preplavljivanjem mreže podacima.
- Phishing: Slanje e-pošte velikom broju korisnika u kojima se traže osjetljivi podaci ili se korisnici preusmjeravaju na lažne web stranice.

Nadalje, postoje i drugi napadi koji se neprestano razvijaju, poput krađe identiteta, ransomware-a, malware-a na mobilnim aplikacijama, socijalnog inženjeringa, prijetnji putem IoT uređaja, trojanaca, "čovjek u sredini" napada, distribuiranih napada uskraćivanja usluge (DDoS).

3.3. VRSTE KIBERNETIČKIH NAPADA

Postoje četiri glavne kategorije kibernetičkih napada:

1) Kibernetički kriminal su kriminalne aktivnosti koje se provode pomoću računala ili informacijske tehnologije spadaju u ovu kategoriju. Primjeri kibernetičkog kriminala uključuju prijevare u online bankarstvu, krađu identiteta, prijevare u online kupnji, itd. Kibernetički kriminal brzo je rastući globalni sektor organiziranog kriminala zbog svoje relativne anonimnosti i mogućnosti pokretanja napada s udaljenih lokacija.
2) Kibernetička špijunaža obuhvaća aktivnosti kojima se stječu tajne informacije bez dopuštenja oštećene strane. Često koristi u industriji kako bi se postigla konkurentska prednost istraživanjem proizvoda ili poslovnih strategija konkurencije. Također se

može koristiti u vojne svrhe kako bi se stekla informacijska prednost nad drugim zemljama.

3) Kibernetički terorizam je planirani i politički motivirani napad nacionalne skupine ili pojedinca. To mogu biti napadi na kritičnu infrastrukturu poput energetskih sustava ili financijskih institucija, stvarajući kaos i strah. Stjecanje sljedbenika putem interneta i društvenih medija također je oblik kibernetičkog terorizma.
4) Kibernetički rat podrazumijeva sukobe koji se vode putem računala i računalnih mreža i često uključuju države. To uključuje korištenje kibernetičkog terorizma, kibernetičke špijunaže i kibernetičkog kriminala kao sredstava za napad na protivnika. Cilj je steći informacijsku prednost nad protivnikom i oslabiti njegovu sposobnost djelovanja.

Ove navedene kategorije nisu međusobno isključive, već se zapravo često preklapaju. Napadači mogu koristiti različite tehnike i metode iz svih navedenih kategorija kako bi postigli svoje ciljeve. U svakom slučaju, zaštita i prevencija od kibernetičkih napada ključne su za očuvanje sigurnosti i integriteta informacijskih sustava.

Slika 1. Vrste napadača

Izvor: ***Cyber Attack Statistics and Trends***, https://www.embroker.com/blog/cyber-attack-statistics/, (27. 7. 2023.)

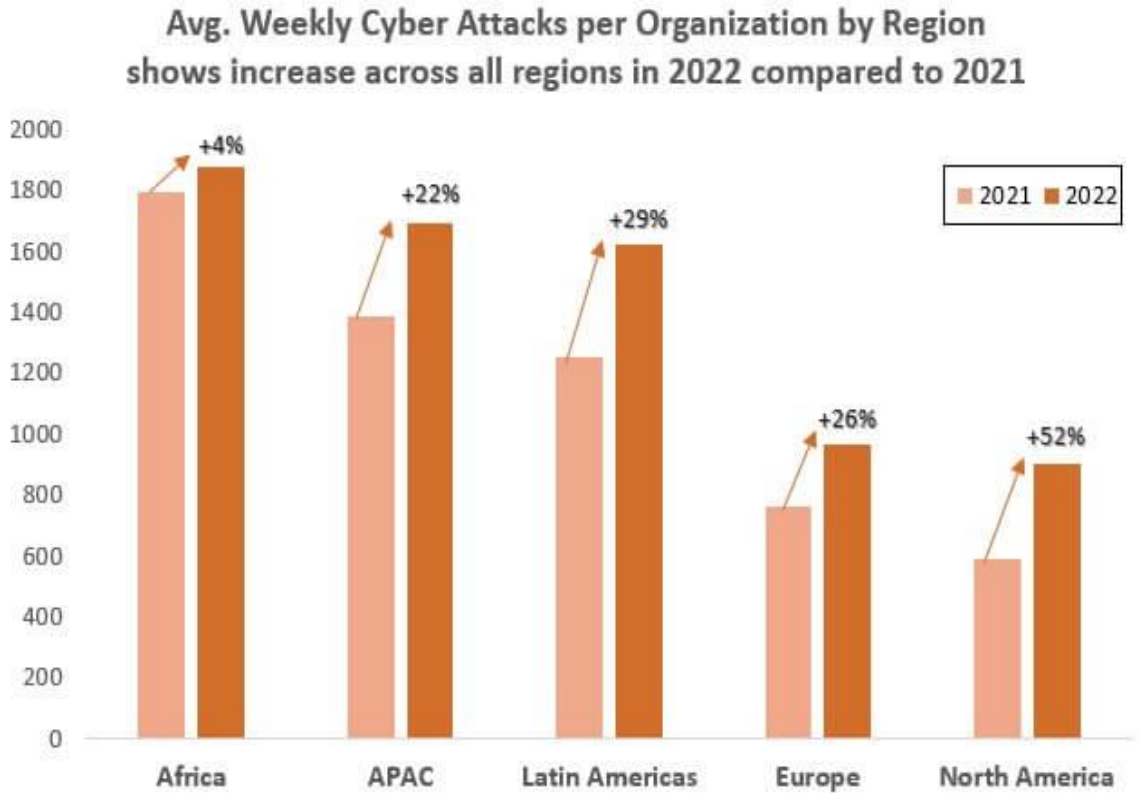
4. RANJIVOSTI KIBERNETIČKE SIGURNOSTI

Kibernetička sigurnost u pomorstvu ima nekoliko ranjivosti koje bi trebalo uzeti u obzir, a to su:

1) Zastarjeli informacijski sustavi jer mnoge pomorske organizacije i brodovi koriste zastarjele informacijske sustave koji nisu ažurirani s najnovijim sigurnosnim zakrpama. To ih čini podložnima poznatim ranjivostima i napadima.
2) Fizički pristup uređajima i infrastrukturi može predstavljati rizik. Neovlašteni pojedinci koji dobiju pristup brodovima, terminalima ili drugim pomorskim objektima mogu izvršiti napade ili instalirati zlonamjerni softver.
3) Slaba mrežna sigurnost je ranjiva na napade poput DDoS napada (distribuirani napadi uskraćivanja usluge), napada "Čovjek u sredini" (Man-in-the-Middle) ili presretanja komunikacije. Nedostatak adekvatnih sigurnosnih mjera na mrežnim komponentama može omogućiti neovlašteni pristup i manipulaciju podacima.
4) Nesigurne bežične mreže na brodovima ili u pomorskim lukama mogu biti ranjive na napade poput hakiranja, prisluškivanja ili krađe identiteta. Slaba autentifikacija ili loše konfigurirane bežične mreže mogu omogućiti napadačima pristup osjetljivim podacima ili upravljanje kritičnim sustavima.
5) Nedostatak svijesti i obuke o kibernetičkoj sigurnosti među pomorskim osobljem može rezultirati pogreškama i nepažnjom koje otvaraju vrata za napade. Osoblje bi trebalo biti educirano o sigurnosnim postupcima, prepoznavanju prijetnji i pravilnom korištenju tehnologije.
6) Nedovoljna zaštita podataka gdje osjetljivi podaci pohranjeni na brodovima ili u pomorskim lukama mogu biti izloženi riziku ako se ne primjenjuju adekvatne sigurnosne mjere. Slaba enkripcija, slab pristup kontroli i nedostatak sigurnosnih kopija podataka mogu olakšati krađu ili oštećenje podataka.[4]

Sve ove ranjivosti ističu važnost jačanja kibernetičke sigurnosti u pomorstvu putem ažuriranja sustava, uspostave snažnih sigurnosnih politika, implementacije sigurnosnih mjera, obuke osoblja i kontinuiranog praćenja i nadzora sigurnosnih postupaka.

[4] MITAGS Guide to Ship Cybersecurity https://www.mitags.org/guide-ship-cybersecurity/ (18. 5. 2023.)



Graf 1. Globalni kibernetički napadi kroz razdoblje 2021. i 2022. godine

Izvor: ***Check Point Research Reports,*** https://blog.checkpoint.com/wp-content/uploads/2023/01/sum2.jpg, (4. 7. 2023.)

4.1. PREUSMJERAVANJE NOVČANOG TOKA

Krajem 2014. godine pomorska industrija je doživjela značajan incident koji je uključivao velikog dobavljača goriva, World Fuel Services (WFS). Cilj napada bila je prijevara s prijenosom novca s ciljem izvlačenja novca na kriminalne račune. WFS je javno objavio da je bio žrtva napada koji je rezultirao gubitkom od gotovo 18 milijuna dolara. Sličan napad dogodio se krajem 2013.Godina u kojoj su pogođene najmanje tri tvrtke. Te su tvrtke mislile da plaćaju svojim dobavljačima goriva u Kini, no kriminalci su novac od transakcija ukrali na njihove vlastite račune. Tvrtke su zbog ovog napada pretrpjele gubitke od 1,65 milijuna američkih dolara. Napad napadača poznat je kao napad "čovjek u sredini", u kojem napadač prodire u komunikacijski kanal između dviju tvrtki. Svaka tvrtka vjeruje da komunicira izravno s ostalih, dok su zapravo obje komunicirale s kriminalcima. Da bi

pokrenuli takav napad, napadači su prvo morali prodrijeti u računalne sustave autora zlonamjernog softvera kako bi nadzirali tekuću komunikaciju. Ovaj incident jasno pokazuje ranjivost pomorskog sektora na kibernetičke napade i potrebu za jačanjem sigurnosnih mjera. Brodarske tvrtke moraju uložiti velike napore kako bi osigurale svoje IT sustave, nadzirale komunikacije i implementirale sigurnosne protokole za zaštitu od takvih napada.

4.2. ZOMBIE ZERO NAPAD

Tvrtka za kibernetičku sigurnost TrapX objavila je detalje napada nazvanog Zombie Zero. Ovaj napad koristio je zlonamjerni softver skriven u skenerima koje koriste logističke tvrtke za popis robe. Incident je potvrdilo osam različitih tvrtki, a malware je otkriven u 16 od 48 unaprijed instaliranih skenera. Nakon što je skener spojen na korporativnu mrežu, pokrenut je niz automatiziranih napada kako bi se pronašli poslužitelji koji u nazivu imaju riječ "finance". Nakon što je takav poslužitelj pronađen, osjetljive informacije su ukradene i poslane u kontrolne centre kojima su upravljali napadači. Ovaj napad naglašava ozbiljnost cyber prijetnji s kojima se organizacije suočavaju, čak i od zlonamjernih aplikacija koje se smatraju legitimnima. Takvi napadi naglašavaju važnost redovitih sigurnosnih pregleda, ažuriranja i praćenja svih uređaja i softvera koji se koriste na korporativnoj mreži. Također je važno educirati zaposlenike o prijetnjama te ih educirati o sigurnosnim praksama koje smanjuju rizik od takvih napada.

4.3. LUKA ANTWERP

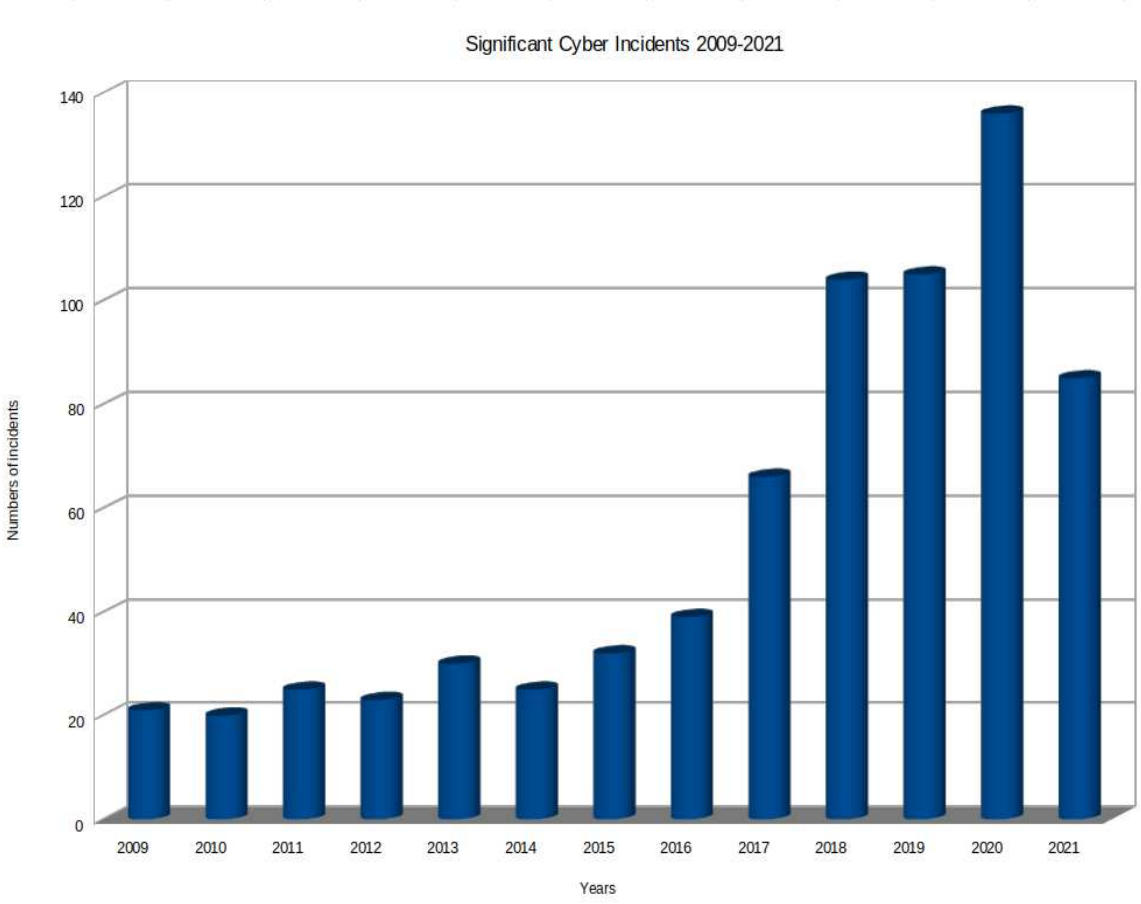
Napad na luku Antwerpen u Belgiji vrhunski je primjer sofisticiranog kibernetičkog napada s ozbiljnim posljedicama. Napadači su uspjeli preuzeti kontrolu nad informacijama sadržanim u računalnim sustavima lučkog terminala i tako doći do podataka o podrijetlu i odredištu kontejnera. Koristili su te informacije za krijumčarenje droge i automatskog oružja u kontejnerima i glatko presretanje kontejnera na putu do odredišta. Napadači su koristili tehnike socijalnog inženjeringa, uključujući slanje zlonamjernog softvera e-poštom, kako bi zarazili računalne sustave kontejnerske tvrtke. Nakon što je infekcija otkrivena, poduzete su neke mjere za sprječavanje budućih napada. Međutim, napadači su bili uporni i koristili su se posebno dizajniranim hardverskim komponentama, poput minijaturnih računala skrivenih

u strujnim kabelima i vanjskim flash diskovima, kako bi bolje nadzirali i krali podatke. Ovaj napad naglašava potrebu za strogim sigurnosnim mjerama u pomorskoj industriji.[5]

4.4. NAPAD RANSOMWAREA NA 1,000 BRODOVA

Okvirno 1.000 plovila pogođeno je ransomware napadom na velikog dobavljača softvera za brodove. DNV, organizacija za pomorstvo sa sjedištem u Oslu, jedna od najvećih pomorskih organizacija na svijetu, izvijestila je da je doživjela ransomware napad 7. siječnja 2023.godine, te da je bila prisiljena isključiti IT poslužitelje povezane s njihovim sustavom ShipManager. Navodi se da su svi korisnici još uvijek mogli koristiti funkcionalnosti ShipManager softvera na brodu izvan mreže. Nema naznaka da su bilo koji drugi softver ili podaci tvrtke DNV bili pogođeni. DNV je izjavio da surađuje s norveškom policijom i tvrtkama za IT sigurnost kako bi odgovorio na incident. DNV je najveće društvo za klasifikaciju na svijetu - organizacija koja upravlja tehničkim certifikacijama za izgradnju i rad brodova i offshore konstrukcija. Više od 13.175 plovila i mobilnih offshore jedinica trenutno koristi usluge DNV-a, koji je ostvario prihod od preko 2 milijarde dolara u 2021. godini. Napad na DNV je najnoviji u nizu koji pogađa industriju brodarstva. Naftne kompanije Oiltanking i Mabanaft, obje u vlasništvu njemačkog logističkog konglomerata Marquard & Bahls, doživjele su kibernetički napad koji je onesposobio njihove sustave za utovar i istovar u veljači 2022. U studenom je tajnik Američkog Ministarstva domovinske sigurnosti Alejandro Mayorkas izjavio Kongresu da najznačajnija prijetnja američkim lukama su kibernetički napadi.

[5] Importance of cybersecurity, https://marine-digital.com/article_importance_of_cybersecurity, (20. 06. 2023.)



Graf 2. Kibernetički napadi u pomorstvu od 2009.-2021. godine

Izvor: ***Vessel Automation***, https://vesselautomation.com/wp-content/uploads/2021/08/Graph-of-incidents.png, (4. 7. 2023.)

4.5. KIBERNETIČKA SIGURNOST U PROMETNOM SUSTAVU

Kibernetička sigurnost u prometnom sustavu odnosi se na zaštitu računalnih sustava, mreža i podataka povezanih s prometom od kibernetičkih prijetnji i napada. Prometni sustav uključuje različite načine prijevoza, poput cestovnog prijevoza, zračnog prijevoza, željezničkog prijevoza, pomorskog prijevoza i drugih oblika prijevoza.

Neki aspekti kibernetičke sigurnosti u prometnom sustavu uključuju:

- Infrastrukturu, poput prometne infrastrukture npr. semafori, putokazi, mostovi, tuneli i pametni prometni sustavi, sama infrastruktura postaje sve više digitalno povezana. Sigurnost takve infrastrukture zahtijeva zaštitu od neovlaštenog pristupa, manipulacije ili prekida rada.

- Vozila jer svaki njihov napredak u tehnologiji donosi i nove sigurnosne izazove. Pametna vozila, autonomna vozila i povezana vozila postaju sve više prisutna u prometu. Kibernetička sigurnost uključuje zaštitu tih vozila od napada koji bi mogli ometati sigurno upravljanje vozilom, manipulirati senzorima, preuzeti kontrolu nad vozilom ili pristupiti osjetljivim podacima.
- Komunikacijske mreže u prometnom sustavu uključuju sigurnu i pouzdanu komunikaciju između različitih elemenata prometnog sustava. To uključuje bežične mreže, mobilne komunikacije i protokole koji se koriste za razmjenu podataka između vozila, infrastrukture i nadzornih centara.
- Putnički podaci jer se prikuplja velika količina podataka o putnicima, uključujući osobne podatke, financijske informacije i putne navike. Zaštitom takvih podataka od neovlaštenog pristupa, krađe ili zloupotrebe važno je osigurati povjerenje korisnika u sustav i poštovati te provoditi propise o privatnosti.
- Napredne tehnologije kao što su umjetna inteligencija (AI) i veliki podaci (Big Data) igraju važnu ulogu u poboljšanju prometnih sustava. Međutim, istovremeno otvaraju nove mogućnosti za kibernetičke napade. Kibernetička sigurnost zahtijeva primjenu sigurnosnih mjera za zaštitu ovih tehnologija od zloupotrebe.
- Suradnja i regulativa u prometnom sustavu zahtijeva suradnju između različitih vladinih agencija, prijevoznike, proizvođače vozila, dobavljače tehnologije i istraživačke institucije. Također je važno uspostaviti odgovarajuću regulativu koja promiče kibernetičku sigurnost i postavlja standarde za zaštitu prometnog sustava. Uzimajući u obzir samu složenost kibernetičke sigurnosti u prometnom sustavu, važno je provoditi redovita testiranja sigurnosti, educirati osoblje o sigurnosnim postupcima, implementirati sigurnosne protokole kako bi se minimizirali sigurnosni rizici i osigurala zaštita prometnog sustava i putnika.[6]

[6] DNV, Maritime cybersecurity, https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html, (14. 6. 2023)

5. SVJETSKA STATISTIKA O KIBERNETIČKIM NAPADIMA

Malware napadi

Između ožujka i svibnja 2023. akteri prijetnji implementirali su prosječno 11,5 napada u minuti, uključujući 1,7 novih uzoraka zlonamjernog softvera u minuti. U 2022. zlonamjerni softver doživio je brzi ponovni porast u odnosu na najnižu razinu u sedam godina 2021. – popevši se na nevjerojatnih 2,8 milijardi napada. Više od 26 000 novih ranjivosti aplikacija i infrastrukture dodano je u Nacionalnu bazu podataka ranjivosti SAD-a 2022. Ruske državne prijetnje skupine pokušale su provaliti u vitalnu infrastrukturu u Ukrajini. Koristili su zlonamjerni softver Industroyer2 za napad, ali nisu uspjeli prije nego što su uspjeli prouzročiti stvarnu štetu. Stručnjaci za kibernetičku sigurnost, Sonicware, pronašli su više od 270 228 varijanti zlonamjernog softvera koje nikad prije nisu viđene. Otprilike 30% provala zlonamjernog softvera događa se putem e-pošte s lažnim poveznicama i privicima.

Ransomware

Jedna od najrazornijih kibernetičkih prijetnji i sve je češća posljednjih godina. Hakeri su napali bolnice, škole i tvrtke s ransomware-om, ostavljajući žrtve da plate otkupninu ili izgube pristup svojim podacima. Bilo je otprilike 638 pokušaja ransomware-a po korisniku u prvoj polovici 2022. 65% organizacija koje su doživjele napad ransomware-a suočile su se s više od 6 dana prekida rada nakon toga. 92% pogođenih organizacija nije koristilo učinkovite mjere za sprječavanje gubitka podataka, što je dovelo do kritičnog gubitka podataka od ransomware-a. Ransomware je prisutan u gotovo 30% svih povreda podataka zlonamjernog softvera.

U 2021. godini ransomware je prouzročio gubitke od preko 49 207 908 dolara što ne uključuje neviđene poslovne gubitke, kao što je izgubljeno vrijeme, oduzete plaće i više. Unatoč smanjenju globalnih napada ransomware-om od 235% u 2022., i dalje je bilo 236,1 milijuna napada diljem svijeta. 72% ispitanih organizacija bilo je pogođeno ransomware-om u 2021., a 13% je doživjelo 6-10 napada ransomware-om tijekom godine.

Phishing

Phishing je kibernetički napad u kojem napadači šalju zlonamjerne e-poruke koje izgledaju kao legitimne poruke. Zatim prevarom navode korisnike da daju osjetljive podatke ili preuzmu zlonamjerni softver. Krađa identiteta putem e-pošte često se koristi za pristup sustavima ili imovini organizacije. Odatle napadači mogu širiti zlonamjerni softver, ukrasti podatke i dobiti pristup drugim ciljevima koristeći privatne podatke organizacije.

Više od 60% ugroženih podataka u prvom kvartalu 2023. dogodilo se kao rezultat problema s vjerodajnicama. U prosjeku je za otkrivanje i obuzdavanje kršenja povezanih s krađom identiteta bilo potrebno 295 dana – treće najduže od bilo koje kibernetičke prijetnje. Tjedno se blokira 710 milijuna phishing e-poruka.

18% kliknutih phishing e-poruka dolazi s mobilnog uređaja a 67% svih povreda podataka započinje tako što netko klikne na naizgled sigurnu vezu, a između 80 i 95% svih povreda počinje krađom identiteta.

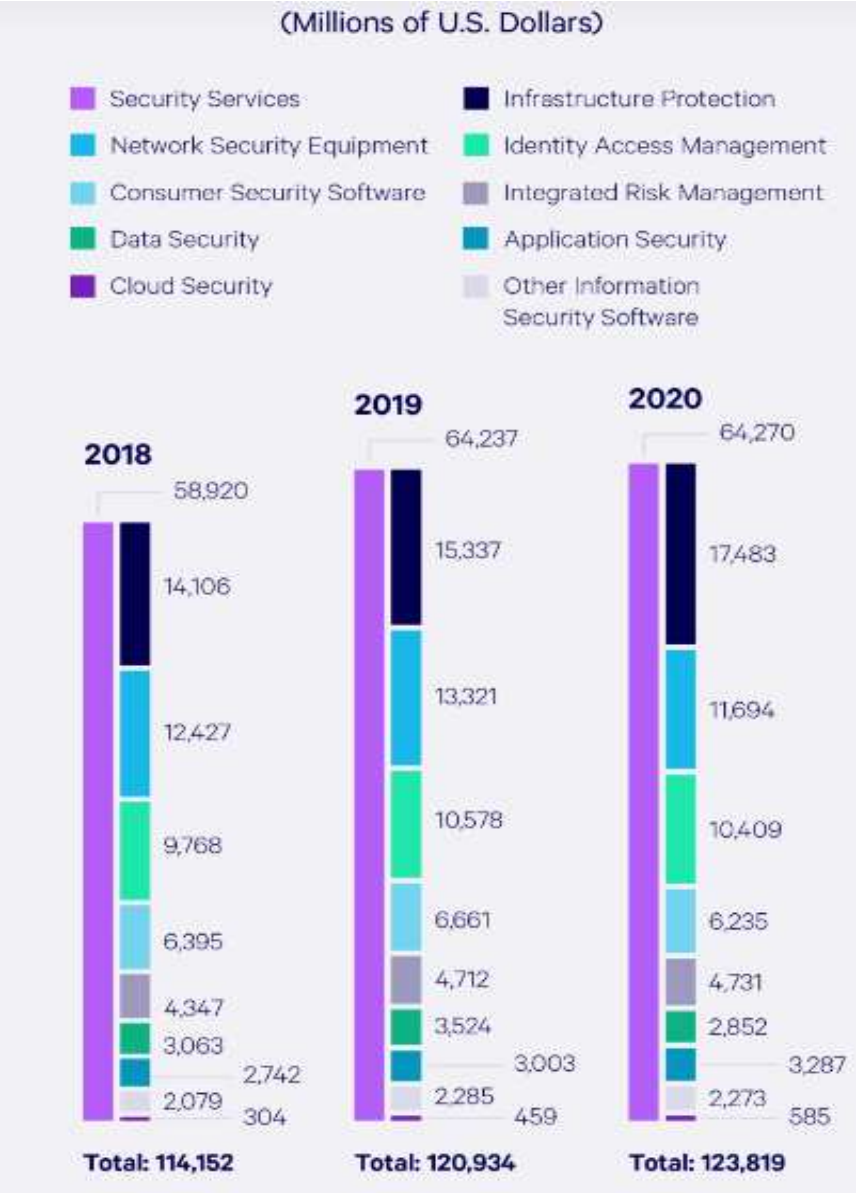
APWG je zabilježio 1.270.883 phishing napada u 2022. Ovo je novi rekord i najveći broj phishing napada koje je APWG ikada vidio.

DDoS i IoT

Napad se izvodi pomoću mreže kompromitiranih uređaja povezanih s internetom, poput računala ili IoT uređaja. To rezultira prekidom mrežnih usluga i mogućim gubitkom podataka o korisnicima.

- Comcast Business otkrio je 51,915 DDoS napada u 2022.
- Microsoft je ublažio prosječno 1,955 DDoS napada dnevno u 2022., što je povećanje od 40 % u odnosu na prethodnu godinu.
- Cloudflare je zaustavio DDoS napad koji je imao 17,2 milijuna zahtjeva u sekundi.
- UDP (User Datagram Protocol) spoof flood napadi porasli su u prvoj polovici 2022. godine, sa 16 % na 55 %. Ova vrsta napada češća je u industriji igara.

Od zabilježenih 2022 DDoS napada, 28% je završeno za manje od 10 minuta, 26% je trajalo između 10 i 30 minuta, 14% je bilo u rasponu od 31 do 60 minuta, a preostalih 32% produžilo se preko sat vremena. Mirai, zlonamjerni (IoT) malware, otkriven je 103,092 puta u cijelom svijetu.



Slika 2. Globalna potrošnja na sigurnost po segmentima

Izvor: ***Cyber Attack Statistics and Trends***, https://www.embroker.com/blog/cyber-attack-statistics/, (27. 7. 2023.)

5.1. SVJETSKA STATISTIKA NAPADA PO SEKTORIMA

Zdravstveni sektor

- Zdravstvena industrija imala je najskuplje povrede podataka u zadnjih 12 godina.
- Troškovi su čak porasli za 41,6% od 2020. 75% povreda zdravstvenih podataka prijavljenih u prvoj polovici 2023. pripisano je hakiranju.

- 21% povreda zdravstvenih podataka dogodilo se kao rezultat neovlaštenog pristupa ili otkrivanja, di je rezultat povećanje od 133% u odnosu na 2022. godinu.
- Mrežni poslužitelji odgovorni su za 65% povreda zdravstvenih podataka u prvoj polovici 2023., dok su računi e-pošte odgovorni za 18%.
- U 2022. bilo je najmanje 849 poznatih incidenata kibernetičke sigurnosti u zdravstvu i 571 povreda podataka.
- Prosječni financijski gubitak zbog povrede podataka u zdravstvu skočio je s oko 9 milijuna dolara na 10,10 milijuna dolara (2022.).

Glavni razlozi zbog kojih ljudi napadaju zdravstvenu industriju su zato što žele novac (95%), da dobiju tajne informacije (4%), jer im to odgovara (1%) ili su iz nekog razloga ljuti na zdravstvenu industriju (1%).

Financijski sektor

Financijski sektori zabilježili su porast napada ransomware-om od 35% u prvom tromjesečju 2022.

- 78% organizacija koje pružaju financijske usluge doživjelo je probijanje sigurnosti u 2023. godini.
- Financijskim institucijama u prosjeku je potrebno nevjerojatnih 233 dana da obuzdaju i ublaže povrede podataka.
- Phishing napadi na financijske institucije kao što su banke imali su najveći udio od 23,2%, što predstavlja najveći broj napada u financijskom sektoru

U prosjeku, financijske organizacije snosile su druge najveće troškove povrede podataka, s 5,97 milijuna dolara, odmah iza zdravstvenih ustanova.

Vladini sektori

- Kibernetički napadi usmjereni na vlade porasli su za 95% diljem svijeta u drugoj polovici 2022.
- Vlade svijeta su odgovorne za 4% svih napada ransomware-om u svijetu.
- Trošak povrede podataka u državnim javnim sektorima eskalirao je za 7,25%, s prosječnim ukupnim troškovima koji su skočili s 1,93 milijuna dolara na 2,07 milijuna dolara.

- U svibnju 2022. Kostarika je bila bačena u izvanredno stanje nakon što je napad ransomware-a onesposobio vladine operacije i zatvorio više bolnica.

Glavni razlozi iza kibernetičkih napada vlade nisu samo zbog novca (80%), već i zbog tajni (18%), zbog osobne ideologije (1%) ili zato što su ljuti na vladu (1%).

Obrazovni sektor

5% svih napada ransomware-om usmjereno je na obrazovne sektore.

- Prosječna cijena povrede podataka u obrazovanju iznosi 3,86 milijuna dolara.
- Obrazovni sektori bili su meta aktera nacionalne države 14% vremena.
- Industrija obrazovnih usluga doživljava dramatičan porast napada ransomware-a, koji čine više od 30% kršenja.
- Sjeverna Koreja je posebno odgovorna za 23% napada na obrazovne sektore.

Energetski sektor

U 2022. napadi ransomware-om bili su usmjereni na energetske sektore u najmanje 4% slučajeva.

- Cyber napadi u prosjeku koštaju energetski sektor 4,72 milijuna po incidentu.
- 22% kibernetičkih napada na naftu i plin bilo je povezano sa špijunažom.
- Energetski sektor vrlo je osjetljiv na društveni inženjering, s obzirom na to da su 60% svih povreda podataka phishing napadi.
- U 2022. bila su najmanje 403 prijavljena incidenta kibernetičkog napada na energetske sektore, sa 179 uspješnih povreda podataka.[7]

Izravni troškovi odgovora na kibernetički napad uključuju angažiranje sigurnosnih stručnjaka za procjenu štete i rješavanje problema, obavještavanje korisnika o potencijalnom izlaganju podataka, ulaganje u ažuriranja ili zamjene sustava kako bi se spriječili budući slični napadi i ponudu krađe identiteta korisnicima zaštitu ili druge pravne lijekove.

Prema IBM-u, prosječna cijena povrede podataka dosegla je 4,35 milijuna dolara u 2022.

- Za popravak štete od cyber napada potrebno je oko 277 dana.

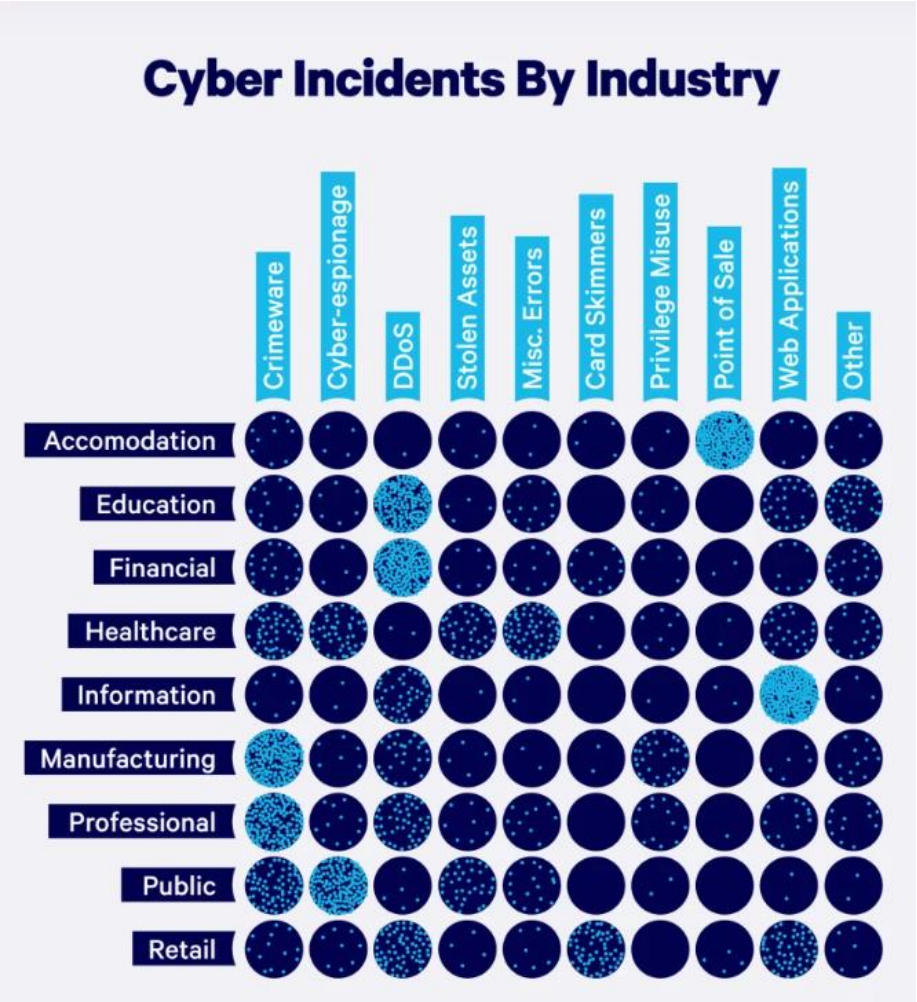
[7] Cyber Attack Statistics, https://parachute.cloud/cyber-attack-statistics-data-and-trends/, (20. 7. 2023.)

- Od organizacija koje su doživjele više od jedne povrede podataka, 57% je troškove incidenta prebacilo na svoje korisnike, dok je samo 51% povećalo ulaganja u sigurnost.

Neizravni troškovi kibernetičkog napada mogu biti čak i značajniji od izravnih troškova. Povreda podataka može dovesti do gubitka kupaca, smanjenja prihoda i dugoročne štete za ugled vaše tvrtke. Štoviše, možda ćete morati platiti regulatorne kazne i pravne postupke ako napad dovede do kolektivne tužbe.

- 60% tvrtki koje su pretrpjele povredu podataka moralo je nakon toga povećati troškove robe i usluga za svoje klijente.
- Poduzeća mogu u prosjeku uštedjeti do 2,1 milijuna dolara procjenom financijskog rizika potencijalnih povreda podataka unaprijed, čime se izbjegavaju skupe naknade za oporavak u slučaju kibernetičkog napada.
- Gubitak poslovanja nakon bilo kojeg kibernetičkog napada košta do 1,42 milijuna dolara godišnje.

Iako kibernetički napad može biti skup, troškovi povezani s njegovim pokretanjem su iznenađujuće niski. Na primjer, postoje čak i pružatelji usluga koji nude sofisticirane komplete za krađu identiteta za manje od 6 dolara dnevno, ovi paketi sadrže višestruke slojeve složenosti i značajke anonimizacije dizajnirane za rad pod većinom sustava za otkrivanje ili prevenciju. Stoga je bitno poduzeti sve potrebne korake kako biste zaštitili svoje poslovanje od skupih kibernetičkih napada prije nego što se dogode.



Slika 3. Kibernetički incidenti po industrijama

Izvor: ***Cyber Attack Statistics and Trends***, https://www.embroker.com/blog/cyber-attack-statistics/, (27. 7. 2023.)

5.2. STATISTIKA NAPADA NA PODRUČJU REPUBLIKE HRVATSKE

Tijekom 2022. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru Republike Hrvatske. Prema podacima iz kvartalnih Izvješća o incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske članovi su prijavljivali phishing (429 prijava), scam (197), phishing URL (186), pogađanje zaporki (133) te malware URL (67) i zaraze pojedinačnih računala malicioznim kodom (67).

Zabilježeno je 10 % više kibernetičkih napada u odnosu na isto razdoblje prošle godine. Opasnost od kibernetičkih prijetnji neprestano raste s obzirom da kriminalci

istražuju nove tehnike i postupke za sve naprednije napade na kritičnu infrastrukturu, tvrtke i građane. Virtualni prostor, posebice zadnja dva desetljeća, postao najmoćniji medij za širenje radikalnih i ekstremističkih ideologija, ali i organiziranje onih koji nastoje nedemokratskim metodama ostvariti svoja politička uvjerenja.

Udio kibernetičkih napada koji ciljaju ključnu infrastrukturu porastao je u jednogodišnjem razdoblju s 20 % na 40 %. Kao odgovor na porast sigurnosnih prijetnji u Hrvatskoj je intenziviran rad na novoj Nacionalnoj strategiji kibernetičke sigurnosti, a policija već godinama jača kapacitete za borbu protiv kibernetičkog kriminala. Samo u posljednje tri godine MUP je izravno uložio preko milijun eura u tehnološku modernizaciju ovog segmenta rada policije, u tijeku je ulaganje od 1.6 milijuna a slijede i nova značajna ulaganja u 2023. godini pa nadalje u okviru unutarnjeg fonda sigurnosti EU.[8]

Kaznena djela	Prijavljena kaznena djela			Razriješena kaznena djela			Naknadno razriješena kaznena djela		
	Broj djela		Trend	Broj djela		Trend	Broj djela		Trend
	2021.	**2022.**	u %	2021.	**2022.**	u %	2021.	**2022.**	u %
Iskorištavanje djece za pornografiju	261	**311**	+19,2	258	**308**	+19,4	224	**252**	+12,5
Neovlašteni pristup	32	**31**	-3,1	6	**13**	+116,7	5	**8**	+60,0
Ometanje rada računalnog sustava	10	**5**	-50,0	4	**2**	-50,0	3	**1**	-66,7
Oštećenje računalnih podataka	21	**25**	+19,0	1	**7**	+600,0	1	**5**	+400,0
Neovlašteno presretanje računalnih podataka	2	**8**	+300,0	1	**3**	+200,0	1	**2**	+100,0
Računalno krivotvorenje	70	**39**	-44,3	67	**38**	-43,3	62	**38**	-38,7
Računalna prijevara	1.158	**1.425**	+23,1	651	**771**	+18,4	638	**749**	+17,4
Zlouporaba naprava	4	**7**	+75,0	4	**7**	+75,0	4	**7**	+75,0
Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača	1								
Povreda žiga	4	**13**	+225,0	4	**13**	+225,0	1	**5**	+400,0
UKUPNO	**1.563**	**1.864**	+19,3	**996**	**1.162**	+16,7	**939**	**1.067**	+13,6

Tablica 1. Poredbeni prikaz kaznenih djela kibernetičkog kriminaliteta

Izvor: ***MUP RH,*** https://mup.gov.hr/UserDocsImages/statistika/2023/Statisticki_pregled_2022_web%20prelim.pdf, (25. 7. 2023.)

[8] MUP RH – Glavno tajništvo – Sektor za pravne poslove i strateško planiranje – Služba za strateško planiranje, statistiku i unaprjeđenje rada, https://mup.gov.hr/UserDocsImages/statistika/2023/Statisticki_pregled_2022_web%20prelim.pdf, (25. 7. 2023.)

6. RAZVOJ PRIJETNJI U POMORSTVU

Pomorska industrija ima ključnu ulogu u modernom društvu jer osigurava opskrbu sirovinama i dostupnost raznovrsnih proizvoda. Osim brodova, sektor također uključuje infrastrukturu poput tvrtki, luka i vanjskih partnera. Moderna tehnologija omogućuje korištenje navigacijskih sustava, upravljanje teretom i brzu razmjenu informacija. Međutim, s razvojem interneta, pomorstvo se suočava s kibernetičkim prijetnjama.

Moderniziranje brodova, uvedeni su novi uređaji, poput elektroničkih pomorskih karata u ECDIS-u (Electronic Chart Identification and Display System). ECDIS prikazuje karte i omogućuje pristup bazi podataka informacija. AIS (Automatic Identification System) također se koristi za razmjenu identifikacijskih podataka broda. Međutim, ti su uređaji ranjivi i potrebno je poduzeti odgovarajuće mjere opreza. Računala se također koriste na brodovima za upravljanje postavkama tereta i strojarnice. Vodeće organizacije u pomorskoj industriji razvile su smjernice za smanjenje rizika od kibernetičkih napada na brodove. Ove smjernice daju smjernice i informacije o zaštitnim mjerama protiv takvih napada, koje treba razmotriti uz postojeća sigurnosna načela međunarodnog upravljanja sigurnošću (ISM) i međunarodnog kodeksa o sigurnosti brodova i luka (ISPS).Važno je da kibernetička sigurnost bude prioritet na svim razinama vlasti, uključujući kopnene tvrtke i brodske posade. Edukacija zaposlenika o kibernetičkim prijetnjama i korištenje odgovarajućih tehničkih rješenja ključni su za smanjenje rizika od napada.[9]

6.1. OBRAMBENE STRATEGIJE

Obrambene strategije u kibernetičkoj industriji osmišljene su kako bi se zaštitile organizacije od kibernetičkih napada i održala sigurnost njihovih sustava i podataka.

Neke od obrambenih strategija koje se koriste u kibernetičkoj industriji su:

- Praćenje prijetnji i analiza ranjivosti gdje organizacije moraju aktivno pratiti i analizirati nove prijetnje i ranjivosti kako bi identificirale potencijalne slabosti u svojim sustavima i poduzele potrebne korake za njihovo rješavanje.

[9] Cybersecurity in the shipping industry, http://forums.capitallink.com/shipping/2017cyprus/ppt/ioannides.pdf, (10. 5. 2023.)

- Jak identifikacijski i autentifikaciji sustavi čine složene lozinke, dvofaktorska autentifikacija ili biometrija koja pomaže u sprječavanju neovlaštenog pristupa sustavima i podacima.
- Redovito ažuriranje softvera i zakrpe čine aplikacije i sustave ažurne s najnovijim sigurnosnim ažuriranjima i zakrpama te na taj način smanjuje rizik od iskorištavanja prije poznatih sigurnosnih propusta.[10]
- Sigurnosno nadgledanje i detekcija je skupina alata koji omogućuju organizacijama da prate mrežne aktivnosti, otkrivaju neobične obrasce i identificiraju potencijalne napade ili zloupotrebe.
- Izoliranje i segmentiranje mreže na manje dijelove ili područja može ograničiti širenje kibernetičkog napada i smanjiti njegov utjecaj na cijeli vaš sustav ili organizaciju.
- Redovita obuka korisnika (zaposlenika) i svijest o sigurnosnim praksama, otkrivanje prijevara putem e-pošte, phishing napada i drugih oblika društvenog inženjeringa ključni su za smanjenje rizika od uspješnih napada.
- Kontinuirano sigurnosno testiranje, gdje provođenje sigurnosnih testova kao što je testiranje penetracije ili testiranje ranjivosti omogućuje organizacijama da identificiraju i poprave ranjivosti prije nego što ih iskoriste napadači. Svaka organizacija treba prilagoditi i kombinirati strategije prema svojim specifičnim potrebama i rizicima kako bi osigurala optimalnu sigurnost svojih sustava i podataka.

6.2. TEHNIČKE MJERE ZAŠTITE

Dok tehničke mjere zaštite od kibernetičkih rizika igraju ključnu ulogu u osiguravanju otpornosti sustava na brodu, provedba takvih mjera mora biti izvediva i isplativa, s posebnom pozornošću na postojeće brodove. Redovito ažuriranje ovih mjera važno je za održavanje njihove učinkovitosti i izbjegavanje rizika od neuspjeha. Internet Security Center (CIS) pruža smjernice kao što su kritične sigurnosne kontrole (CSC) koje se mogu primijeniti za rješavanje ranjivosti računala. CSC kontrole su dokazane kontrole visokog prioriteta koje

[10] O. Fitton, D. Prince, B. Germond, M. Lacy: „The future of maritime cyber security “, Lancaster University, 2015.

pomažu organizacijama da procijene i poboljšaju svoju sigurnost. Za opremu i podatke na brodu, odabrani su sljedeći primjeri CSC-ova:

- Ograničavanje i kontroliranje mrežnih pristupnika, protokole i usluge koje reguliraju pristup mrežnim sustavima pomoću kontrolirane mreže ili podsustava. Zatvorite mrežne priključke koji se ne koriste i konfigurirajte mrežne uređaje poput vatrozida, usmjerivača i preklopnika.
- Određivanje kontroliranih i nekontroliranih mreža, uzimajući u obzir koji su sustavi povezani na kontrolirane i nekontrolirane mreže. Kontrolirane mreže moraju spriječiti sigurnosne prijetnje korištenjem vatrozida, sigurnosnih pristupnika, usmjerivača i preklopnika. Nenadzirane mreže trebaju biti izolirane od nadziranih mreža kako bi se spriječile infekcije zlonamjernim softverom.
- Inspekcije mreža bitnih za rad broda trebaju osigurati visoku razinu sigurnosti za sustave bitne za rad broda.
- Kontroliranje mreža koje dobavljačima omogućuju pristup sustavima za ažuriranje sustava ili daljinsko održavanje.
- Sustavi za kontrolu i upravljanje teretom za utovar tereta, planiranje tereta i upravljanje kontejnerima.
- Mreža za goste i kontrola privatnog pristupa internetu znači bilo koju bežičnu mrežu za goste ili privatni pristup internetu za posadu.

Implementacija ovih mjera zaštite na brodovima pomaže u stvaranju otpornog i sigurnog okruženja protiv kibernetičkog napada. Važno je pridržavati se smjernica i najboljih praksi te redovito provoditi nadogradnje i ažuriranja kako bi se održala učinkovitost i osigurala zaštita od napada. Fizička sigurnost je ključna komponenta kibernetičke obrane i igra važnu ulogu u zaštiti osjetljivih OT i IT kontrolnih komponenti na brodu.

Neki od aspekata fizičke sigurnosti u kontekstu kibernetičke sigurnosti na brodu:

1) Zaključavanje prostora koja sadrže osjetljive kontrolne komponente kako bi se spriječio neovlašteni pristup. Oprema koja je ključna za sigurnost i rad, poput servera ili mrežnih ormara, također treba biti zaštićena od neovlaštenog pristupa.
2) Fizička zaštita osjetljive korisničke opreme di je važno osigurati fizički pristup opremi poput izloženih USB priključaka na mostovima sustava što se može postići korištenjem zaštitnih mjera poput poklopaca ili zaključanih ormarića.

3) Sigurnost satelitske i radiokomunikacije di imaju LAN priključak koji povezuje brod s mrežama. Zaštita od prisluškivanja može se postići korištenjem Virtual Private Network (VPN) veze ili šifriranih protokola. Zaštita od hakiranja i drugih napada može uključivati suradnju s pružateljem usluge, korištenje sigurnih poslužitelja na kopnu ili implementaciju vatrozida na brodu.
4) Deaktivacija nepotrebnih funkcija kako bi se smanjio potencijalni napadni vektor, preporučuje se deaktivacija nepotrebnih funkcija na satelitskim terminalima. To može uključivati onemogućavanje daljinske administratorske stranice ili prosljeđivanja priključaka (port forward) koji mogu predstavljati rizik.
5) Kontrola pristupa i mrežni vatrozidi trebaju biti kontrolirani kako bi se spriječio neovlašteni pristup. Javna IP adresa broda ne bi trebala biti izravno dostupna s interneta, već bi veze trebale prolaziti kroz mrežu i vatrozid na kopnu radi kontrole pristupa.
6) Sigurnost administrativnih sučelja gdje komunikacijskih terminali obično pružaju upravljačka sučelja koja su dostupna putem mreže. Važno je osigurati sigurnost tih sučelja kroz ograničenje mreža koje mogu pristupiti.

6.3. PROCEDURALNE MJERE ZAŠTITE

Ove mjere zaštite trebale bi biti dio politika i postupaka upravljanja sigurnošću tvrtke i implementirane na praktičan i troškovno učinkovit način. Proceduralne kontrole usmjerene su na to kako brodsko osoblje koristi sustav. Planovi i postupci koji sadrže osjetljive podatke moraju se čuvati u tajnosti i njima se mora upravljati u skladu s politikama tvrtke.

Neke od mjera zaštita uključuju:

1) Obuku i svjesnost koju osoblje treba proći o kibernetičkoj sigurnosti i trebaju biti svjesni rizika povezanih s korištenjem IT sustava na brodu. To uključuje prepoznavanje phishing napada, upotrebu sigurnih lozinki, zaštitu podataka i druge sigurnosne postupke.
2) Ograničen pristup posjetiteljima poput vlasti, tehničara ili agenata kojima treba ograničiti pristup računalima na brodu. Ako je pristup dopušten, trebao bi biti ograničen u pogledu privilegija i pod nadzorom.
3) Korištenje osobnih uređaja di treba postaviti određene postupke za korištenje osobnih IT uređaja posade na brodu, uzimajući u obzir sigurnost kritičnih sustava.

Komunikacija putem osobnih uređaja trebala bi biti odvojena od kritičnih IT ili OT sustava.

4) Nadogradnje i održavanje softvera vrlo je bitna komponenta jer redovito ažurirani hardver i softver na brodu pomaže pri održavanju odgovarajućeg nivoa sigurnosti. Ovo uključuje ažuriranje operativnih sustava, firmware-a i ostalog softvera na računalima, usmjerivačima, prekidačima itd.
5) Alati za antivirusnu zaštitu i sprječavanje zlonamjernog softvera trebaju se koristiti za skeniranje softvera koji mogu otkriti i riješiti zlonamjerni softver. Ti alati trebaju biti ažurirani i upravljani, a ažuriranja treba distribuirati brodovima pravodobno.
6) Udaljeni pristup gdje je obavezno uspostaviti politike i postupke za kontrolu udaljenog pristupa IT i OT sustavima na brodu. To uključuje jasne smjernice o dozvoljenim pristupima, koordinaciju s kapetanom broda i bilježenje svih slučajeva udaljenog pristupa.

7. USPOSTAVLJANJE PLANA ZA HITNE INTERVENCIJE

Razumijevanje važnosti sigurnosnih incidenata povezanih s kibernetičkom sigurnošću na brodu te razvoj planova odgovora koji pokrivaju relevantne hitne situacije su ključni za sigurnost i kontinuitet poslovanja.

Ovdje je primjer incidenata koji bi trebali biti obuhvaćeni za hitne situacije na brodu:

1) Gubitak dostupnosti elektroničke navigacijske opreme ili integriteta podataka vezanih za navigaciju.
2) Gubitak dostupnosti ili integriteta vanjskih izvora podataka, kao što je GNSS (Global Navigation Satellite System).
3) Gubitak ključne povezanosti s obalom, uključujući komunikacije putem Globalnog Pomorskog Sustava Hitnog Poziva i Sigurnosti (GMDSS).
4) Gubitak dostupnosti industrijskih kontrolnih sustava, uključujući pogonske, pomoćne sustave i druge kritične sustave, te gubitak integriteta upravljanja i kontrole podataka.
5) Incident s ucjenjivačkim softverom (ransomware) ili ometanjem usluge (denial of service).

Planovi protumjera trebaju biti osmišljeni kako bi se adekvatno upravljalo tim incidentima. Ovi planovi trebaju uključivati upravljanje komunikacijama i eskalaciju kako bi se osigurala pravilna obalna podrška. Također, važno je osigurati da planovi protumjera i povezane informacije budu dostupni u obliku koji nije elektronički, s obzirom na mogućnost gubitka elektroničkog pristupa njima u slučaju kibernetičkih incidenta.

Treba razmotriti razdvajanje operativno-tehničkih (OT) sustava od mrežne veze sa kopnom radi zaštite sigurnosti broda. Veze između obalnih i OT sustava mogu biti korisne za razne primjene, ali istovremeno predstavljaju potencijalni vektor napada na kritične sustave broda. Planovi trebaju specificirati situacije u kojima se takvi OT sustavi trebaju privremeno odvojiti od mrežne veze sa kopnom radi sprječavanja napada i održavanja sigurnosti broda.

Za učinkovito prekidanje veza s kopnom, mreža i usluge, povezanosti trebaju biti dizajnirane na način da se mreže mogu brzo fizički izolirati ili isključiti. Odgovorno osoblje s obale treba pružiti ovaj dizajn i postupak kapetanu, a posada treba biti obučena za upravljanje brodom u slučaju prekida veze s OT sustavom.

Važno je razviti i testirati ove planove te osigurati da kapetan, časnici i posada budu upoznati s postupcima za reagiranje na kibernetičke incidente. Također, planovi trebaju biti redovito pregledani i ažurirani kako bi se osigurala njihova učinkovitost.

7.1. ODGOVOR I OPORAVAK OD SIGURNOSNOG INCIDENTA

Planiranje odgovora na kibernetičke incidente je ključno. Međutim, važno je razumjeti da planovi neće uvijek savršeno odgovarati stvarnim scenarijima. Stoga je potrebno redovito vježbati planove i razvijati protumjere na temelju naučenih lekcija.

Priprema je prva faza odgovora na incidente. U ovoj fazi treba identificirati ključne komponente na brodu, izrađivati sigurnosne kopije podataka, identificirati točke neuspjeha i definirati alternativna rješenja. Također treba izraditi plan odgovora na incidente koji uključuje uloge i odgovornosti posade i osoblja na obali, komunikacijske puteve i procese oporavka podataka.

Detekcija i analiza su druga faza odgovora. Tim za odgovor treba saznati kako se incident dogodio, koje su sustave pogođene i u kojoj mjeri, te koliko prijetnja i dalje ostaje.

Kontrola i iskorjenjivanje su treća faza. U ovoj fazi treba kontrolirati izbijanje incidenta, uklanjati pogođene uređaje s mreže, provjeravati pravila vatrozida i ažurirati protuvirusne programe. Također je važno napraviti sliku diska pogođenih sustava i razmotriti snimanje memorije.

Obnova nakon incidenta je četvrta faza. U ovoj fazi treba obnoviti sustave i podatke, provesti istragu incidenta i poduzeti mjere za sprječavanje ponovnog pojavljivanja. Plan oporavka treba biti prilagođen vrsti broda i instaliranim sustavima.[11]

Važno je provoditi obuku i svijest o kibernetičkoj sigurnosti te redovito testirati postupke oporavka i suradnju između broda i obale. Mogućnost oporavka podataka je ključna tehnološka mjera zaštite. Treba uspostaviti razdoblja zadržavanja i scenarije obnove kako bi se prioritetno obnovili kritični sustavi. Istraživanje kibernetičkog incidenta može

[11] Cyber Security onboard ships, https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf, (12. 5. 2023.)

pružiti vrijedne informacije o ranjivostima i trebalo bi se provesti u skladu s postupcima tvrtke.[12]

[12] A Comprehensive Guide to Maritime Cybersecurity, https://www.missionsecure.com/hubfs/Assets/eBooks/A%20Comprehensive%20Guide%20to%20Maritime%20Cybersecurity_Final.pdf, (25. 5. 2023).

8. ZAKLJUČAK

Uz sve veći broj kibernetičkih napada diljem svijeta, kibernetička sigurnost igra ključnu ulogu u modernom društvu. Ovi napadi ne pogađaju samo privatne korisnike, već i velike tvrtke, uključujući i pomorski sektor. Čak i kada se prijetnje dogode u virtualnom prostoru, njihove posljedice mogu biti izuzetno ozbiljne. Važno je razumjeti osnovne pojmove i metode koje se koriste u izvođenju takvih napada. Analizirajući stanje u pomorstvu, vidljivo je da je glavni razlog dosadašnjih napada stjecanje financijske koristi. Međutim, s pojavom novih situacija vezanih uz terorističko djelovanje, napadi sve više poprimaju politički karakter, s ciljem nanošenja materijalne štete i ugrožavanja ljudskih života. Iz tog razloga, akreditirana tijela izdaju smjernice s ciljem minimiziranja rizika od cyber napada. Obavještajni podaci o kibernetičkoj sigurnosti pomorske industrije igraju ključnu ulogu u sprječavanju raznih vrsta napada. Stoga je važno već u prvim fazama izobrazbe pomoraca osposobiti stručnjake s potrebnim znanjem iz područja kibernetičke sigurnosti. Spominjanje kibernetičkih napada u pomorskom sektoru relativno novo, s obzirom na napredak informacijske tehnologije, ne treba ga zanemariti. Svaki pojedinac ima odgovornost ulagati u svoje znanje o informacijskoj sigurnosti kako bi doprinio sigurnosti cijele zajednice. Stoga je važno istaknuti potrebu kontinuiranog usavršavanja i svijesti o važnosti kibernetičke sigurnosti u pomorskom sektoru.

9. LITERATURA

Knjige:

(1.) Fitton, O., Germond, B., Lacy, M., Prince, D. (2015). The future of maritime cyber security. Lancaster University. (7. 5. 2023.)

(2.) Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. Technology Innovation Management Review. (7. 5. 2023.)

(3.) Wu, C.-H. (John), Irwin, J. D. (2013). Introduction to computer networks and cybersecurity. CRC Press.Elektronički izvori: (2. 5. 2023.)

Elektronički izvori:

http://forums.capitallink.com/shipping/2017cyprus/ppt/ioannides.pdf (10. 5. 2023.)

https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (12. 5. 2023.)

https://www.mitags.org/guide-ship-cybersecurity/ (18. 5. 2023.)

https://www.missionsecure.com/hubfs/Assets/eBooks/A%20Comprehensive%20Guide%20to%20Maritime%20Cybersecurity_Final.pdf (25. 5. 2023.)

https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html (14. 6. 2023.)

https://www.maritime-cybersecurity.com/ (15. 6. 2023.)

https://marine-digital.com/article_importance_of_cybersecurity (20. 6. 2023.)

https://mup.gov.hr/UserDocsImages/statistika/2023/Statisticki_pregled_2022_web%20prelim.pdf (25. 7. 2023.)

https://www.embroker.com/blog/cyber-attack-statistics/ (27. 7. 2023.)

POPIS KRATICA

Kratica	Puni naziv na stranom jeziku	Tumačenje na hrvatskom jeziku
AIS	Automatic Identification System	Automatski identifikacijski sustav
BMS	Building Management System	Napadi na sustave upravljanja brodovima
CIS	Coordinated Information System	Informacijski sustav za komunikaciju

CSC	Customer Service Center	Sigurnosni kontrolni centar
DDoS	Distributed Denial of Service	Distribuirani napad uskraćivanjem usluge
ECDIS	Electronic Chart Display and Information System	Elektronički kartografski i navigacijski informacijski sustav
DoS	Denial of Service	Napad uskraćivanja usluga
ERP	Enterprise Resource Planning	Planiranje resursa poduzeća
GMDSS	Global Maritime Distress and Safety System	Pomorski sustav hitnog poziva i sigurnosti
GNSS	Global Navigation Satellite System	Globalni navigacijski satelitski sustav
ICT/IT	Information and Communication Technologies	Informacijska i komunikacijska tehnologija
ICS/OT	Industrial Control System	Industrijski kontrolni sustav/ Operacijska tehnologija
IoT	Internet of Things	Internet stvari
ISM	International Safety Management	Međunarodni upravljački kod za sigurnost brodova
ITPS	Information Technology and Business Strategy	Informacijska tehnologija i profesionalne usluge
MES	Manufacturing Execution System	Sustav izvršenja proizvodnje
SCADA	Supervisory Control and Data Acquisition	Nadzor i upravljanje nad industrijskim procesima
VPN	Virtual Private Network	Virtualna privatna mreža

POPIS TABLICA

POPIS ILUSTRACIJA

POPIS GRAFIKONA