Evolucija kibernetičkih prijetnji u pomorskoj industriji

Botunac, Ive

Sveučilište u Zadru

Pomorski odjel - Nautički odsjek

Preddiplomski sveučilišni studij nautike i tehnologije pomorskog prometa
(jednopredmetni – izvanredni)

Ive Botunac

Evolucija kibernetičkih prijetnji u pomorskoj industriji

Završni rad

Zadar, 2016.

Sveučilište u Zadru

Pomorski odjel - Nautički odsjek

Preddiplomski sveučilišni studij nautike i tehnologije pomorskog prometa (jednopredmetni – izvanredni)

Evolucija kibernetičkih prijetnji u pomorskoj industriji

Završni rad

Student/ica:

Ive Botunac

Mentor/ica:

doc. dr. sc. Marijan Gržan

Zadar, 2016.

Izjava o akademskoj čestitosti

Ja, Ive Botunac**,** ovime izjavljujem da je moj završni rad pod naslovom **Evolucija kibernetičkih prijetnji u pomorskoj industriji** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 4. lipnja 2016.

SADRŽAJ

1. UVOD

Zahvaljujući konstantnom razvoju računalnih tehnologija, svjedoci smo primjene računala u gotovo svim aspektima života. Oslanjanjem na tehnološka dostignuća znatno nam je olakšano obavljanje svakodnevnih poslova te im time poklanjamo sve veće povjerenje. Korištenjem osobnog računala kao svakodnevnog pomagala, isti trend se odražava i na industrijski sektor. Danas je gotovo nemoguće zamisliti bilo koji oblik poslovanja bez upotrebe računala kao sredstva za postizanje veće učinkovitosti. Razvojem globalne podatkovne mreže koju nazivamo internet omogućeno nam je umrežavanje s udaljenim računalima i samim time ostvarivanje komunikacije s njima.

Ovakav brz razvoj primjene računala nalazi svoju značajnu ulogu i u pomorskoj industriji. Uvođenjem modernih rješenja u integrirane sustave na brodu, današnjim pomorcima se uvelike olakšavaju svakodnevni poslovi i vođenje same navigacije. Automatizacijom se povećava razina sigurnosti u smislu izbjegavanja sudara i ostalih neželjenih događaja koji se mogu zbiti tijekom plovidbe. Interakcija na razini čovjeka i računala stvara poveznicu koja rezultira sve većim oslanjanjem čovjeka na automatizirani sustav. Upravo ovakva poveznica stvara sasvim novu prijetnju koju bilježimo u svim industrijama, a to su kibernetički napadi. Korištenjem modernih tehnika i znanja, maliciozni korisnici stavljaju fokus na pomorstvo kao velik izvor prihoda. Iskorištavanjem nedovoljne edukacije o novom obliku sigurnosne prijetnje koja zahvaća pomorsku industriju, napadači odmah u startu ostvaruju prednost. Dodatni problem očituje se u tome što određene pomorske konvencije tek sada izdaju naputke i strategije za održavanje rizika od kibernetičkih napada na prihvatljivoj razini. Istraživanjem pratimo razvoj računalnih napada i njihove primjene u cilju stjecanja svjesnosti o ovom obliku prijetnji.

Ovaj završni rad podijeljen je kroz poglavlja počevši u drugome poglavlju s uvodom u sami pojam i definicijom računalne sigurnosti što je ujedno i osnova za razumijevanje daljnjeg rada. Nakon toga slijede definicije i kategorizacija računalnih napada gdje se opisuju njihove metode i strukture. Glavna tema rada o području kibernetičkih prijetnji u pomorskoj industriji počinje s četvrtim poglavljem i nastavlja se do samog zaključka. Kako se kroz cijeli rad protežu stručni pojmovi vezani za računalstvo, za neke termine ne postoje odgovarajući hrvatski prijevodi, stoga se koriste engleski nazivi.

2. UVOD U RAČUNALNU SIGURNOST

2.1. Općenito o računalnoj sigurnosti

Računalnu sigurnost možemo definirati kao zaštitu računalnih tehnologija fokusiranu na zaštitu računala, mreža, računalnih programa i podataka od neovlaštena pristupa kako bi se time spriječilo nedozvoljeno izmjenjivanje i uništavanje podataka. Pojam računalne sigurnosti obuhvaća široko područje koje dijelimo na određene kategorije od kojih kao najvažnije smatramo informacijsku te mrežnu sigurnost. U ovome području sigurnost je proces održavanja prihvatljive razine rizika kojoj je neki sustav izložen. Sukladno ovom poimanju računalne sigurnosti, da bi se ona mogla održavati, potrebno je provesti niz zaštitnih mjera kako bismo se obranili od vanjskih i unutarnjih prijetnji. Ubrzanim razvojem informacijskih i komunikacijskih tehnologija raste i broj podataka koji se prenose putem njih. Taj proces u mnogim slučajevima nije popraćen odgovarajućim zaštitnim mehanizmima te se povećava rizik izloženosti potencijalnim računalnim napadima.

2.1.1. *Informacijska sigurnost*

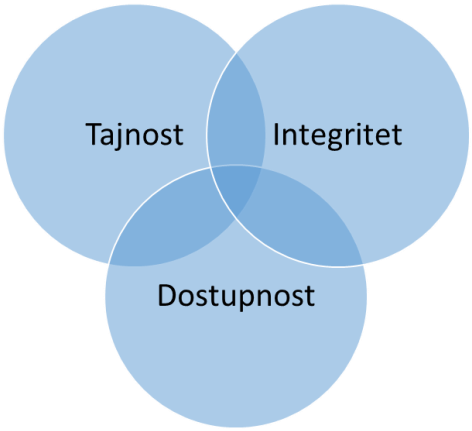
Definirano Zakonom o informacijskoj sigurnosti čl. 2, „Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“ [6]. Kako bi se održavala informacijska sigurnost, prethodno se provode odgovarajuće organizacijske i tehničke procedure u održavanju stupnja pouzdanosti sustava na prihvatljivoj razini. Informacijski sustav je svaki komunikacijski, računalni sustav u kojem se informacije prenose i pohranjuju kako bi ih ovlašteni korisnik mogao upotrijebiti.

2.1.2. *Mrežna sigurnost*

Specijalizirano polje u području računalne sigurnosti je osiguravanje sigurnosti mrežnih infrastruktura. Održavanje mrežne sigurnosti provodi se korištenjem određenih hardverskih uređaja i softverskih rješenja kako bi se blokirao dolazak zlonamjernog prometa na štićena računala. Postavljanjem autorizacijskih metoda omogućuje se pristup mreži samo ovlaštenim osobama gdje se identifikaciju korisnika potvrđuje unošenjem odgovarajućeg imena i lozinke. Pod hardverskom zaštitom podrazumijevamo razne izvedbe vatrozida (engl. *firewall*) koji služe kako bi filtrirali ulazne i izlazne mrežne pakete.

2.2. Definiranje sigurnosnih zahtjeva

Da bismo razumjeli osnovna načela za koja se zalaže područje informacijske sigurnosti, moramo definirati sigurnosne zahtjeve (Slika 1.) koje treba zadovoljiti kao bismo sustav zadržali sigurnim. Svaka organizacija nastoji svoje povjerljive podatke zadržati sigurnim i dostupnim samo ovlaštenim osobama. Kako bismo ostvarili ove namjere, definirali smo tri osnovna sigurnosna zahtjeva za tajnost, integritet i dostupnost podataka. Nakon definiranja sigurnosnih zahtjeva, sljedeći korak zahtijeva njihovo provođenje i pridržavanje od svih korisnika pojedinog informacijskog sustava.



Slika 1. Sigurnosni zahtjevi

2.2.1. *Tajnost podataka*

Tajnost podataka odnosi se na zaštitu podataka od neovlaštenog i neželjenoga pristupa. Ovaj zahtjev je od iznimne važnosti jer ne želimo da povjerljivi podaci neke organizacije budu javno dostupni kako ne bi došlo do otkrivanja poslovnih tajni i unutar organizacijskih komunikacija. Za ostvarivanje ovoga zahtjeva koriste se razne metode enkripcije podataka i primjene kontrole pristupa. Kriptiranjem podataka koristeći se određenim kriptografskim algoritmima pretvaramo podatke u oblik koji može biti razumljiv samo ovlaštenoj osobi uz posjedovanje odgovarajućega ključa. Kontrolom pristupa postavljamo ulaz u sustav putem potvrđivanja identifikacije korisnika, najčešće putem korisničkog imena i lozinke.

2.2.2. *Integritet podataka*

Integritetom podataka podrazumijevamo osiguravanje potpunosti i nepromijenjenosti podataka tijekom razdoblja u kojem oni postoje. Ispunjavanjem ovog sigurnosnog zahtjeva za integritetom podataka pri razmjeni informacije između dvije strane stvara se povjerenje u osiguravanju izvornosti poslane informacije i njezine originalnosti. Ovaj zahtjev postaje posebno važan zbog sve veće prisutnosti elektroničkog poslovanja u industriji te kao ključ sigurnosti i povjerenja uvodi se digitalni potpis. Digitalni potpis je sigurnosna oznaka koju se može dodati dokumentima. Dokument koji se potpisuje sažima se koristeći se funkcijama sažimanja (engl. *hash function*) te se šifrira korisnikovim ključem i potom šalje s originalnim

dokumentom. S druge strane, osoba koja prima poruku na temelju originalnog dokumenta koristi isti algoritam sažimanja i isti ključ kako bi potom svoj dobiveni rezultat mogla usporediti s poslanim potpisom. Ako se dobiveni rezultat i potpis podudaraju, znamo da se prilikom prijenosa osigurao integritet poruke.

2.2.3. *Dostupnost podataka*

Kao garanciju ovlaštenim korisnicima da u svakome trenutku mogu pristupiti svojim podacima, moramo osigurati njihovu dostupnost. U određenom trenutku, ako su podaci nedostupni, to možemo smatrati istim kao i da podaci više ne postoje. Zbog sveprisutne globalne mreže mnogi svoje podatke drže na sigurnim, udaljenim poslužiteljima kako bi time osigurali veći prostor i dostupnost svim svojim korisnicima bez obzira na geografsku udaljenost. Dostupnost podataka može biti osporena ako su dijelovi sustava oštećeni uslijed nastanka tehničkih kvarova, kao posljedica prirodnih pojava ili ljudskih pogrešaka.

2.3. Razumijevanje sigurnosnih prijetnji

Kako bismo mogli bolje razumjeti područje računalne sigurnosti nakon definiranja sigurnosnih zahtjeva koje osiguravamo, moramo razumjeti sigurnosne prijetnje kojima smo izloženi. Prijetnja kao pojam je skup okolnosti koje mogu nanijeti štetu sustavu kroz provođenje napada u svrhu iskorištavanja ranjivosti sustava. Iza provođenja napada na sustav mogu stajati pojedinci ili skupine čija motivacija dolazi iz potpuno različitih očekivanja i ciljeva.

2.3.1. *Profil napadača*

U području računalne sigurnosti termin „napadač“ koristimo za osobu koja bez prethodne autorizacije ulazi u zaštićene sustave te time ulazi u prekršaj zakona države u kojoj je napad počinjen. S druge strane, u žargonu šire javnosti često se susrećemo s terminom „haker“ (engl. *hacker*) koji se koristi za opisivanje ovakve vrste kriminalaca što je potpuno pogrešan opis. Naziv „haker“ u računalstvu koristimo za opisivanje osobe koje odlično poznaju računala, softver i hardver te su samim time stručnjaci u specifičnim poljima računalnih znanosti [8]. Mnogi od njih bave se istraživanjima u području računalne sigurnosti ne bi li time doprinijeli ranom otkrivanju sigurnosnih propusta i na vrijeme zaštitili korisnike.

Napadače iz ove sekcije ili drugim riječima kriminalce nazivamo krekerima (engl. *cracker*). Krekere možemo opisati također kao računalne stručnjake koji istražuju mogućnosti novih računalnih tehnologija, a dio njih je motiviran kriminalnim pobudama [8]. Motivaciju za napad pronalaze u financijskoj dobiti koju ostvaruju raznim prevarama ili pak u dolasku do određene moći i reputacije koju ostvaruju u određenim krugovima ljudi.

3. RAČUNALNI NAPADI

Kako bismo dobili cjelokupnu sliku o području računalne sigurnosti, nakon objašnjenja sigurnosnih zahtjeva i prijetnji s kojim se susrećemo, u ovome poglavlju postavlja se uvid u računalne napade. Računalni napad je napad pokrenut s računala protiv drugog računala, računalnog sustava ili *web*-stranice koji dovodi u pitanje povjerljivost, integritet i dostupnost informacija koje su sadržane na napadnutom sustavu. Kroz korištene literature i izvore [1, 3, 7] možemo pronaći razne definicije kategorija, vrsta i metoda računalnih napada kojim autori pobliže opisuju ovo područje. Ovim poglavljem, radi lakšeg razumijevanja daljnjeg rada, obrađujemo podjelu napada na kategorije, potom opisujemo najčešće korištene metode za njihovu provedbu. Kroz svaku podjelu važno je spomenuti najčešći oblik napada i osnovno načelo njegova djelovanja.

3.1. Kategorije računalnih napada

Osnovnom podjelom napade možemo promatrati kao:

- **nasumične napade** u kojima napadač nema određenu metu nad kojom provodi napad, već on putem mreže postavlja zamke kojima hvata svoje žrtve

- **ciljane napade**, koji su zlonamjerni napadi usmjereni na točno određenog pojedinca, tvrtku, sustav ili softver – ovakav napad se provodi za izdvajanje informacija, ometanje poslovanja ili uništavanje podataka.

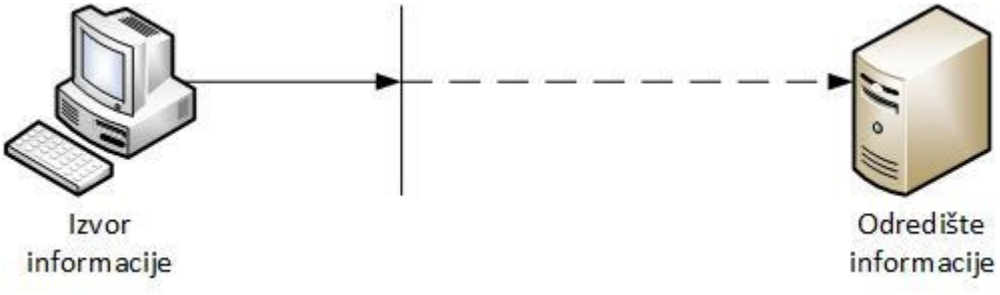
Kategorije napada dodatno su grafički prezentirane kako bismo imali jasniju sliku o njihovoj izvedbi. Kada kažemo da sustav nije izložen napadu, smatramo da informacije odnosno podaci putuju neometano od svoga izvora prema odredištu (Slika 2.).

Slika 2. Normalan tok informacija

3.1.1. *Napad prekidom komunikacijskoga toka*

Provedbom aktivnog napada prekida dolazi do presijecanja toka informacija koje se kreću od izvora prema odredištu (Slika 3.). U ovoj kategoriji uključujemo napade s namjerom

oštećivanja komponenata fizičkog sklopovlja koje se koristi u mrežnoj komunikaciji. Možemo spomenuti i korištenje uređaja za namjerno ometanje signala koje također dovodi do prekida komunikacijskoga toka. Najvažnijim za spomenuti smatramo napad DDoS (Distributed Denial of Service) kojim prekidamo uslugu iscrpljivanjem mrežnih resursa slanjem lažnih zahtjeva na poslužitelj.

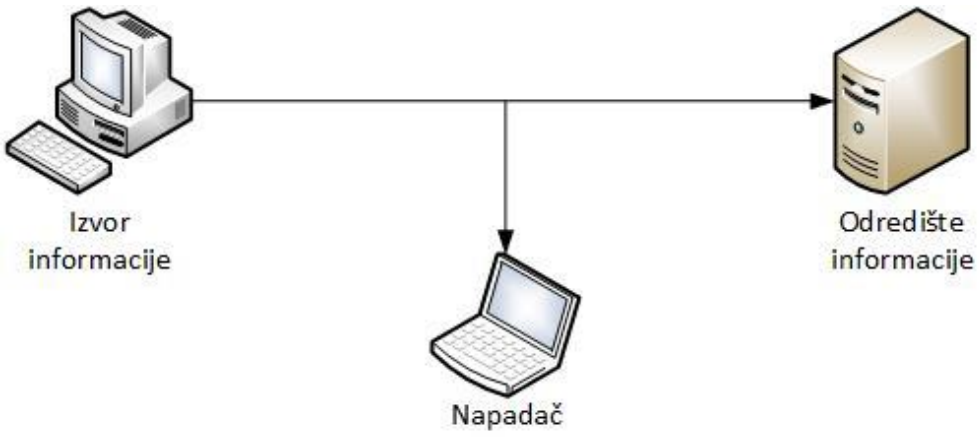


Slika 3. Prekid toka informacija

Ovaj napad iako ima mnogo varijanta i primjena, ali najčešće za njega čujemo u kontekstu gdje je napadnuta neka *web*-stranica. Specifičnost se ogleda u provođenju napada s botnet mreže koju prethodno napadač posjeduje. Termin botnet koristimo za skupinu zaraženih računala nekim određenim zlćudnim programom koji su u potpunoj kontroli napadača. Napadač potom koristi tu mrežu zaraženih računala kako bi slao zahtjeve za spajanje na određeni poslužitelj koji neće biti u stanju odgovoriti na sve te zahtjeve. Upravo zbog ovoga nastaju česte nedostupnosti *web*-poslužitelja kojima želimo pristupiti.

3.1.2. *Napad presretanjem informacija*

Napadom presretanja napadač se postavlja u komunikacijski kanal između izvora i odredišta u cilju prisluškivanja (engl. *sniffing*) prometa koji se odvija između njih (Slika 4.). Ovim napadom dolazi se do osjetljivih informacija poput korisničkih podataka za prijavu na sustav. Sve većim razvojem i korištenjem bežičnih mreža, zlonamjernim korisnicima omogućen je značajno lakši pristup komunikacijskom kanalu i postavljanju u njega. Najpoznatiji napad koji spada pod ovu kategoriju poznat je pod nazivom „čovjek u sredini“ (engl. *Man In The Middle*).

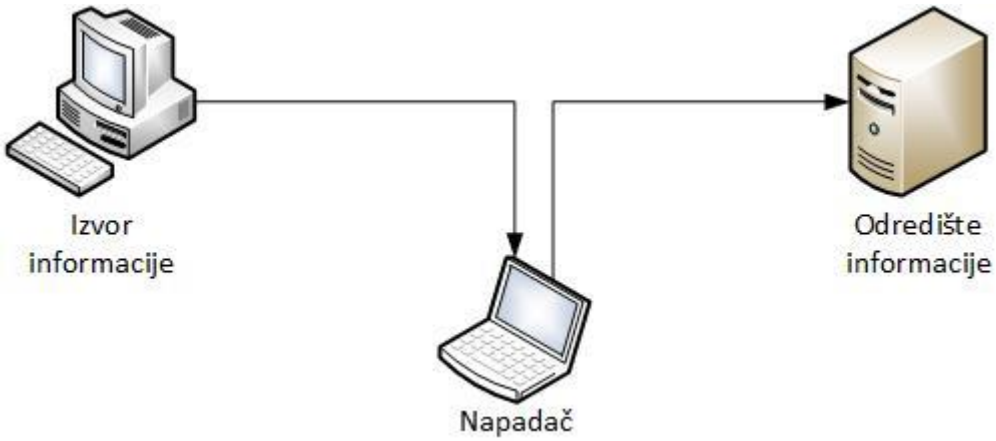


Slika 4. Presretanje informacije

Razvojem sigurnosnih komunikacijskih protokola koji se koriste u cilju kriptiranja podataka koji se razmjenjuju znatno je smanjena mogućnost presretanja prometa. Danas se koristi sigurnosni sloj SSL/TSL za koji možemo reći da se nalazi između transportnog TCP i aplikacijskog HTTP sloja koji su sastavni dio mrežne komunikacijske strukture. Spominjanjem sigurnosnog protokola moramo i spomenuti infrastrukturu javnoga ključa (engl. *Public Key Infrastructure*) koja je sastavni dio ove vrste zaštite. Infrastruktura javnoga ključa objedinjuje sve uloge, pravila i postupke potrebne za stvaranje, upravljanje, distribuciju digitalnih certifikata. Njezina primarna svrha je olakšati prijenos podataka kroz mrežu poput elektroničke trgovine, bankarstva i dokaza za potvrdu identiteta prilikom prijave. Osnovu čine digitalni certifikati koji sadrže javne i privatne ključeve kako bi spomenuti protokoli mogli provesti radnje enkripcije i dekripcije podataka.

3.1.3. *Napad promjenom informacije*

Kod napada promjenom smatramo za cilj dolazak do informacija kojima primjenom modifikacije sadržaja napadač ostvaruje svoju namjeru (Slika 5.). Kako bi napadač uopće došao do informacija, prethodno već mora imati kontrolu nad zaraženim sustavom ili treba biti postavljen u komunikacijski kanal. Motivacija iza ovakvih napada može biti sadržana u svrsi podmetanja lažne informacije, provođenja raznih prevara ili pak prekrivanja nekog prethodno provedenog napada.

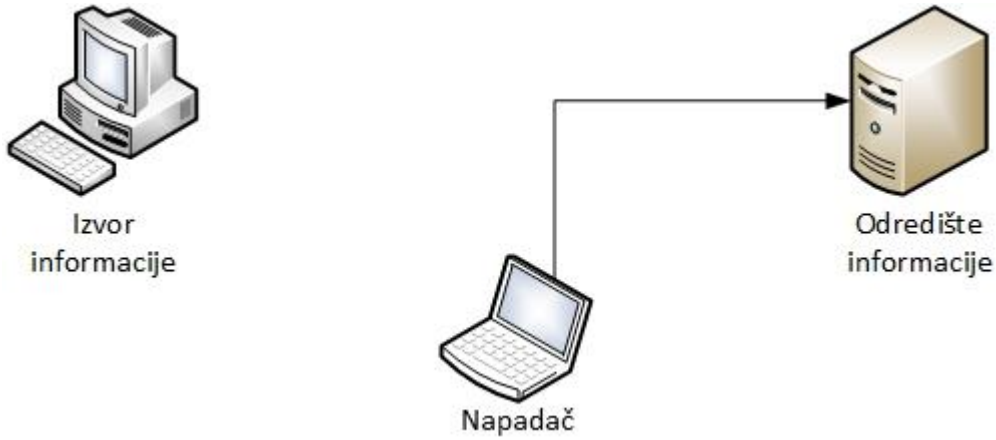


Slika 5. Promjena informacije

Primjena ovog napada može se promotriti kroz primjere ako se putem interneta izvršavaju razne uplate ili isplate, a napadač prati toga korisnika. Tim napadač može na takvim zahtjevima koje provodi korisnik napraviti izmjene ne bi li preusmjerio sredstva na neke druge račune. Jedna od učestalih pojava ovoga napada veže se za društvene mreže. Ako napadač dođe u posjed korisničkog imena i lozinke korisnika, on može pod tim imenom može obavljati lažne radnje kako bi nanio štetu korisniku.

3.1.4. *Napad lažnom informacijom*

Kreiranjem lažne informacije (engl. *spoofing*) napadač lažira svoj identitet i na taj način zavarava drugu stranu kojoj se predstavlja ili šalje informacije (Slika 6.). Ovaj napad je veoma učinkovit kod komunikacije putem elektroničke pošte gdje napadač koristi tehnike kojima lažira polazišnu adresu i na taj način prenosi zlonamjerne sadržaje. Provođenje ciljanog napada korištenjem lažnih informacija obično smatramo početkom u kojem napadač dolazi do pristupa kako bi dalje mogao provesti neki drugi oblik spomenutih napada.



Slika 6. Slanje lažne informacije

Osim slanja lažne elektroničke pošte, poznat je i napad pod nazivom *phishing*, što bi u prijevodu značilo „pecanje“. Obilježje napada je postavljanje lažne *web*-stranice koja je u osnovi kopija neke prave stranice te potom potrebe da se korisnik namami kako bi otvorio upravo tu lažnu stranicu. Ako korisnik to učini i unese svoje identifikacijske podatke, njega napadač „upeca“. Dalje će napadač preusmjeriti korisnika na pravu *web*-lokaciju, ali će zato i njegove identifikacijske podatke pohraniti na svoj poslužitelj. Korisnik svojim nemarom biva žrtva ovoga napada jer prethodno nije gledao URL (Uniform Resource Locator) adresu lokacije na koju se spaja.

3.2. Metode za provedbu napada

Nakon kategoriziranja vrsta napada neizostavno je obraditi metode koje se koriste kako bi se isti napadi mogli izvršiti. Kroz kategorije računalnih napada već smo spomenuli neke od najpoznatijih predstavnika. Iako danas postoje brojne metode kojima se napadači koriste, u ovome radu obrađujem dvije najzanimljivije s pogleda na pomorsku industriju. Kod provedbe računalnih napada može se primijetiti kombinacija korištenja više metoda u svrhu postizanja konačnog cilja. Smatram da najvažniju ulogu danas zauzimaju zlćudni programi i umijeće tehnike i vještine društvenoga inženjeringa koji zajedno čine cjelinu. Kako bi kreirani zlćudni program dostavili na željeni sustav, napadači se najčešće koriste upravo tehnikama prevara koje su vezane za društveni inženjering.

3.2.1. *Zloćudni softver*

Naziv zloćudni softver (engl. *malware, malicious software*) ili maliciozni programski kôd koristimo kao zajednički naziv za sve programe napisane sa svrhom počinjenja štete na računalnom sustavu. Pod ovim nazivom podrazumijevamo viruse, crve, trojance i mnoge druge koje susrećemo u području računalne sigurnosti. Svaki od navedenih zloćudnih programa posjeduje neke specifične karakteristike koje ga odlikuju, ali u svakodnevnom govoru možemo primijetiti da se koristi naziv virus. Razvoj zloćudnih programa smatra se najvećom prijetnjom u području računalne sigurnosti gdje se tijekom protekle godine prema istraživanju [11] pojavilo preko 431 milijuna novih inačica što je za gotovo 36 % veće nego u odnosu na prethodnu godinu.

Neke od specifikacija koje odlikuju današnje zlonamjerne programe ogledaju se kroz uspostavu anonimne kontrole nad zaraženim računalom ili sustavom. Time smatramo da napadač može putem udaljenog pristupa upravljati sadržajem nad zaraženim računalom bilo to prenošenje datoteka ili njihovo brisanje. Jedna od funkcionalnosti je bilježenje pritisnutih tipki na tastaturi (engl. *keylogging*) čime napadač može doći u posjed osjetljivih podataka kao što su lozinke ili pak brojevi kreditnih kartica. Tu se još nalaze mogućnosti poput pravljenja snimke ekrana korisnika koja se potom šalje na napadačev poslužitelj. Noviji zloćudni programi posjeduju i mogućnost izvlačenja lozinki koje su spremljene u *web*-preglednike korisnika pa time dolaze u posjed svih računa na koje se prijavljivalo s računala.

Trendom u razvoju zloćudnih programa smatramo pojavu takozvanih *ransomware*-virusa za koje ne možemo pronaći odgovarajući prijevod pa stoga kroz rad koristimo engleski naziv. Glavna karakteristika kojom se odlikuju je kriptiranje sadržaja na računalu koje time postaje nečitljivo korisniku te traženju uplaćivanja novčane svote napadačima kako bi dekriptiranjem sadržaj učinili ponovno čitljivim.

3.2.2. *Društveni inženjering*

Razvojem tehnologije i sigurnosnih rješenja u cilju zaštite računala od neželjenih prijetnji stvara se lažno vjerovanje da smo time u potpunosti osigurali sustav. Najvažnija karika u lancu koji povezuje cjelokupni računalni sustav su ljudi jer oni ostvaruju izravnu interakciju sa sustavom. Upravo ova metoda za provedbu napada koju nazivamo društveni inženjering (engl. *social engineering*) oslanja se na iskorištavane ljudske ranjivosti i pogreške kako bismo dobili kontrolu nad sustavom.

Tehnike društvenoga inženjeringa možemo podijeliti u dvije kategorije [10]:

- **Napadi usmjereni na ljude** se zasnivaju na stvaranju veze međuljudskih povjerenja i poznanstava kako bi se time mogla ostvariti manipulacija s osobama koje posjeduju informacije ključne u provedbi planiranog napada. U ovoj kategoriji možemo i spomenuti lažno predstavljanje u kojem se napadač prema korisniku predstavlja kao lažna osoba kako bi ovakvom manipulacijom ostvario poziciju iz koje može potraživati informacije. Napadači u ovome slučaju moraju biti vrhunski manipulatori koji svojim nastupom i lažnim uvjeravanjem mogu doći do svoga cilja. Osim uvjeravanja napadači iskorištavaju moralnu odgovornost pojedinca i želju za

pomoć ne bi li time probudili osjećaje koji će njihovu žrtvu navesti da izvrši sve što se od nje potražuje.

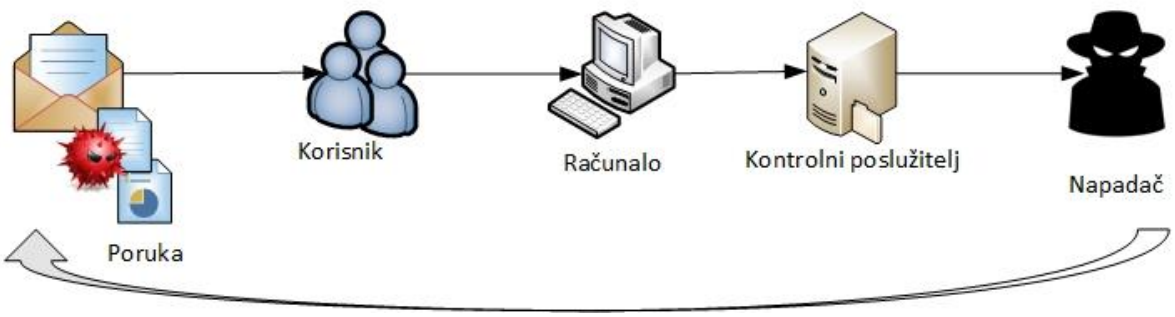
- **Napadi preko računala** spadaju u domenu dosta sofisticiranih napada koji svoju prednost ostvaruju u prevarama na daljinu. Znači, korisnik s napadačem nije u direktnom kontaktu već se taj kontakt ostvaruje korištenjem mrežne komunikacije. Napadač za provedbu ovih napada koristi se tehnikama slanja lažnih poruka u kojima se predstavlja kao netko drugi ili danas korištenjem sveprisutnih društvenih mreža kako bi ostvario kontakt s korisnikom.

Napadi se većinom odvijaju u nekoliko faza (Slika 7.) gdje je u početku bitno prikupiti što više informacija o korisniku ili sustavu nad kojim se planiralo provesti napad. Nakon ove faze slijedi razvijanje odnosa s korisnikom kako bi stekli povjerenje. Konačni cilj je upravo iskorištavanje toga povjerenja kako bi se ostvarila namjera s kojom je sam napad započet.

Slika 7. Faze u provedbi napada

3.3. Struktura napada

Kako bi se uspješno provelo računalni napad, postoje određeni koraci koji definiraju sami tijek napada. Daljnjim istraživanjem u radu koristit ćemo termin „ciljani napad“. Upravo zato smatram da je bitno pojasniti redoslijed koraka koji se takvim napadom provode [7]. Provođenje prethodnog izviđanja i svih dostupnih informacija o meti je najvažniji korak prilikom planiranja napada. Nakon što napadač odluči krenuti u napad, to čini prikazanim koracima (Slika 8.) gdje kreće od namjere postavljanja zloćudne aplikacije na računalo korisnika. Potom aplikacija komunicira s kontrolnim poslužiteljem koji je u kontroli napadača.



Slika 8. Vektori napada

3.3.1. *Izviđanje i prikupljanje informacija*

Prvi korak je izviđanje i prikupljanje informacija gdje napadač dolazi do relevantnih saznanja o svojoj meti. U ovome koraku od velike pomoći su mu javno dostupne internetske tražilice i društvene mreže preko kojih može doći i do osobnih podataka pojedinca poput adrese elektroničke pošte. S ovim napadač ima dovoljno informacija kako bi mogao stupiti u kontakt sa svojom metom. Ako napadač provede temeljito istraživanje o meti, bila to privatna osoba ili neka tvrtka, veće su šanse za ostvarivanje uspješnog napada. Temeljitom pripremom raspolaže brojnim informacijama koje koristi prilikom provođenja tehnike društvenog inženjeringa. Ovim korakom ujedno i planira tijek napada sa svim mogućim ishodima koji se mogu dogoditi kako bi pravodobno mogao reagirati.

3.3.2. *Inficiranje i iskorištavanje sustava*

Nakon što napadač stupi u kontakt sa svojom metom koristeći se tehnikama društvenog inženjeringa, može nagovoriti osobu da preuzme putem poruke zloćudni program ne znajući za njegove namjere. Naprednije tehnike koje se provode su vezane za iskorištavanje ranjivosti programa ili *web*-stranica koje osoba koristi i posjećuje. U trenutku kada se računalo zarazi zloćudnim programom, napadač ostvaruje pristup njemu i dolazi do svih privilegija nad računalom korisnika. Ujedno posjedovanje upravo te kontrole nad računalom je glavni cilj svakoga napada. Dalje napadač može pristupati računalu po želji i izvršavati planirane radnje napada.

3.3.3. *Održavanje kontrole pristupa*

Zadnji korak u procesu provođenja napada je što dulje zadržati pravo pristupa. Uspješnost u održavanju kontrole pristupa ovisi o tome u kojoj ćemo mjeri pristupati napadnutom sustavu. Ako smo koristili zloćudni program kako bismo ostvarili pristup, postoji mogućnost da korisnik primijeti određene poteškoće u radu svoga računala. Takve poteškoće daju mu do znanja da postoji neki neočekivani problem i pritom može doći do otkrivanja napada.

4. RAZVOJ PRIJETNJI U POMORSTVU

4.1. Izazovi prijetnji u pomorstvu

Pomorska industrija je temelj za učinkovito funkcioniranje svih aspekata modernog društva, od opskrba sirovinama poput nafte, željeza i žita do gotovo svakog proizvoda koji možemo naći u lokalnim prodavaonicama [22]. Kada spominjemo pomorsku industriju, ne mislimo samo na brodove koji čine jednu od sastavnica industrije, već na kompletnu infrastrukturu koju čine kompanije, luke i mnogi vanjski suradnici uključeni u ovu industriju. Važan oslonac u ovoj industriji danas je moderna tehnologija koja uvelike pomaže u provedbi navigacije, rukovanju teretom i pravovremenoj razmjeni informacija. Omogućavanje ovih pogodnosti koje uvelike pridonose u obavljanju aktivnosti u pomorstvu možemo prepisati i razvoju interneta. Čim spominjemo korištenje interneta, to automatski možemo povezati s činjenicom da time pomorska industrija postaje isto izložena kibernetičkim prijetnjama kao i bilo tko drugi.

Ako prvo promatramo same brodove, primijetit ćemo da je kroz modernizaciju uveden cijeli niz novih uređaja koji se koriste. Primjerice, za navigaciju se primjenjuju elektroničke karte koje su integrirane u sustav koji nazivamo ECDIS (Electronic Chart Display and Identification System). Taj sustav nam pruža prikaz samih karata kao i pristup bazi podataka u kojoj su smještene informacije o elementima koje prikazuje karta. U poveznici s ostalim uređajima i senzorima na brodu, njime se može prikazati radarska slika i razni drugi parametri plovidbe. Osim ECDIS-a koristi se i uređaj pod nazivom AIS (Automatic Identification System) čija je namjena razmjena identifikacijskih podataka o brodu koristeći se VHF frekvencijskim opsegom. Detaljniji način rada AIS uređaja i ranjivosti kojima je on izložen obrađujemo u sljedećem poglavlju.

Na brodu su također prisutna razna računala koja služe za upravljanje rukovanjem tereta te su smještena u namjenskim kontrolnim prostorijama. Isto tako, računala se koriste i u odjelu strojarnice gdje služe za kontroliranje parametara rada motora i ostalih bitnih elemenata koji su tamo smješteni.

4.1.1. *Razvoj strategije kibernetičke sigurnosti*

Neke od vodećih svjetskih pomorskih organizacija zajedno su pokrenule smjernice kako bi se smanjila opasnost od kibernetičkih napada na brodove [18]. Cilj ovih smjernica je pružiti jasne i sveobuhvatne upute i informacije za održavanje zaštitnih mjera od ovakve vrste napada. Ove smjernice treba promatrati kao sastavni dio već postojećih sigurnosnih pravila i zahtjeva sadržanih u ISM (International Safety Management) i ISPS kodu (International Ship and Port Facility Security).

Računalnu sigurnost treba uzeti u obzir na svim razinama upravljanja počevši od kompanija na kopnu do članova posade na brodu. Zaštitne mjere trebale bi uključivati pravovaljanu edukaciju zaposlenika u industriji te primjenu odgovarajućih tehničkih rješenja kako bi se smanjio rizik od izloženosti napadima.

4.2. Pregled dosadašnjih događaja

Unutar područja računalne sigurnosti u pomorstvu, informacije o samim napadima su u određenoj mjeri nedostupne. Tu nedostupnost možemo pripisati nekim od razloga koji se tiču politike koju vode kompanije gdje one ne odaju takve informacije javnosti. S druge strane tu je strah kompanija; ako bi informacije o napadu procurile u javnost, kompanija bi mogla izgubiti povjerenje koje joj pružaju korisnici. Sličan rezultat bi se odrazio ako bi izašla informacija o krađi podataka koje kompanija posjeduje te bi se tim činom ugrozio sâm korisnik.

Bez obzira na ove razloge, ipak su u javnost dospjele neke informacije o napadima koje su pretrpjele neke kompanije. Tvrtka CyberKeel, koja se bavi istraživanjem računalnih napada u pomorstvu, objavila je dokument [21] u kojemu iznosi pojedinosti o nekim napadima. Daljnjom razradom teme ovog poglavlja i pretraživanjem dostupnih izvora na mreži spomenut ću značajnije napade.

4.2.1. *Presretanje novčanog toka*

Krajem 2014. godine dogodio se incident u koji je bila uključena pomorska industrija, točnije jedan od vodećih opskrbljivača goriva WFS (World Fuel Services). Provedeni napad bio je fokusiran na prevaru u prijenosu novčanih transakcija na račun kriminalaca [21]. Nakon napada, WFS kompanija je objavila u javnosti podatak kako su bili žrtva napada koji im je prouzrokovao gubitak od gotovo 18 milijuna dolara. Sličan napad dogodio se i ranije krajem 2013. godine [25] koji je zahvatio najmanje tri tvrtke koje su vjerovale da svoje uplate šalje svome opskrbljivaču u Kini. Međutim, kriminalci su presretali njihovu komunikaciju i preusmjerili novčane transakcije na svoje račune. Ovim napadom kompanije su ostale oštećene za 1,65 milijuna dolara.

Napad koji su napadači provodili poznat je pod nazivom „čovjek u sredini“ gdje se napadač postavio u komunikacijski kanal između dvije kompanije. Samim time svaka kompanija je vjerovala da se komunikacija odvija direktno između njih, ali u stvarnosti su obje komunicirale s kriminalcima. Prethodno, kako bi napadači mogli provesti ovakav napad, bilo je potrebno postaviti zloćudni program na računalo kompanije kako bi bili u mogućnosti pratiti spomenutu komunikaciju.

4.2.2. *Zombie Zero napad*

Američka tvrtka koja se bavi računalnom sigurnošću TrapX objavila je detalje napada koji su nazvali Zombie Zero. Pod tim imenom krije se zloćudni program koji je bio skriven unutar skenera koji su koristile logističke kompanije za popis robe [26]. Napad je potvrdilo 8 različitih kompanija te je zloćudni program pronađen na 16 od 48 skenera s kojima je dolazio predinstaliran.

Kada bi se skener spojio na mrežu kompanije, pokrenuo bi se niz automatiziranih napada kojima je cilj bilo pronaći servere s riječi „finance“ u njihovome imenu. Nakon što bi se pronašao server, uslijedilo bi izvlačenje povjerljivih informacija te njihovo slanje na kontrolne centre koji su bili u vlasništvu napadača.

4.2.3. *Luka korištena za krijumčarenje droge*

Jedan od značajnijih napada zadesio je luku Antwerp u Belgiji, koji se odvijao kontinuirano u razdoblju od 2011. g. do 2013. g.. kad je i otkriven [37]. Ovim napadom bilo je omogućeno da napadači kontroliraju i nadziru informacije u računalnim sustavima terminala. Samim time imali su sve potrebne podatke o polazišnim i odredišnim destinacijama kontejnera. Oni su tom prilikom koristili kontejnere za skrivanje raznih vrsta opojnih droga i automatskog oružja. Kada bi kontejner trebao stići na svoje odredište, presretali su ga kako bi preuzeli svoju krijumčarenu robu bez da bi luka išta znala o tome. Ipak nakon nekog vremena lučkim radnicima je postalo sumnjivo kako je kontejner za koji piše da sadrži banane i grede nestao iz luke. Policijskom akcijom u kojoj su sudjelovale belgijska i nizozemska policija pronađena je tona kokaina i oružja te 1,3 milijuna eura u kovčegu.

Ovaj napad je postignut koristeći se metodama društvenog inženjeringa kako bi se prevarom putem elektroničke pošte zaposlenicima dostavilo zloćudni program. Kontejnerska kompanija je otkrila da im je sustav zaražen te su po tome pitanju poduzeli određene mjere kako bi zaustavili buduće napade. Međutim, u drugome napadu korištene su specifične hardverske komponente koje su se postavile na samu tipkovnicu računala kako bi bilježili sve što se tipka. Dodatno su korištena i posebno dizajnirana mini računala (Slika 9.) koja su bila skrivena unutar razdjelnika strujnoga kabela te vanjskim prijenosnim memorijama.

Slika 9. Hardver korišten u napadu

4.3. Motivacija napada na pomorsku industriju

Motivacija za provedbu napada u pomorstvu nema značajnih razlika od motivacije za napad u brojnim ostalim industrijama. Možemo reći da je primarni cilj napadača ostvariti financijsku dobit. Dodatno cilj u pomorstvu može biti manipuliranje podacima o teretu, krađa informacija i uzrokovanje prekida u transportu.

Prethodno smo spomenuli slučaj u kojemu je krađa novca izvedena napadom „čovjeka u sredini“ gdje je napadač direktno utjecao na tijek novčanih transakcija. Nakon pomno odrađenih

analiza ovakvog napada jasno su definirani propusti koji su se dogodili te danas kompanije koriste dodatne sustave verifikacije prilikom novčanih transakcija. Drugi način na koji napadači dolaze do novčane dobiti je putem zloćudnog programa zvanog *ransomware*. Već smo u prethodnom poglavlju spomenuli sam način rada programa koji se zasniva na kriptiranju sadržaja na zaraženom računalu i potom traženja otkupnine kako bi se isti sadržaj dekriptirao.

Kroz spomenute primjere vidimo da se koristilo manipuliranje informacijama kako bi se u prijevozu kontejnera mogla prokrijumčariti droga. Tim primjerom je pokazano da su napadače unajmili dileri kako bi izvršili traženi zadatak što ih dovodi u direktnu povezanost s kriminalnim djelom. Kranji cilj u takvim napadima je opet financijske naravi koja se ostvaruje kroz krijumčarenje droge i ostale ilegalne robe.

Danas, u vrijeme kada su teroristički napadi sve češći i razorniji, postoji određeni rizik od njih i u pomorskoj industriji. Time motivacija za napad nije u postizanju financijske dobiti, već u nanošenju materijalne štete i gubicima ljudskih života. Možemo smatrati da napadači motivirani ovakvim pristupom stvaraju ozbiljnu prijetnju za cijelu industriju mnogo opasniju od gubitka financijskih sredstava.

5. ANALIZA CILJANIH NAPADA

Već smo se u prijašnjim poglavljima susreli s terminom ciljanih napada koje smo definirali kao napade usmjerene prema određenom cilju nasuprot nasumičnim napadima. Ovako možemo stvoriti poveznicu da su u pomorskoj industriji zastupljeni upravo ciljani napadi. Prema prethodno navedenim primjerima napada koji su se zbili, vidimo da su se napadači prethodno morali dobro informirati o metama svog napada i načinima njihova poslovanja. Upravo to čini ove napade specifičnim i predstavlja izazov s kojim se susreću sigurnosni stručnjaci.

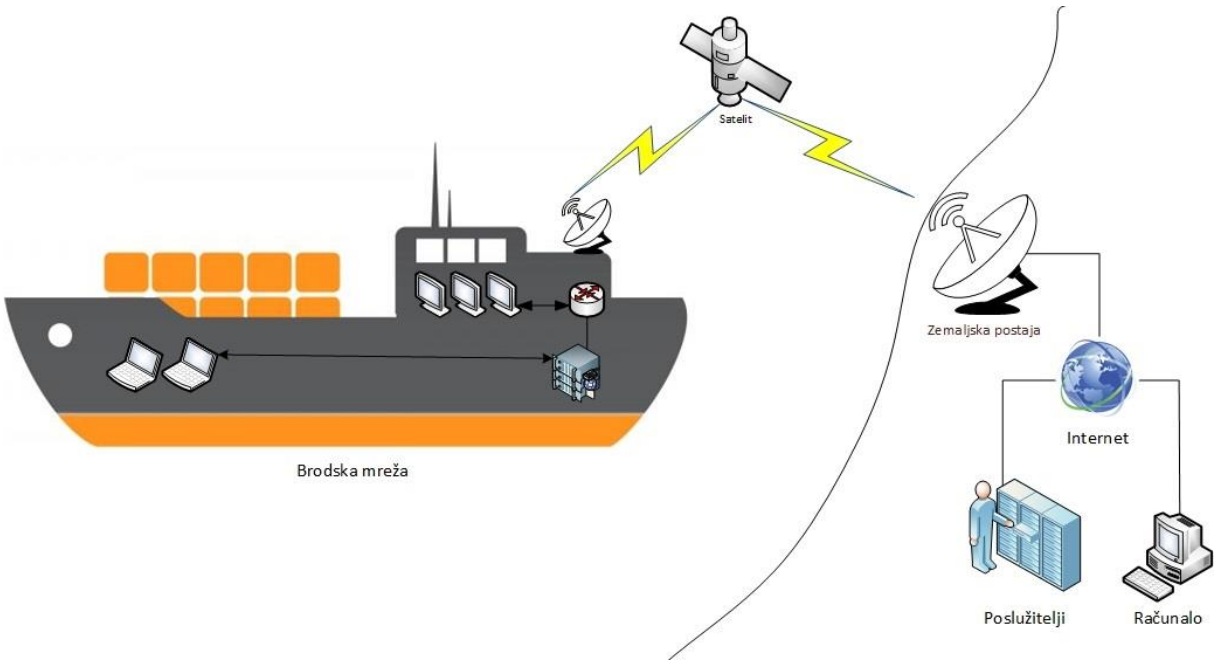
Nasuprot ovako definiranim ciljanim napadima, potrebno je spomenuti potkategoriju koju se naziva APT (Advanced Persistent Threat). Za APT napade možemo reći da su prvenstveno politički ili poslovno motivirani što ih i čini posebnim jer većinom svi ostali nalaze motivaciju u financijskoj dobiti. Cilj ovim napadima su velike korporacije, državne institucije i sve ostale infrastrukture za koje se smatra da posjeduju važne informacije koje nisu dostupne javnosti [9]. Središnju ulogu općenito u provođenju ciljanog napada ili pak APT napada imaju zloćudni programi koji su dizajnirani s točno određenim ciljem kako bi ostvarili namjere napadača.

5.1. Brodska mreža i pristup internetu

Za razumijevanje načina na koji su brodovi izloženi kibernetičkim prijetnjama ciljanih napada moramo prethodno proučiti na koji način je izveden pristup internetu. Iako su dosadašnjim računalnim napadima u pomorskoj industriji bili izloženi većinom infrastrukturni dijelovi kompanija koji su smješteni na kopnu, to ne umanjuje mogućnost napada na sam brod. Danas je na brodovima standardno omogućen satelitski pristup internetu koji se koristi u razmjenama poslovnih i privatnih informacija.

5.1.1. *Satelitski pristup internetu*

Satelitske sustave se koristi za prijenos širokopojasnih usluga kako bi na brodu mogli koristiti sve pogodnosti koje takve usluge pružaju. Mrežna izvedba na brodu se pretežito ne razlikuje od one na kopnu (Slika 10.). Preko antena se prima signal koji se putem koaksijalnih ili optičkih kabela prenosi do centralne jedinice sustava te dalje preko usmjerivača (engl. *router*) dovodi do krajnjih korisnika. Korisnici se mogu spojiti na mrežu LAN kabela, a kod modernih izvedbi je zastupljeno korištenje bežičnih pristupnih točaka [27].



Slika 10. Brodska mrežna infrastruktura

Jedan od standarda koji se koristi je sustav FleetBroadband, koji je razvila satelitska telekomunikacijska kompanija pod nazivom INMARSAT (International Maritime Satellite Organization). Sustav dolazi u tri različite inačice od kojih je najčešće korištena SAILOR FleetBroadband 500 te pruža pristup internetu pri brzini od 432 kbps. Na brodu ovaj sustav nalazi primjenu za korištenje standardnih internetskih usluga poput pristupa *web*-stranica, slanja elektroničkih poruka pa sve do ažuriranja podataka na ECDIS sustavima.

5.1.2. *Implementacija računalstva u oblaku*

Računalstvo u oblaku je novi oblik poslovnog modela koji se temelji na pružanju računalnih resursa kao usluge. Ovim pristupom omogućeno je razmjenjivanje računalnih resursa o potrebi, dok pod pojmom računalnog resursa smatramo cijela računala, aplikacije, memorijski prostor. Prednost korištenja računalstva u oblaku za pomorski sektor ogleda se u [28]:

- nižim troškovima za softver i hardver
- pristupu softveru i podacima bilo gdje na brodu gdje imamo pristup internetu
- nižim troškovima za održavanje samoga softvera i hardvera

- mogućnosti praćenja svih procesa koji se odvijaju s bilo kojeg računala
- poboljšavanju učinkovitosti zaposlenika

U računalstvu u oblaku postoje tri osnovne vrste poslovnih modela koji se razlikuju po uslugama koje pružaju. Redom, to su: infrastruktura kao usluga (engl. *Infrastructure-as-a-Service, IaaS*), platforma kao usluga (engl. *Platform-as-a-Service, PaaS*), softver kao usluga (engl. *Software-as-a-Service, SaaS*). Svaki od ovih modela ima svoje prednosti i nedostatke koji se ogledaju u korištenju, stoga za pomorstvo smatram da je model softvera kao servisa najviše korišten. Tim modelom aplikacija se nalazi instalirana na poslužiteljskom računalu te njoj mogu pristupiti svi njezini korisnici putem svojih uređaja. U pomorstvu ovaj model donosi brojne pogodnosti jer posjedovanjem jedne aplikacije koja se nalazi u oblaku pristup imaju svi – od broda do kompanije pozicionirane na kopnu. Kao primjer, može se raditi o aplikacijama za rukovanje teretom, izračunima stabiliteta broda i raznim drugim.

Korištenjem računalstva u oblaku, unatoč brojnim pogodnostima koje pruža, postajemo izloženi još većim sigurnosnim prijetnjama. Jedan od čestih napada je izazivanje prekida veze gdje napadač može slati prekomjeran broj zahtjeva za spajanje na koje poslužitelji ne mogu odgovoriti i time se zagušuje te prekida veza. Veliki rizik predstavlja ako se jedan od uređaja nađe pod zarazom od strane zlućudnog programa te tim činom napadač dođe u posjed pristupnih podataka za spajanje na poslužitelj. Još postoje brojne naprednije mogućnosti kojima napadač može provesti napad bazirane na iskorištavanju ranjivosti *web* aplikacija.

5.2. Softverska prijetnja Automatskog identifikacijskog sustava

Stupanjem na snagu IMO rezolucije A.917(22) [32] propisana je obaveza o ugradnji AIS uređaja od 1. 7. 2002. godine za sve brodove u međunarodnoj plovidbi od 300 bruto tona te za sve putničke brodove. Upotreba AIS sustava donijela je brojne pogodnosti u vidu praćenja pomorskog prometa i povećanja sigurnosti. Uređaj radi u interakciji s brojnim senzorima na brodu kako bi se dobilo pravovaljane informacije o koordinatama, brzini, kursu i ostalim informacijama koje sustav koristi.

Emitiranje podataka s AIS uređaja je autonomno i konstantno te se odvija na dvjema VHF frekvencijama: 161.975 MHz i 162.025 MHz. Podaci koji se razmjenjuju između AIS stanica mogu biti statički i dinamički. Pod statičke podatke spadaju oni koji se postavljaju ručno prilikom ugradnje uređaja poput MMSI broja (Maritime Mobile Service Identity) koji je ujedno identifikacijska oznaka broda, dok su dinamički odnosno promjenjivi podaci vezani za one koji se automatski ažuriraju, a daju nam informacije o koordinatama, brzini, navigacijskom statusu i svima ostalima koji su podržani ovim sustavom.

5.2.1. *Format i metoda razmjene podataka*

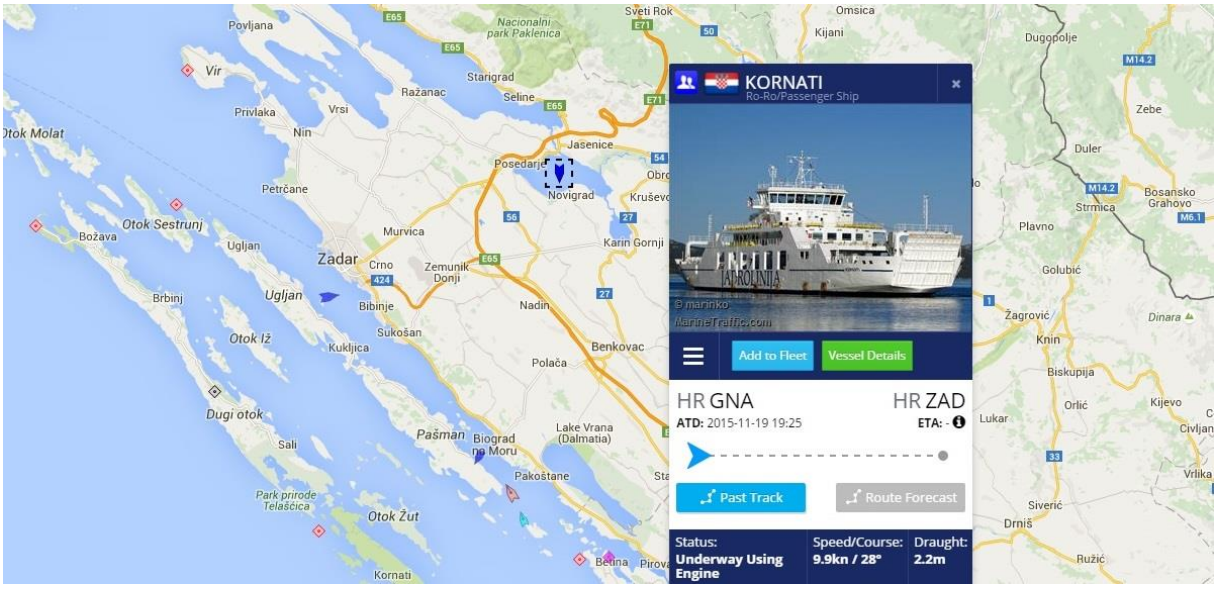
Podaci u ovome sustavu izmjenjuju se međusobno između brodova i postavljenih AIS obalnih stanica. Takav model je gotovo standardiziran te se putem interneta podaci dalje razmjenjuju s kontrolnim centrima. Kod AIS sustava postoje javni davatelji usluga, od kojih je poznatiji MarineTraffic.com, i državni koji posjeduju svoju vlastitu infrastrukturu.

Sadržaj i format poruka koje se razmjenjuju definirani su ITU preporukama [31] te se koriste za to posebno dizajnirani protokoli i načini kodiranja [33, 34]. Definirano je ukupno 27 vrsta poruka od kojih svaka ima svoju namjenu dok najvažnijima smatramo one koje šalju izvještaj o poziciji i kretanju broda. Primjer jednog podatka koji se razmjenjuje možemo prikazati kao rečenicu sadržanu nizom znakova koja se prilikom slanja koristeći NMEA [33] način kodiranja pretvara u binarni sadržaj.

5.2.2. *Prijetnja izvršena putem softvera*

Prijetnjom smatramo bilo kakvo ometanje koje onemogućuje pravovremeni rad i vjerodostojnost sustava. Istraživanjem koje je proveo istraživački tim tvrtke Trend Micro [30] angažirane u području računalne sigurnosti pokazani su broji nedostaci ovoga sustava. Jedan od njih vezan je za nedostatak provjere valjanosti podataka koji se razmjenjuju. Ovim propustom u osnovi svatko može kreirati lažni podatak s podacima od nekog postojećeg broda te zatim podatke poslati na server koristeći se za to predviđenim načinom. Ovaj primjer se odnosi na privatne javne poslužitelje čiji su podaci o adresi samog poslužitelja javno dostupni. Sukladno ovakvome propustu, možemo zaključiti da ako i državni AIS sustavi rade na isti način te ako bismo podatke poslali na njihove poslužitelje, postigli bismo isti učinak.

Koristeći se računalno programiranim algoritmom koji bi na temelju unesenih podataka stvorio binarni zapis, a potom NMEA kodiranjem smisleni podatak razumljiv sustavu, razvijamo sasvim novu prijetnju. Napadač je ovim činom u mogućnosti kreirati lažnu poziciju nekoga broda (Slika 11.) ili prikazati podatke o prijevozu opasnoga tereta što izravno može kršiti međunarodne propise i standarde o onečišćenju mora s brodova. Spektar mogućih prijetnji koji se ovim propustom omogućuju je golem te dovodi u pitanje sigurnost broda i posade.



Slika 11. Promjena lokacije broda

5.3. Ransomware kao nova prijetnja

Danas je sve rasprostranjenija vrsta zloćudnoga programa nazvanog *ransomware* upravo zbog otkupnine koju zahtijeva kako bi omogućio korisniku ponovni pristup podacima. Načelo funkcioniranja ovog programa krije se u korištenju kriptografskih metoda odnosno simetrične i asimetrične kriptografije koja se zasniva na RSA i AES (Advanced Encryption Standard) algoritmu. Nakon što računalo postane zaraženo ovom prijetnjom, *ransomware* kreće s pretraživanjem sadržaja na računalu ovisno o tome koju vrstu datoteke napadač želi kriptirati i samim time pristupa kriptiranju sadržaja.

Moderni *ransomwarei* koriste se kombinacijom simetrične i asimetrične kriptografske tehnike. Princip rada se zasniva na tome da se na zaraženom računalu generira ključ kojim enkriptira podatke. Zatim se taj ključ kriptira javnim RSA ključem koji *ransomware* prethodno preuzme s napadačeva servera. Jedini način da korisnik dođe do ključa kojim je obavljena enkripcija sadržaja je da sazna privatni RSA ključ koji je pohranjen na napadačevu serveru. Upravo je to uvjet kojim napadač traži otkupninu u zamjenu za privatni RSA ključ, pa bi se time dobio AES ključ [36].

Tipična otkupnina koju traže napadači je u iznosima od 100 do 10.000 dolara, a ponekad se potražuje da iznos mora biti plaćen virtualnom Bitcoin valutom [35].

5.4. Primjena društvenog inženjeringa u aspektu pomorstva

Kako je već prethodno obrađena tema društvenog inženjeringa, ovdje pobliže opisujem koji su načini primjene tih tehnika u pomorskoj industriji. U cjelokupnom području računalne sigurnosti najslabija karika su uvijek bili ljudi odnosno korisnici računalnih sustava. Kroz vrijeme se razvijaju sve bolji zaštitni mehanizmi, sigurniji načini prijave na sustave, novi kriptografski standardi, ali na razvoj ljudi možemo utjecati samo edukacijom. Vidimo da se tek od početka ove godine počelo nešto mijenjati po tome pitanju kada govorimo o pomorstvu. Unutar Internacionalne pomorske organizacije (engl. *International Maritime Organization*), Odbor za pomorsku sigurnost (engl. *Maritime Safety Committee*) donosi smjernice kako provoditi računalnu sigurnost na brodu. S tim ciljem izdaje spomenuti priručnik sa smjernicama i mjerama kao bi se rizik održao na prihvatljivoj razini. Bez obzira na ove smjernice, mnogi pomorci teško razumijevaju termine koji se koriste što je uzrok nedovoljnoj informatičkoj pismenosti. Upravo je to ono na što se napadači hvataju kada razmišljaju o planiranju napada na ovu industriju.

5.4.1. *Društvene mreže kao izvor informacija*

Zastupljenost društvenih mreža u modernom okruženju postaje standard za koji možemo reći da je to ujedno javno dostupni životopis i pregled privatnih aktivnosti osobe. Olako se shvaća privatnost i dijeljenje sadržaja s osobama s kojima komuniciramo putem interneta. Mnogi uživaju sve blagodati koje ovakve mreže pružaju te im upravo to postaje jedan od svakodnevnih sastavnih dijelova života. Kako pomorci čine veliku strukturu zaposlenika u industriji te su oni prije svega kao i svi ostali društvena bića, krećemo s pretpostavkom da također imaju svoje osobne mrežne profile.

Početni cilj napadača u planiranju ovakvih napada je doći do imena pomoraca koji plove na brodovima. Ovo i ne predstavlja neki veliki problem budući da preko javno dostupnih stranica raznih učilišta mogu saznati imena, od profesora pa sve do studenata. Takvim načinom razmišljanja pretpostavlja se da je netko od studenata pomorac ili poznaje nekog pomorca što lako provjeravaju pretragama putem društvenih mreža i ostalih mrežnih aktivnosti korisnika. Jedan od načina je da kontaktiraju direktno nekoga od zaposlenika unutar kompanije koristeći se spomenutim tehnikama lažnog predstavljanja ne bi li došli do imena.

Nakon što napadači dođu do osobe za koju smatraju da preko nje mogu izvršiti napad, slijedi provođenje društvenog inženjeringa. Postoji gotovo bezbroj tehnika, ili bolje reći umijeća, kojima napadač može manipulirati svojom žrtvom. Konačno napadač teži tome da na prijenosno računalo žrtve instalira zloćudni program imajući na umu da postoji šansa da se njime korisnik jednog dana spoji na brodsku mrežu.

6. ZAKLJUČAK

Računalna sigurnost je ozbiljno područje u gotovo svim djelatnostima gdje je prisutna uporaba računala. Svakodnevno smo kroz medije svjedoci sve većem broju pojave računalnih napada koji pogađaju kako privatne korisnike, tako i velike korporacije. Mnogi olako shvaćaju ovakve prijetnje budući da se radi o nečemu neopipljivom što se odvija u virtualnom prostoru, dok posljedice jasno daju do znanja upravo suprotno. Možemo reći, sukladno dokazima, da ova nova pojava koju nazivamo kibernetičkim prijetnjama zahvaća upravo i pomorsku industriju.

Kroz istraživanje provedeno u radu daje se jasan uvid o definiranju osnovnih termina koji se koriste u računalnoj sigurnosti te metodologiji korištenoj u provođenju računalnih napada. Za cilj je postavljeno upravo podizanje razine svijesti o postojanju prijetnji i ozbiljnosti posljedica ishoda napada. Početnom obradom teme postupno dolazimo do pregleda stanja iz aspekta pomorske industrije. Uvidom u dosadašnje napade koji su zadesili industriju kao polazišna motivacija stavljala se financijska dobit. Međutim, obrađivanjem teme i pogledom na novonastale situacije koje se sve više okreću oko terorističkih aktivnosti, smatram da ostvarivanje financijske dobiti nije jedina motivacija. Napadi sve više postaju politički orijentirani s ciljem nanošenja materijalne štete uz postojanje mogućnosti o ugrozi ljudskih života. Kao takve, ove prijetnje su prepoznale i ovlaštene organizacije koje su zajedno izdale smjernice kako bi se razina rizika od kibernetičkih napada svela na minimum.

U donošenju novih znanstvenih spoznaja o napadima kroz rad se obrađuje tema primjene društvenoga inženjeringa u svrhu dolaska do informacija o članovima posade. Ovaj oblik napada do sada još nije nigdje spomenut te provođenje preventivnih radnji u smislu edukacije može spriječiti njegovu pojavu. Općenito, kako bi se radilo na sprečavanju bilo kojeg oblika računalnih napada, može pomoći pravodobno informiranje zaposlenika u industriji. Smatram da postoji potreba za pronalaskom stručnoga kadra kako bi se kroz obrazovanje pomorca već u samim počecima moglo usaditi potrebno znanje o ovoj temi. Iako je samo spominjanje računalnih napada u pomorstvu tek u svojim počecima koji prate razvoj računalnih tehnologija, to ne znači da može biti zanemareno. Stoga je posebno važno naglasiti da svaki pojedinac mora prvenstveno sam težiti ulaganju u znanje ne bi li time doprinio cijeloj zajednici.

LITERATURA

[1] M. BAČA: „Uvod u računalnu sigurnost“, Narodne novine, Zagreb, 2004.

[2] M. GASSER: „Building a secure computer system“, Van Nostrand Reinhold Company, New York, 1988.

[3] S. ŠIMUNDIĆ, S. FRANJIĆ: „Računalni kriminalitet“, Sveučilište u Splitu, Split, 2009.

[4] C. H. J. WU, J. D. IRWIN: „Introduction to computer networks and cybersecurity“, CRC Press, 2013.

[5] …; „Computer security“, Wikipedia, 29 ožujka 2016 [Na mreži] dostupno na https://en.wikipedia.org/wiki/Computer_security

[6] N. N.; „Zakon o informacijskoj sigurnosti“, Narodne novine 79/07, 1. travnja 2016. [Na mreži] dostupno na http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti

[7] A. SOOD, R. ENBODY: „Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware“, Syngress, 2014.

[8] …; „Haker“, Wikipedia, 17. travnja 2016. [Na mreži] dostupno na https://hr.wikipedia.org/wiki/Haker

[9] CERT: „APT napadi“, Hrvatska akademska i istraživačka mreža, 14. veljače 2016. [Na mreži] dostupno na http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-12-333.pdf

[10] CERT: „Napredne tehnike socijalnog inženjeringa“, Hrvatska akademska i istraživačka mreža, 14 veljače 2016 [Na mreži] dostupno na http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-292.pdf

[11] SYMANTEC: „2016 Internet Security Threat Report“, Symantec Corporation, 3. ožujka 2016. [Na mreži] dostupno na https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[12] R. SALTZMAN, A. SHARABANI: „Active Man in the Middle Attacks“, OWASP AU, 2009.

[13] S. KIM, J. PARK, K. LEE, I. YOU, K. YIM: „A Brief Survey on Rootkit Techniques in Malicious Codes“, Journal of Internet Services and Information Security, 2012., p. 134-147.

[14] C. HADNAGY: „Social engineering: The art of human hacking“, John Wiley & Sons, 2010.

[15] C. HADNAGY: „Unmasking the Social Engineer: The Human Element of Security“ John Wiley & Sons, 2014.

[16] U. BAYER, I. HABIBI, D. BALZAROTTI, E. KIRDA, C. KRUEGEL: „A View on Current Malware Behaviors“, InLEET, 2009.

[17] CERT: „Stuxnet - malver za cyber rat“, Hrvatska akademska i istraživačka mreža, 14. veljače 2016. [Na mreži] dostupno na http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2011-03-324.pdf

[18] MSC: „The Guidelines on cybersecurity on board ships“, Maritime Safety Committee, 96th session Agenda item 4, 2016.

[19] MSC: „Guidelines for Cyber risk Management“, Maritime Safety Committee, 96th session Agenda item 4, 2016.

[20] MSC: „Measures aimed at improving cybersecurity on ships“, Maritime Safety Committee, 96th session Agenda item 4, 2016.

[21] CYBERKEEL: „Maritime Cyber Crime Risks“, Cyberkeel, 4. svibnja 2016. [Na mreži] dostupno na http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

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

[23] NNC GROUP: „Preparing for Cyber Battleships – Electronic Chart Display and Information System Security“, NCC Group Publication, 2014.

[24] O. FITTON, D. PRINCE, B. GERMOND, M. LACY: „The future of maritime cyber security“, Lancaster University, 2015.

[25] G. DEE: „Man in the Middle Attack made a 1.65 Million US Dollar Profit for Victimizing Three Businesses 2013“, 4. svibnja 2016. [Na mreži] dostupno na http://stayaway2.blogspot.hr/2013/12/man-in-middle-attack-made-165-million.html

[26] TRAPX SECURITY: „TrapX Discovers ‘Zombie Zero’ Advanced Persistent Malware“, 4. svibnja 2016. [Na mreži] dostupno na http://trapx.com/07-09-14-press-release-trapx-discovers-zombie-zero-advanced-persistent-malware/

[27] T. KUČIĆ, E. BABIĆ: „Internet na brodovima, Satelitski Internet“, Pomorski fakultet u Rijeci

[28] P. RISTOV, M. PERIĆ, V. TOMAS: „The implemetation of cloud computing in shipping companies“. Pomorstvo: Scientific Journal of Maritime Research, 2014., p.80-87.

[29] INMARSAT: „FleetBroadband Best Practices Manual“, 4. svibnja 2016. [Na mreži] dostupno na http://www.inmarsat.com/wp-content/uploads/2013/10/Inmarsat_FleetBroadband_Best_Practices_Manual.pdf

[30] M. BALDUZZI, A. PASTA, K. WILHOIT: „A security evaluation of AIS Automated identification system“, ACSAC ‘14 Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, 2014, pp. 436-445.

[31] INTERNATIONAL TELECOMMUNICATIONS UNION: „Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency ban“, Recommendation ITU-R M.1371-5, 2014.

[32] INTERNATIONAL MARITIME ORGANIZATION: „Guidelines for the onboard operational use of shipborne automatic identification systems (AIS)“, Resolution A.917(22), 2001.

[33] E. S. RAYMOND: „AIVDM/AIVDO Protocol Decoding“, 4. svibnja 2016. [Na mreži] dostupno na http://catb.org/gpsd/AIVDM.html

[34] E. S. RAYMOND: „NMEA Revealed“, 4. svibnja 2016. [Na mreži] dostupno na http://www.catb.org/gpsd/NMEA.html#GIDS

[35] UNITED STATES COAST GUARD: „Maritime Cyber Bulletin, 4. svibnja 2016. [Na mreži] dostupno na http://www.brymar-consulting.com/wp-content/uploads/Misc/MCB_004-16.pdf

[36] K. SAVAGE, P. COOGAN, H. LAU: „The evolution of ransomware“, Symantec, 4. svibnja 2016. [Na mreži] dostupno na http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[37] A. PASTERNACK: „To Move Drugs, Traffickers Are Hacking Shipping Containers“, 4. svibnja 2016. [Na mreži] dostupno na http://motherboard.vice.com/blog/how-traffickers-hack-shipping-containers-to-move-drugs

SAŽETAK

Prateći razvoj primjene računala u pomorskoj industriji postajemo sve svjesniji izloženosti računalnim napadima. Kako trend računalnih napada iz godine u godinu bilježi porast, raste potreba za uvođenjem novih sigurnosnih standarda i pravila. Pomorska industrija postaje interesantna napadačima upravo zbog važnosti u trgovačkom prometu kao i velikih novčanih transakcija koje se provode. Porastom prijetnji od terorističkih i piratskih napada dolazi do sasvim druge motivacije kojom napadači bivaju vođeni. Daljnjim konstantnim usavršavanjem tehnika kojima se koriste napadači u primjeni provođenja ciljanih napada razina održavanja sigurnosti sustava biva narušena. Upravo zato pomorska industrija treba težiti uvođenju potrebne edukacije u cilju povećanja informatičke pismenosti i svjesnosti o kibernetičkim prijetnjama. Iako se ovim pristupom otvara sasvim novo područje sigurnosti u pomorstvu, ono ne smije biti zanemareno.

KLJUČNE RIJEČI

pomorska računalna sigurnost; računalni napadi; kibernetičke prijetnje; ranjivosti

ABSTRACT

Evolution of the cyber threat in the maritime industry

Following the development of computer use in the maritime industry, we are becoming increasingly aware of our vulnerability to computer threats. As the trend of computer threats has been growing from year to year, there is a need to introduce new security and safety standards and rules. The maritime industry is becoming interesting to attackers because of its importance to trade traffic and large financial transactions carried out. The growth of terrorist and pirate threats results in a completely different motivation the attackers are driven by. Further constant improvement of techniques used by attackers in carrying out targeted attacks impairs the level of maintaining security and safety standards. Therefore, the maritime industry needs to strive to introduce education which aims at raising information literacy and awareness of cybernetic threats. Even though such an approach opens a completely new security and safety area in maritime industry, it should not be neglected.

KEY WORDS

maritime cyber security; cyber attack; cyber threat; vulnerability