Sigurnost podataka i informacija u sustavima nadzora i upravljanja pomorskim prometom

Security of Data and Information in Vessel Traffic Management Information Systems

Pančo Ristov
Pomorski fakultet
Sveučilište u Splitu
e-mail: panco.ristov@pfst.hr

Ante Mrvica
Jadrolinija d.o.o. Rijeka
e-mail: ante.mrvica@jadrolinija.hr

Pavao Komadina
Pomorski fakultet
Sveučilište u Rijeci
e-mail: komadina@pfri.hr

DOI 10.17818/NM/2016/1.7
UDK 656.61:007
Pregledni rad / *Review*
Rukopis primljen / *Paper accepted*: 5. 11. 2015.

Sažetak

Suvremeni nadzor i upravljanje pomorskim prometom zahtjeva implementaciju sve složenijih pomorskih procesa podržanih različitim aplikacijama, često uz interakciju s vanjskim svijetom. Informacijsku podršku u nadzoru i upravljanju pomorskim prometom (VTS služba) pruža sustav VTMIS, specijalizirani sustav za nadzor i upravljanje pomorskim prometom u našoj zemlji. S ciljem unaprjeđenja sigurnosti, efikasnosti i raspoloživosti komponenti sustava za nadzor i upravljanja pomorskim prometom potrebno je osigurati mehanizme nadzora i upravljanja sustavom kao cjelinom. Takvi mehanizmi prate ispravnost rada softverskih, hardverskih modula i ispravnost rada operatora, a sposobni su poduzimati i predefinirane korektivne akcije. Uspostava sustava za upravljanje informacijskom sigurnošću može biti od presudne važnosti kako bi se ostvarila i zadržala raspoloživost usluga koje pruža sustav za nadzor i upravljanje pomorskim prometom. Drugim riječima, neophodno je uvođenje sustava za upravljanje informacijskom sigurnošću informacijskih resursa u skladu s definiranim standardima.

KLJUČNE RIJEČI

VTMIS sustav
nadzor
upravljanje
sigurnost
upravljački centri

Summary

Modern control and management of maritime transport requires the implementation of increasingly complex marine processes supported by different applications, often with the interaction with the outside world. Information support for the control and management of maritime traffic (VTS service) is provided by a VTMIS system for control and management of maritime transport on Croatian coast. In order to improve safety, efficiency and availability of components of systems for control and management of maritime traffic it is necessary to ensure the mechanisms of control and management of the system as a whole. Such mechanisms monitor the correct operation of software, hardware modules and the proper operation of the operator, and they are able to undertake the pre-defined corrective actions. Establishment of a system for information security management can be crucial in order to achieve and maintain availability of services provided by the system for control and management of maritime transport. In other words, it is necessary to introduce the system for information security management of information resources in accordance with the defined standards.

KEY WORDS

VTMIS system
control
management
security
control centers

1. UVOD / *Introduction*

Svjetska trgovina kontinuirano raste i brodski promet je ključna komponenta u prijevozu robe. Za prijevoz robe koristi se sve manje malim te sve više velikim brodovima i na taj se način povećava konkurentnost u pomorskom prometu, tako da sigurni nadzor i upravljanje pomorskim prometom postaju sve složeniji. Za realizaciju svih poslovnih procesa u nadzoru i upravljanju pomorskim prometom koriste se suvremenim IT (Informacijska tehnologija) rješenjima implementiranima u VTMIS (*Vessel Traffic Management Information System*) sustavu. VTMIS sustav omogućava jednostavno povezivanje i komunikaciju između svih podsustava, kao i udaljeni pristup bilo kojeg ovlaštenog domaćeg i/ili međunarodnog pomorskog subjekta.

VTMIS sustavi su dizajnirani i implementirani korištenjem standardnih informacijskih komponenti. Osim sustava za nadzor i kontrolu pomorskog prometa uvode se nove aplikacije namijenjene povećanju sigurnosti pomorskog prometa i zaštiti mora i morskog okoliša.

Kao potpora u izvršavanju pomorskih procesa uvode se sustavi kao što su ekspertni sustavi, simulacijski sustavi, sustavi skladištenja podataka itd.

Kako bi se realizirao siguran VTMIS sustav koji će VTS službi i ostalim pomorskim subjektima osigurati kontinuirani i pouzdan nadzor i upravljanje pomorskim prometom uz minimalnu mogućnost otkaza hardverskih i softverskih modula, potrebno je VTMIS sustav sagledati kao cjelinu. VTMS sustav treba analizirati kao jedinstvenu cjelinu te primijeniti posebne mehanizme za svaki podsustav kojima se ostvaruju napredne mogućnosti nadzora i kontrole. Definiranje, implementiranje, održavanje i poboljšavanje sigurnosti podataka i informacija može biti od presudne važnosti kako bi se zadržala ili povećala sigurnost pomorskog prometa, zaštita mora i morskog okoliša i na taj način zadovoljile zakonske norme i standardi u pomorskom prometu.

Sustav sigurnosti je čitav niz mjera i postupaka za zaštitu podataka i informacija koji su u obradi, pohranjeni ili je u tijeku njihov prijenos od gubitka povjerljivosti, cjelovitosti i raspoloživosti samih podsustava i na taj način se osigurava funkcionalnost podsustava VTMIS sustava u pretpostavljenim pomorskim uvjetima.

Jedan od osnovnih koraka pri uspostavi sigurnosne politike je procjena ranjivosti sustava. Kroz procjenu rizika identificiraju se prijetnje računalnoj infrastrukturi organizacije i njezina ranjivost. Sigurnosna ranjivost definira se kao nedostatak koji zlonamjernom korisniku omogućava narušavanje sigurnosti sustava i/ili informacija. Cilj procjene ranjivosti je identifikacija potencijalnih rizika povezanih s različitim aspektima informacijskog sustava. Razne sigurnosne organizacije razvile su vlastite metode za njihovo sustavno praćenje [1].

2. VTMIS sustav / *VTMIS system*

VTMIS sustav sastoji se od podsustava za prikupljanje, procesuiranje, spremanje i dostavljanje podataka u skladu s EU (*European Union*), IMO (*International Maritime Organization*) standardima i SOLAS (*Safety of Life at Sea*) konvencijama. VTMIS sustav je izgrađen na načelima fleksibilne, otvorene i modularne arhitekture koja omogućava nadogradnju sa standardnim informacijsko-komunikacijskim komponentama. Programska podrška VTMIS sustava strukturirana je u module prema funkcionalnosti i općoj primjenjivosti unutar sustava. Integracija svih funkcijskih modula izvršena je sredstvima standardnih sučelja. Cjelokupni softver u sustavu mora ispunjavati ISO standarde: funkcionalnost, prenosivost, efikasnost**,** pouzdanost, pogodnost za održavanje i upotrebljivost. Za prijenos podataka i informacija između podsustava VTMIS sustava koristi se VPN (*Virtual Private Network*) mreža. Potporu hardverskim modulima pružaju mehanizmi kao što su: osiguranje neprekidnog napajanja, klimatizacija, sustavi za gašenje požara itd.

Podsustavi VTMIS sustava su: pomorski radarski podsustav, AIS (*Automatic Identification System*) podsustav, pomorski komunikacijski podsustav, CCTV (*Closed Circuit Television*) podsustav, meteorološki i hidrološki podsustav, radio goniometarski podsustav i upravljački (nacionalni, sektorski i lokalni) centri.

Od 2011. godine u probni rad, a zatim i u operativni rad, pušten je hrvatski VTMIS sustav. VTS služba obavlja sljedeće funkcije: prikupljanje podataka o pomorskim objektima i pomorskom prometu, praćenja i nadzor plovidbe, pružanje podataka pomorskim objektima (IS), organizacija plovidbe i upravljanje pomorskim prometom (TOS) i davanje plovidbenih savjeta i podrške u plovidbi pomorskim objektima (NAS). Vrsta i količina podataka i informacija koje se izmjenjuju između brodova i upravljačkih centara u HVTMIS prikazan je u tablici 1.; vidi [8].

2.1. Operatorske konzole / *Operator console*

Operatorska konzola je multifunkcionalna konzola. Kontakt operatora s informacijskim resursima odvija se uglavnom putem operatorske konzole koja je sastavni dio upravljačkog centra i ostalih podsustava. Operatorska konzola omogućava grafički prikaz informacija iz različitih izvora u visokoj rezoluciji (radarskih i video signala iz različitih izvora, npr. analognih i digitalnih radarskih signala, analognih i digitalnih signala iz TV ili IC kamere, sintetičkih signala poput raznih taktičkih simbola, mapa, itd), jednostavni unos podataka i upravljanje sustavom putem višerazinskih izbornika, unos podataka preko standardne tipkovnice, kugle ili programibilnih funkcijskih tipki, brzu obradu podataka, fleksibilnu učinkovitu analognu i digitalnu komunikaciju. Time predstavljaju sigurnosni rizik koji se mora odgovarajuće i tretirati. Operatori koriste operatorsku konzolu za komunikaciju između podsustava VTMIS sustava i vanjskih domaćih i međunarodnih pomorskih subjekata u razmjeni podataka i informacija, što povećava njezinu sigurnosnu izloženost.

2.2. Serveri / *Servers*

U svakom upravljačkom centru serveri pružaju platformu aplikacijama s ciljem realizacije usluga na kojima se temelje procesi u nadzoru i kontroli pomorskog prometa. Zbog takvog položaja serveri su istodobno i visokovrijedni i dobro zaštićeni informacijski resursi. Tijekom operativnog rada, pristup serverima

Tablica 1. Dostupnost podataka u VTMIS sustavu
Table 1 The availability of data in the VTMIS system

	Prekršaji	Nepotpuni AIS podaci	Nenajavljeni brodovi	IS+TOS+ NAS	Informacije	Savjeti	Upozorenja	Nadzor
2011.	86	181	98	844	226	59	189	365
2012.	68	260	228	2373	535	320	598	556
2013.	32	173	150	1983	438	432	432	355
2014.	100	219	100	-	514	299	627	-

dozvoljen je isključivo u kontekstu usluge koje pružaju i održavanje istih.

Ovisno o namjeni i konfiguraciji upravljačkih centara najčešće su korišteni aplikacijski, kao što su: VTS (*Vessel Traffic System*) server, server baze podataka, server zapisivanja i ponavljanja, server upozorenja i serveri opće namjene (Mobilni server, E-mail server, Web server i sl.).

2.3. Računalna mreža / *Computer network*

Neophodan podsustav za ispunjavanje funkcija podsustava VTMIS-a je pouzdan i elastičan komunikacijski podsustav koji će propustiti prave informacije do pravog odredišta bez zakašnjenja. Glavna komponenta komunikacijskog podsustava je računalna mreža. Za povezivanje računalnih elemenata unutar podsustava koristi se lokalnom računalnom mrežom, a za povezivanje podsustava između sebe većinom se koristi virtualnom privatnom mrežom. Suvremene aktivne dijelove predstavljaju inteligentni uređaji koji se sastoje od hardvera i programske podrške, a u većoj ili manjoj mjeri pate od ranjivosti svojstvenih računalu.

2.4. Primarni izvori podataka / *The primary sources of data*

Radarski sustav i AIS sustav su primarni izvori podataka u VTMIS sustavu. Prijenos podataka između primarnih izvora podataka i upravljačkih centara odvija se potpuno automatski. AIS uređaj s broda, u krugu dometa VHF radio veze, odašilje podatkovne pakete do prve AIS bazne postaje ili drugog broda. Podatkovni paketi šalju se u strogo definiranom redoslijedu koji je točno sinkroniziran preciznim vremenskim signalima iz globalnog sustava satelitske navigacije. Te vremenske signale brodski AIS dobiva iz GPS (*Global Positioning System*) prijemnika koji je sastavni dio AIS sustava. AIS sustav kao izvor podataka u VTMIS sustavu i otvorenoj razmjeni podataka između brodova i AIS bazne stanice povećava njegovu sigurnosnu izloženost.

3. PRIJETNJE RADU VTMIS SUSTAVU / *Threats to VTMIS System Operation*

Prijetnja sigurnosti VTMIS sustava je svaki događaj koji može izazvati narušavanjem integriteta, pouzdanosti i dostupnosti podataka i informacija. Svaka prijetnja i neovlašteni pristup VTMIS sustavu ima različite posljedice na stanje izvršavanja poslovnih procesa u upravljačkim centrima ili na sigurnost odvijanja pomorskog prometa. Mehanizmi informacijske sigurnosti suprotstavljaju se takvim prijetnjama. Na temelju prakse i znanstvene literature treba imati na umu da je nemoguće imati savršenu sigurnost podataka i informacija.

Prijetnje mogu nastati spontano (kvarovi, nesavršenost hardverskih i/ili softverskih modula, nepažnja i sl.) ili namjerno kao posljedica zlonamjerne aktivnosti. Prijetnja koja se uspije materijalizirati izaziva privremeni ili trajni gubitak podataka i/ili informacija. U skladu s time modeliraju se očekivana vremena do oporavka nakon nastanka pojedinog kvara, posebno kvar kritičnih komponenata unutar upravljačkih centara i podsustavi podržani računalom, a jednako tako i mjera i postupaka u slučaju trajnog kvara.

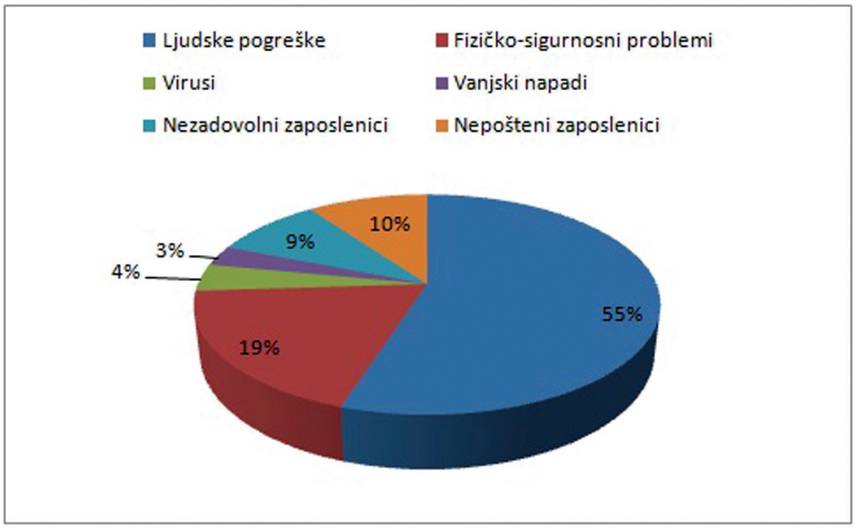
Na temelju istraživanja koja su obavljena i objavljena pokazuju da je za distribuirane sustave, kao što je VTMIS sustav, najveća prijetnja za sigurnost podataka ljudski faktor, odnosno operatori u upravljačkim centrima i drugim podsustavima.

Da bi prijetnja mogla utjecati na sigurnost informacijskih resursa, pa tako i na kritične komponente, treba postojati način pristupa sustavu. Mogući načini pristupa su: veza s Internetom (službene i neslužbene pristupe Internetu od strane ovlaštenih pomorskih subjekata), izravne ili neizravne veze s brodovima, veze s ovlaštenog servisa/proizvođača opreme, satelitske i radio veze, koje uvijek mogu biti ugrožene grješkama na prijenosnom putu [14]. Također su osjetljive pristupne točke pomorskih subjekata koje traže pojedine usluge, kao i zlonamjerno oblikovani IP (*Internet Protocol*) paketi, napadi fragmentacijom IP paketa, ranjivost protokola SNMP (*Simple Network Management Protocol*), otvorenost TCP (*Transport Control Protocol*) i UDP (*User Datagram Protocol*) priključaka za određene usluge koje koriste umrežena računala, kao i nekontrolirani pristup preko USB priključka.

Posebna kategorija prijetnji su zlonamjerne aktivnosti, bilo da potječu od zaposlenika ili izvana. Takve aktivnosti imaju obilježja kriminalnog djela. Tako npr. ubacivanje krivih informacija u pakete AIS poruka, pirati, krijumčari ili teroristi mogu iskoristiti za izvršavanje nečasnih i opasnih aktivnosti na brodu ili bilo kojem objektu na obali.

3.1. Kvarovi / *Failures*

Kvarovi hardvera posljedice su mehaničkog trošenja, lošeg procesa proizvodnje, slabe kontrole proizvodnje, ugradnje loših elemenata, ljudskih pogrešaka tijekom proizvodnje i dizajna ili više sile. Kvarovi koji se mogu pojaviti kod sklopovlja mogu biti trajni, povremeni i prolazni. Tretiraju se kao statistički, uglavnom kroz pokazatelje pouzdanosti i raspoloživosti računalnih sustava. Postoje četiri načina za povećanje pouzdanosti hardverskih modula: ugradnja pouzdanih elemenata; dizajn sustava na takav način da otkaz pojedinog modula ne može izazvati pad



Slika 1. Vrste prijetnji

Figure 1 Types of threats

cijelog sustava; nabavka elemenata iz više izvora i ugradnja suvišninih elemenata s brzim prebacivanjem na suvišni element.

Iz prakse i stručne literature prihvaćeno je pravilo da u svakom programu ima pogrešaka. Pogreška programa može biti posljedica pogrešaka u kodu, pogrešnog korištenja, pogrešne interpretacije specifikacija koju softver treba zadovoljiti (nestručnosti programera), primjene neodgovarajućih testova ili drugih nepredviđenih problema. Programske pogreške ne možemo izbjeći iz dva razloga: kontrola programa se još uvijek provodi na razini pojedinačnog softverskog modula i programiranje i programsko inženjerstvo se mijenjaju i razvijaju puno brže nego tehnike u računalnoj sigurnosti. Iz softverske se prakse zna da je nemoguće generirati potpuno ispravni programski modul.

3.2. AIS sustav / *AIS system*

Na temelju primjene AIS sustava u stvarnim uvjetima uz sve pozitivne osobine koje AIS sustav nudi operatorima u upravljačkim centrima i pomorcima na brodu, pojavljuju se mane. Tako npr., u slučaju izostanaka prijema sinkronizirajućeg signala zbog problema globalnog sustava satelitske navigacije ili kvara GSP prijemnika [15], AIS sustav ne bi ispravno funkcionirao. Iz tog razloga nastao bi problem u praćenju pomorskog prometa, posebno u područjima gdje VTS radari ne bi detektirali brodove, posebno mala plovila zbog kratkog radarskog horizonta i male moći tih radara. Osim toga, otvorena komunikacija AIS sustava s ostalim pomorskim subjektima predstavlja ranjivost koju je moguće koristiti u destruktivne namjene na razne načine (zlonamjerne aktivnosti). Primjerice, ukoliko se mijenjaju i krivotvore pojedini statički i/ili dinamički (identitet broda, lokacija, kurs, brzina plovidbe) podaci broda, isti neće biti sumnjiv VTS službi, pa će uljez prići ciljanom objektu i izvršiti kriminalne aktivnosti. AIS protokoli nemaju nikakvih sigurnosnih funkcija kojima se utvrđuje identitet, valjanost i vjerodostojnost. Budući da je većina trgovačkih brodova opremljena ovakvim sustavima, zabrinjavajuće je što IMO kao regulatorno tijelo koje njegovu upotrebu i nalaže, nije naložilo nikakve izmijene spomenutog protokola ili bilo koju drugu metodu kojom bi se ovaj sigurnosni propust eliminirao.

3.3. Ljudski faktor / *Human factor*

Ovisno o namjeni sustava, čovjek sudjeluje u rukovanju i održavanju ili je u ulozi operatora. Zato ljudi unose određenu količinu nesigurnosti. Ovisno o pažnji koja je posvećena procesu rada prilikom implementacije i/ili prilikom izvršavanja događaju se pogreške, od neispravno donijete odluke u pomorskom prometu do masovnih sustavnih pogrešaka kao što je nevođenje računa o upozorenjima koje generiraju dijagnostički programi. Čimbenici koji utječu na pouzdanost čovjeka su: stres, vrijeme, edukacija, uvjeti (ergonomija), procedure i dr.

Uloge i odgovornosti zaposlenika u VTS službi je potrebno definirati i dokumentirati u skladu sa sigurnosnom politikom. Tijekom aktivne službe dobro je da se osoblju VTS službe pruži kontinuirana edukacija u pogledu informacijske sigurnosti i to s ciljem podizanja razine svijesti o sigurnosti podataka i informacija u kontroli, upravljanju i organizaciji pomorskog prometa.

4. UPRAVLJANJE SIGURNOŠĆU VTMIS SUSTAVOM / *VTMIS system security management*

Sigurnost VTMIS sustava je složen dinamički proces u kojem je jasno da, bez kvalitetnog sustavnog pristupa sigurnosti, sustav nije moguće u cijelosti zaštiti. Teorija sigurnosti kaže da je sigurnost cijeloga informacijskog sustava uvijek proporcionalna sigurnosti njegove najslabije (kritične) točke.

Sveobuhvatni pristup postignut je implementacijom i primjenom standardiziranih sustava za upravljanje informacijskom sigurnošću (*Information System Management System - ISMS*) što predstavlja skup standarda koji adresiraju različite aspekte informacijske sigurnosti. Najpoznatiji i najopćenitiji sustav za upravljanje informacijskom sigurnošću definiran je standardom ISO/IEC 27001:27005. Standard opisuje model za zasnivanje, uspostavu, vođenje, nadgledavanje, reviziju, održavanje i usavršavanje ISMS sustava. Implementacija standarda odvija se kroz dvije faze. Prva faza je tzv. administrativna u kojoj menadžment osigurava punu podršku implementaciji. Druga se faza odvija kroz nekoliko koraka: određivanje opsega i granice ISMS, definiranje politike ISMS, evidencija imovine, procjena rizika, donošenje dokumenata „Izjava o prihvatljivosti" (*Statement of Applicability* - SoA), prihvaćanje i odobrenje uprave, implementacija ISMS-a, izrada procedure za upravljanje incidentima, provođenje nadzora, identifikacija i implementacija itd. Standard razlikuje dvije vrste zahtjeva za upravljanje informacijskom sigurnošću: metodološki zahtjevi i zahtjevi za sigurnosne kontrole (Anex A).

Potrebno je izvoditi provjeru učinkovitosti ISMS-a uzimajući u obzir rezultate sigurnosnih ispitivanja, incidente, rezultate mjerenja učinkovitosti, prijedloge i povratne informacije svih uključenih strana. Ključni dokument koji se u cijelom projektu implementacije koristi kao temelj za donošenje odluke uprave o konačnom prihvaćanju strukture ISMS je „Izjava o prihvatljivosti". U dokumentu se točno definira koje sve kontakte treba primijeniti u organizaciji kako bi se uspostavio planirani ISMS.

5. NADZOR I UPRAVLJANJE SIGURNOŠĆU PODATAKA I INFORMACIJA VTMIS SUSTAVA / *Control and management of data and information security of the VTMIS system*

Upravljanje sigurnošću računalnih resursa može se promatrati na dvije razine, i to: na razini pojedinih elemenata podsustava i upravljanje cjelovitim VTMIS sustavom.

Prema istraživanju o računalnoj sigurnosti u pomorskom sektoru agencije za mrežnu i informatičku sigurnost Europske unije (*European Network And Information Security Agency)*, upozoreno je na nekoliko nedostataka, a neki od važnijih problema koji su pronađeni su sljedeći [6]:

- Svijest o problemima vezanim za računalnu sigurnost u pomorskoj industriji je niska ili nepostojeća, zbog čega je svim pomorskim subjektima preporučeno da poduzmu potrebne korake kako bi se to promijenilo.
- Preporučeno je da se što boljim tehničkim karakteristikama kritičnih računalnih i komunikacijskih komponenti osigura njihova sigurnost.
- Budući da su pomorski zakoni i regulative, koji su trenutno na snazi, usmjereni samo na fizičku zaštitu, preporučeno je dodavanje pravila koja bi se odnosila na aspekt računalne sigurnosti.
- Također je preporučen holistički pristup, na temelju procjene

računalnoga sigurnosnog rizika imajući pritom u vidu posebnosti pomorske industrije.
- Upozoreno je i na potrebu ujednačavanja nacionalnih zakona članica, zakona Europske unije i regulativa IMO-a u sektoru računalne sigurnosti, kao i na bolju razmjenu informacija i statističke podatke iz računalne sigurnosti.

5.1. Nadzor i upravljanje elementima podsustava VTMIS sustava / *Control and management of subsystem elements of the VTMIS system*

a. Operatorska konzola / *Operator console*

Operatorska konzola predstavlja sučelje između informacijskih resursa sustava i čovjeka i zbog toga predstavlja jednu od prvih linija obrane protiv prijetnji koje dolaze, kako izvana, tako iz samih zaposlenika u podsustavima. Osnovni uvjet za sigurnost same operatorske konzole je upravljanje pristupom operatora i ostalih ovlaštenih osoba. Potrebno je omogućiti samo autorizirani pristup i spriječiti neautorizirani pristup. Da bi se to omogućilo, dobro je osigurati formalne procedure za kontrolu pristupa informacijskim resursima i uslugama. Zaštitni sustav operatorske konzole sastoji se od centralnog upravljanja sustavom antivirusa, lokalnog vatrozida, lokalnog sustava za otkrivanje upada, sustava za sakupljanje dnevničkih zapisa (sigurnosne događaje i sigurnosne incidente), skeniranje računala, konfiguriranje računala radi sprečavanja sigurnosnih prijetnji, centralnog sustava za upravljanje korisničkim računima i procedure za instalaciju redovitih osvježavanja i zakrpa.

b. Server / *Server*

Serveri u upravljačkim centrima predstavljaju kritičnu komponentu i prva linija obrane je tzv. očvršćivanje. Postupak očvršćivanja servera uglavnom se svodi na modificiranje instalacije operacijskog sustava i/ili aplikacije kako bi se smanjio broj ranjivosti. Druga linija je implementacija sustava otkrivanja neovlaštenog upada u računalni sustav. Sustavi za otkrivanje i sprječavanje upada su nove tehnike za zaštitu od zlonamjernih upada u računalni sustav. Ovaj sustav može se implementirati na jednom računalu (*Host Intrusion Detection System*), cjelokupnoj mreži (*Network Intrusion Detection System*) i mješoviti sustav.

Najčešći napad na servere je distribuirano uskraćivanje usluga (*Distributed Denial of Service-DDoS*) koji pruža server. Trajanje i scenariji su najvažnije karakteristike DDoS napada. U izvješću laboratorija Kaspersky, broj i trajanje DDoS napada u četvrtom kvartalu 2014. i prvom kvartalu 2015. prikazani su u tablici 2. [7].

Tablica 2. Trajanje DDoS napada u Q1 2015 i Q4 2014

Table 2 Duration of DDoS attacks in Q1 2015 and Q4 2014

Trajanje napada (h)	Broj napada u Q4 2014	Broj napada u Q1 2015
150+	5	0
100-149	8	3
55-99	299	121
20-49	735	433
10-19	1679	703
5-9	2161	1426
0-4	8425	9594

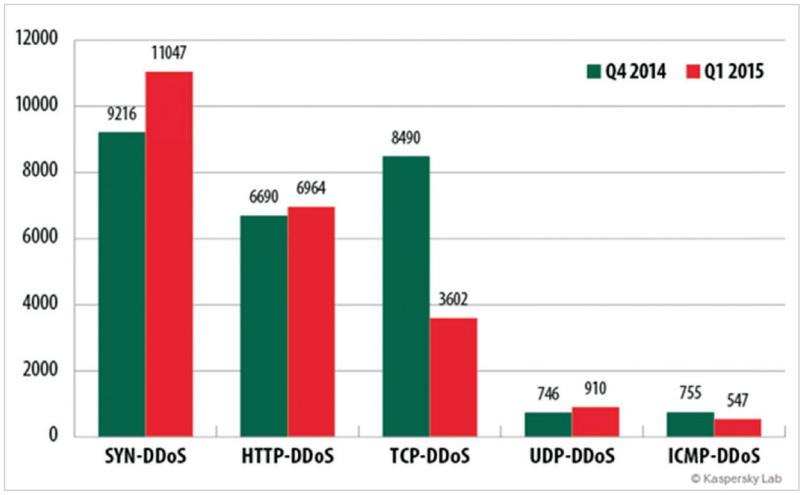
U VTMIS sustavu postoji namjenski server za sakupljanje dnevnika operacijskog sustava, dnevnika aplikacija i dnevnika dijagnostičkog podsustava. Na taj način središnji nadzorni sustav može pratiti točno izvršavanje aplikacijskog sustava i na taj način korištenje usluga koje pruža VTMIS sustav. Zbog povećanja sigurnosti pomorskog prometa i zaštite od kvarova u svim upravljačkim centrima kritični serveri kao što su VTS server i server distribuirane baze podataka su u toploj redundanciji.

U današnje vrijeme najčešći DDoS napad je *flood* (plavljenje servisa) napad u kojem se šalje veliki broj legitimnih ili lažiranih zahtjeva prema određenom servisu, čime se troše resursi servera pa se krajnjim korisnicima otežava ili onemogućava pristup. Prema izvješću laboratorija Kaspersky najčešće korišteni napad je SYN-DDoS (sinkronizacija klijenta s poslužiteljem) i TCP-DDoS napad. Manje korišteni DDoS napadi su UDP- DDoS i ICMP (*Internet Control Message Protocol*) DDoS.

c. Virtualna privatna mreža / *Virtual private network*

Za povezivanje računalne infrastrukture unutar podsustava VTMIS sustava koristi se VPN mreža. VPN mreže to čine "preusmjeravanjem" prometa putem Interneta ili neke druge javne mreže na način koji pruža istu sigurnost i značajke kao i privatna mreža. VPN mreža preko javne mreže stvara sigurni kanal „tunel" između dvaju krajnjih čvorišta. Tunel može biti stalni ili privremeni. Zahvaljujući VPN vezi, putem javne mreže mogu se prenositi podaci koristeći se infrastrukturom preusmjeravanja na Internetu. Prednost ovog rješenja je nezavisnost od tehnologije prijenosa jer je uvijek potrebna samo internetska veza, tako da se za prijenos može koristiti bilo koja komercijalna raspoloživa tehnologija.

VPN mreža mora ispunjavati nekoliko sigurnosnih zahtjeva: povjerljivost podataka (VPN mreža mora osigurati



Slika 2. Najčešće korišteni tipovi DDoS napada u Q4 2014 i Q1 2015 [7]

Figure 2 The most frequently used types of DDoS attacks in Q4 2014 and Q1 2015

kriptiranje podataka tako da nitko, osim servera, ne može pročitati. To se postiže korištenjem algoritmom kao što su DES, RSA i Diffie Hellman), autentifikacijom i autorizacijom (VPN mreža mora verificirati strane uključene u uspostavu VPN tunela, a može se izvršavati na razini prespojnika i razini poslužitelj – klijent), integritetom podataka (VPN mreža mora osigurati provjeru jesu li podaci promijenjeni - za ispunjenje ovog zahtjeva najčešće se koristi MD5 algoritam), prava pristupa (VPN mreža osigurava provjeru identiteta korisnika i dopušta VPN pristup samo registriranim korisnicima). Osim toga, VPN mreža mora osigurati mogućnost praćenja događaja.

Vodeća IT tvrtka na polju sigurnosti računala, RSA Research, objavila je detaljan izvještaj o napadima koji su se odvijali preko VPN mreže. Napadi preko VPN-a, koje su istraživači nazvali prema Terracotta mreži, su koristile različite APT (*Advanced Persistent Threat*) grupe, a svakako poznatija među njima je *Shell Crew*, odnosno *Deep Panda*. Ciljevi napada su najčešće vojne i IT kompanije, kao i vladine organizacije, kako bi došli u posjed tajnim dokumentima koji se tiču osjetljivih projekata. Napadi se odvijaju preko komercijalnih VPN servisa. Najveći sigurnosni problem predstavlja korištenje slabijih algoritama za šifriranje tijekom tuneliranja prometa.

d. AIS sustav / *AIS system*

S ciljem povećanja sigurnosti rada AIS sustava mora se poduzeti više koraka. Prvi korak je omogućiti autorizirani pristup tijekom puštanja u rad ili operativne uporabe i spriječiti neautorizirani pristup. Da bi se to omogućilo, dobro je osigurati formalne procedure za kontrolu pristupa statičkim podacima, dinamičkim podacima, podacima o plovidbi i sigurnosnim podacima. Drugi korak je povećati pouzdanost GPS prijemnika kako bi se povećala njegova osjetljivost ili ugraditi hladnu ili toplu redundanciju. Otvorena komunikacija AIS sustava predstavlja ranjivost koja se može iskoristiti u destruktivne svrhe. Zbog toga, nadležne međunarodne i domaće pomorske institucije moraju razmišljat o šifriranju/kriptiranju AIS podataka. Za povećanje sigurnosti cijelog sustava najjednostavnije je udvostručiti cijeli sustav ili pojedine komponente kao što je GPS prijemnik.

5.2. Nadzor i upravljanje cjelovitijom sigurnošću VTMIS sustavom / *Control and management of a more comprehensive security of the VTMIS system*

Da bi se realiziralo učinkovito upravljanje sigurnosnim mehanizmima u VTMIS sustavu funkcije upravljanja, potrebno je generalizirati i centralizirati. Centralizirani sustav omogućio je učinkovitiju kontrolu informacija i provođenje sigurnosne politike sustava. U tu svrhu primjenjuju se sustavi namijenjeni upravljanju informacijskim sustavom. Tako npr. poznata pomorska Norveška tvrtka Kongsberg proizvela je sustav za upravljanje informacijskim sustavom K-IMS (*Kongsberg Information Management System*). Ispravnom uporabom takvih sustava bitno se pridonosi podizanju i održavanju visoke razine sigurnosti informacijskog sustava u cjelini.

5.2.1. Upravljanje kontrolom pristupa temeljenom na korisničkim ulogama / *Access control based on user roles*

U informacijskim sustavima mehanizmi kontrole pristupa ograničavaju korisnike i procese u smislu izvođenja različitih operacija nad objektima, kao što su datoteke, TCP/UDP priključci, itd. Za svaku takvu akciju mehanizmi kontrole pristupa dodjeljuju svakom korisniku posebne ovlasti za obavljanje određenih akcija na računalu. Kad se spominje kontrola pristupa, uzimaju se u obzir četiri situacije: sprečavanje pristupa, ograničavanje pristupa, dozvola pristupa i oduzimanje prava pristupa.

Prema metodama implementacije kontrole pristupa modeli se dijele na: diskrecijski model (*Discretionary Access Control*), mandatori model (*Mandatory Access Control*) i model grupa i uloga (*Role-based access control* - RBAC) [5].

Za sustave kao što je VTMIS sustav najprikladniji je model RBAC iz razloga što je sustav uloga definiran skupom uloga koje su uobičajeno vezane za dužnosti koje subjekti obnašaju u VTS službi. Svaka uloga ima određene ovlasti te svi zaposlenici koji imaju određenu ulogu, imaju i ovlasti te uloge. U velikim sustavima potrebno je imati nekoliko grupa i funkcijskih uloga koje se dodjeljuju zaposlenicima, tj. grupu definira skup određenih pravila, a ulogu uređeni skup prava pristupa koja se mogu, u nekom razdoblju uporabe određenog resursa, vezati uz pravila [5]. U VTS službi definirane su sljedeće uloge: VTS operator, voditelj VTS smjene, VTS nadzornik, VTS instruktor, VTS menadžer i VTS tehničko osoblje. Zaposlenik u VTS službi može imati jednu ili više uloga. RBAC model dozvoljava kombiniranje uloga, a to je jako bitno u organizaciji VTS službe. Tako npr. u upravljačkom centru jedna osoba istovremeno može biti u ulozi voditelja VTS smjene i VTS nadzornika.

U RBAC modelu korisnicima se ne dodjeljuju prava pojedinačno, već preko uloga, pojednostavljuje se dodjela ovlasti kao i dodavanje ili brisanje korisnika. U ovom modelu se dodjeljuje značenje svakoj dozvoljenoj operaciji nad objektima. Tako npr. u operaciju „kreiranje računa za pruženu uslugu“ ima određeno značenje za neki objekt. Osim toga, model dozvoljava da jedna uloga može imati više prava, pravo pristupa se može dodijeliti različitim ulogama. Npr., pravo pristupa daljinskog upravljanja radarskim sustavom može dodijeliti VTS operatoru i voditelju VTS službe. Potrebno je utvrditi jesu li uloge dodijeljene zaposlenicima VTS službe prikladne i funkcioniraju li implementirane sigurnosne kontrole kako je očekivano.

5.2.2. Upravljanje programskom podrškom / *Software support management*

U složenim informacijsko-komunikacijskim sustavima neophodno je potrebno implementirati i funkciju upravljanja programskom podrškom i na taj način povećati cjelokupnu računalnu sigurnost. U takvim sustavima na serverima i operatorskim konzolama „vrte“ se brojne aplikacije i servisi. Posebno su serveri opće namjene osjetljivi na vanjske napade. Ova funkcija nastoji osigurati poštivanje sljedećih pravila: na računalima se nalaze potrebni programi; na računalima se nalaze samo dozvoljeni programi i verzije programa koje se nalaze na računalima najnovijeg su datuma. Nepoštivanje bilo kojeg od gore nabrojanih pravila negativno utječe na sigurnost cjelokupnog sustava. Funkcija upravljanja programskom podrškom poželjno je implementirati u VTMIS sustav zato što aplikacijski i serveri opće namjene te računala opće namjene (operatorske konzole) su po svojoj namjeni mnogobrojni i po hardverskoj i softverskoj konfiguraciji potpuno jednaki.

Programska podrška za upravljanje

cjelokupnim softverom posjeduje bazu različitih verzija aplikativnog i sustavnog softvera. U toj bazi vode se sljedeći atributi: naziv i oznaka verzije, na kojem računalu/serveru je instalirana, status verzije (aktivna ili pasivna), datum instalacije, datum deinstalacije, oznaka medija, izvršitelja instalacije/deinstalacije i sl.

Poseban slučaj upravljanja programskom podrškom je obrana od virusa i drugog zloćudnog koda. Osobnosti virusa su: teško se prepoznaje, teško se uništava ili deaktivira,ima široko područje širenja, posjeduje mogućnost reinfekcije, lako se kreira i strojno je neovisan. Zbog svih ovih karakteristika, sustav za upravljanje programskom podrškom sastoje se od središnjeg servera koji kontinuirano preuzima najnovije virusne definicije i distribuira ih prema antivirusnim klijentima koje se nalaze na štićenim računalima.

Kod VTMIS sustava koriste se antivirusni sustavi na operatorskim konzolama i serverima opće namjene. Što se tiče aplikacijskih servera vrlo je malena vjerojatnost zaraze virusom. Velika vjerojatnost zaraze je za server baze podataka iz razloga što pojedini pomorski subjekti preko pristupnih točaka mogu koristiti podatke o plovilima. Zaro je potrebno propisati posebne fizičke i administrativne kontrole koje se jednostavno implementiraju.

5.2.3. Registracija sigurnosnih događaja i incidenata / *Registration of security events and incidents*

Suvremena informatička tehnologija omogućava razvoj i implementaciju novih tehnika s mogućnošću da se vjerojatnost nastupa otkaza smanji na najmanju mjeru, odnosno ugradnja tehnike dijagnostike u sklopu svakog modula računalnog sustava već je u fazi dizajna. Dijagnostički sustav treba uspješno riješiti probleme ispitivanja funkcionalnosti sustava tijekom aplikacijskih programa i dijagnosticiranja neispravnosti u slučajevima detekcije neispravnog funkcioniranja, a da bi se omogućilo pravodobno interveniranje i otklanjanje neispravnosti te se ponovno uspostavila raspoloživost sustava. Pojedine aplikacije koje obrađuju sigurnosno osjetljive informacije za neke od kritičnih operacija prijavljuju identitet njihovog pokretača. Zbog toga je potrebno kontinuirano zapisivanje svih događaja od rada stroja do aktivnosti operatora u realnom vremenu. Ovaj mehanizam praćenja rada sustava kroz neko razdoblje omogućava uvid u rad sustava, a samim time i pomoć u procjeni sigurnosti kritičnih točaka, određivanje uzorka nepredviđenih događaja te otklanjanje sigurnosnih propusta. Zapisi se trebaju čuvati određeno razdoblje kako bi se mogle upotrijebiti u budućim istragama i nadzorima kontrole pristupa. Zapisi trebaju biti zaštićeni od neovlaštene modifikacije. Tehnologija za čuvanje zapisa u VTMIS sustavu temelji se na serverskoj tehnologiji.

5.2.4. Nadzor stanja sustava / *System condition monitoring*

S ciljem očuvanja sigurnosti VTMIS sustava potrebno je uključiti neku od tehnologija za nadzor u upravljanje računalnim resursima. Upravljanje računalnim resursima treba shvatiti kao metodologiju koja opisuje uporabu različitih automatiziranih alata, tehnika i sustava te omogućuje upravljanje mnogobrojnim uređajima i sustavima dostupnim u tipičnim distribuiranim arhitekturama.

Programska podrška za upravljanje i nadzor u najvećoj mjeri utemeljena je na protokolu SNMP. SNMP je najrasprostranjeniji protokol predviđen za rad na TCP/IP mrežama, odnosno upravljanje umreženim računalima i uređajima.

SNMP protokol definira dva osnovna entiteta, menadžere i agente. Menadžer je server koji izvršava softver za upravljanje i nadzor i koji je odgovoran za cijelu mrežu ili dio mreže. Agent je dio softvera implementiran u neki upravljivi objekt i ima dvojaku ulogu. Prvo, agent osluškuje u potrazi za dolaznim SNMP zahtjevima koje šalje menadžer te odgovara na njih i drugo, agent nadgleda događaje na sustavu gdje se nalaze i stvaraju tzv. SNMP klopke (*SNMP traps*) obavijesti koje šalje menadžeru serveru i obavještava ga kako se nešto dogodilo.

SNMP menadžer je obično konfiguriran tako da dohvaća ključne podatke s nadziranih uređaja periodički koristeći *SNMP get* zahtjeve. SNMP agent ima mogućnost, ne samo odgovoriti na zahtjeve, već i samoinicijativno slati podatke. *SNMP trap* predstavlja informaciju koju šalje agent ukoliko se dogodio nepredviđeni događaj. Postoje veliki broj obavijesti (klopki) koje agent može poslati i oni najviše ovise o tipu uređaja koji se nadzire. Administrator sustava određuje koje će se klopke obrađivati, a koje odbacivati. Pored toga, postoji i asinkroni način korištenja SNMP protokola. Tim načinom SNMP agenti, prema unaprijed definiranim kriterijima, izvještavaju SNMP menadžera o interesantnim događajima. Ukoliko se dogodi razlika između planiranog i realnog stanja to znači da postoji nepravilnost i da postoji sigurnosno oslabljeno mjesto.

Najnovije verzije upravljačkih sustava imaju mogućnost upravljanja pojedinim entitetima (server, operatorska kontrola, disk itd.) sustava. To znači da se takvo upravljanje koristi kao prethodno definirani odgovor na određeni događaj ili kao pomoć administratoru u izvršavanju propisanih procedura. Primjer takvog upravljanja je održavanje automatiziranih radarskih postaja, tj. upravljački sustav pokreće paljenje radarskog sustava, izvršava instalaciju/reinstalaciju sistemskog i/ili aplikativnog programa te postupak gašenja radara.

6. ZAKLJUČAK / *Conclusion*

S ciljem povećanja sigurnosti pomorskog prometa, kao i zaštite mora i morskog okoliša izvršena je integracija pomorskih sustava u jedan jedinstveni sustav za nadzor i upravljanje pomorskim prometom.

Povezivanje s brodovima i ostalim domaćim i međunarodnim pomorskim subjektima, izloženost globalnoj mreži i primjena standardnih informacijsko-komunikacijskih tehnologija rezultira činjenicom da i pomorski sustavi postaju ranjivi na prijetnje kao i ostali informacijski sustavi u ostalim područjima gospodarstva. Kako bi se ostvario najveći stupanj sigurnosti računalne opreme podsustava VTMIS sustava, potrebno je sustavno analizirati i implementirati mehanizme za nadzor i upravljanje koji su u skladu sa standardom ISO 27001:2005. U radu su opisane glavne komponente sustava za nadzor i upravljanje sigurnošću informacijskih resursa u podsustavima VTMIS sustava.

Za učinkovitu zaštitu svih podsustava VTMIS-a potrebno je razviti niz mjera i pravilno ih implementirati. Pritom treba voditi računa da ne postoji savršeno rješenje pošto dovoljno veliki napad, kao što je SYN-DDoS, može zaustaviti rad i najbržih poslužitelja.

Posebni naglasak je dan na RBCA modelu za kontrolu pristupa, upravljanje programskom podrškom, registracija događaja te nadzor stanja podsustava VTMIS-a. Također, neophodno je potrebno da domaće i međunarodne pomorske subjekte posvete posebnu pažnju u kreiranju i primjeni rezolucija, konvencija i preporuka za sigurnost podataka i informacija u pomorskim informacijskim sustava.

Zaposlenici u upravljačkim centrima, pomorci na brodovima i ostali korisnici usluga VTMIS sustava moraju povećati svjesnost o računalnoj sigurnosti.

LITERATURA / *Reference*

[1] Ristov, P. Nenadić, A., Mrvica, A.„Sigurnost računalnih sustava na brodu", IMSC 2014, Split, 2014.

[2] Malware protection K-IMS, http://www.km.kongsberg.com/ks/web /nokbg0240.nsf/ AllWeb/7C335BD142FAD546C12579EA0043E14A?OpenDocument

[3] ISO/IEC27001:2701:2005, "Information technology – Security techniques – Information security management systems – Requirements", Switzerland, 2005.

[4] Miroslav B., „Uvod u računalnu sigurnost", Narodne Novine d.d., Zagreb, svibanj 2004.

[5] CARNET, „Modeli kontrole pristupa", CCERT–PUBDOC–2008–02–218

[6] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts (9.09.2015).

[7] Statistics on botnet-assisted DDoS attacks in Q1 2015, Kaspersky Lab, May 29, 2015.

[8] Ministarstvo pomorstva, prometa i infrastrukture - Uprava sigurnosti plovidbe, Hrvatska, http://obris.org/hrvatska/meki-napadi-na-ais-moguci-i-na-jadranu/ (01.06.2015.)

[9] Hadjina, N. ,„Zaštita i sigurnost informacijskih sustava (nastavni materijali sa zbirkom zadataka)" FER, Zagreb.

[10] Essential SNMP, 2nd Edition, O'Reilly, 2005.

[11] FCAPS whitepaper, http://www.futsoft.com/pdf/fcapswp.pdf (10.09.2015.)

[12] NCERT-PUBDOC-2010-09-313: SNMP protocol, Zagreb, 2010.

[13] Balduzzi, M., Pasta, A., Wilhoit, K., "A Security Evaluation of AIS Automated Identification System", http://www.iseclab.org/people/embyte/papers/ais_acsac14.pdf (11.09.2015.)

[14] Hirner, T., Farkaš, P., Krile, S., "One Unequal Error Control Method For Telemetric Data Transmission", Journal of Electrical Engineering (JEE), Bratislava, Slovakia, 2011, Vol. 62, No 3, pp. 166-170.

[15] Lušić, Z., Kos, S., Krile, S., "Structural Analysis of Positioning Methods at Sea" (Strukturna analiza metoda pozicioniranja na moru), Naše more, Dubrovnik, 2008., Vol. 55, No 1-2, pp. 3-17