Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2024

Valtteri Louhivuori

Laivojen tekniset kyberturvallisuusratkaisut

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2024 | 31 sivua

Valtteri Louhivuori

Laivojen tekniset kyberturvallisuusratkaisut

Opinnäytetyö käsitteli laivojen teknisen kyberturvallisuuden teknisiä ratkaisuja. Aluksilla käytettävät järjestelmät ovat monimutkaisia ja ne liittyvät useisiin laivojen kriittisiin järjestelmiin, jotka huolehtivat laivan turvallisuudesta.

Työn tarkoituksena oli tutkia laivojen kyberturvallisuutta, sen nykytilaa ja haasteita. Tavoitteena oli tarjota käytännön näkökulma laivojen tietoturvan hallintaan ja selvittää miten parhaiten varmistetaan laivojen turvallinen ja luotettava toiminta digitalisoituvassa ympäristössä.

Opinnäytetyössä tarkasteltiin laivojen ja varustamoiden tietoturvaan liittyviä haasteita ja riskejä, joita moderni teknologia ja digitalisaatio ovat tuoneet mukanaan merenkulkuun. Työssä keskityttiin erityisesti laivojen järjestelmien haavoittuvuuksiin, mahdollisiin hyökkäysvektoreihin ja niiden torjuntaan tarvittaviin ratkaisuihin ja esiteltiin toimintamalleja joihinkin tilanteisiin. Työssä analysoitiin nykyisiä käytäntöjä ja arvioitiin niiden tehokkuutta.

Tämän opinnäytetyön avulla voidaan laivan kyberturvallisuuden tilaa tarkastella järjestelmällisesti ja aloittaa kyberturvallisuuden parantamiseen johtavat toimet huomioiden merenkulun erityispiirteet.

Asiasanat:

Kyberturvallisuus, laiva, valvonta, merenkulku, järjestelmät, standardit

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024 | 31 pages

Valtteri Louhivuori

Ships technical cybersecurity solutions.

The thesis focused on technical solutions for the cybersecurity of ships. The systems used on board are complex and are related to several critical ship systems responsible for the safety of the vessel.

The purpose of the study was to investigate the cybersecurity of ships, its current state, and challenges. The goal was to prove a practical perspective on managing ship cybersecurity and to determine the best way to ensure the safe and reliable operation of ships in a digitalized environment.

The thesis examined the challenges and risks related to ship and shipping companies’ cybersecurity brought about by modern technology and digitalization. It specifically focused on the vulnerabilities of ship systems, potential attack vectors, and the solutions needed to counter the, presenting operational models for specific situations. The thesis analyzed current practices and evaluated their effectiveness.

Through this thesis, the state of a ship’s cybersecurity can be systematically examined, and actions leading to the improvement of cybersecurity can be initiated, taking into account the peculiarities of maritime operations.

Keywords:

Cybersecurity, ship, surveillance, maritime industry, systems, standards

Sisältö

Kuvat

Taulukot

Käytetyt lyhenteet

AIS	Automatic Identification System. Merellä käytettävä navigointijärjestelmä. (All About AIS 2012.)
DMZ	Demilitarized Zone. Tietoturvan verkkoalue. (Enoch, S ym. 2021.)
DSC	Digital Selective Calling. Laivoilla käytettävä digitaalinen selektiivikutsu. (Highland wireless 2023.)
ECDIS	Electronic Chart Display System. Laivoilla käytettävä karttajärjestelmä. (Caprolu ym. 2020.)
EDR	Endpoint Detection and Response. Kyberturvallisuuden valvontajärjestelmä. (Wurzenberger, M. ym. 2024.)
GMDSS	Global Maritime Distress and Safety System. Maailmanlaajuinen meriliikenteen varoitus- ja turvallisuusjärjestelmä. (INCAS 2016.)
GT	Gross Tonnage. Bruttovetoisuus (Svanberg ym. 2019.)
GUI	Graphical User Interface. Graafinen käyttöliittymä (Zamfir, V-A. ym. 2019.)
HF	High frequency. Suurtaajuus (INCAS 2016.)
IDS	Intrusion Detection System. Tietoturvallisuuden valvontajärjestelmä. (Clemente, N. 2008.)
IOT	Internet Of Things. Esineiden internet. (Caprolu ym. 2020.)
IPS	Intrusion Prevention System. Järjestelmä joka estää tunkeutumisen käytettäviin järjestelmiin. (Clemente, N. 2008.)
IT	Information Technology. Tietotekniikka (Nganga, A. ym. 2023.)
JSON	JavaScript Object Notation. JavaScript-objektin merkintä (Zamfir, V-A ym. 2019.)

MITM	Man In The Middle. Hakkerointi metodi. (Mraković, I. ym. 2019.)
OT	Operational Technology. Operatiiivnen teknologia (Nganga, A. ym. 2023.)
SART	Search and Rescue Transponders. Merenkulun turvallisuudessa käytettävä etsintä- ja pelastusjärjestelmä. (INCAS 2016.)
S-AIS	Satellite AIS. Merenkulun navigointijärjestelmä joka hyödyntää satelliitteja. (INCAS 2016.)
SEM	Security Event Management. Tapahtumien hallinta. (Zamfir, V-A. ym. 2019.)
SIEM	Security Information and Event Management. Suojaustiedot ja tapahtumien hallinta (Zamfir, V-A. ym. 2019.)
SIM	Security Info Management. Turvallisuus tiedon hallinta. (Zamfir, V-A. ym. 2019.)
SOC	Security Operations Center. Tietoturvavalvomo (Nganga, A. ym. 2023.)
SSL	Secure Socket Layer. Suojausprotokolla (Mraković, I. ym. 2019.)
TLS	Transport Layer Security. Salausprotokolla (Mraković, I. ym. 2019.)
VDES	VHF Data Exchange System. VHF-tiedonsiirtojärjestelmä (INCAS 2016.)
VHF	Very High Frequency. Korkea taajuus.(INCAS 2016.)
VSAT	Very-Small-Aperture Terminal. Satelliitti järjestelmä. (INCAS 2016.)
VTS	Vessel Traffic Service. Alusliikennepalvelu. (All About AIS 2012.)

XDR	Extended Detection and Response. Kyberturvallisuuden valvontajärjestelmä. (Wurzenberger, M. ym. 2024.)

1 Johdanto

Meriliikenne on ollut aina yksi kaupankäynnin tärkeimmistä kuljetusmuodoista. Maailmanlaajuisesti 90 prosenttia kaupasta käydään meriteitse. Kaupankäynnin alusta saakka merirosvous, kilpailu ja valtiolliset intressit ovat vaikuttaneet laivojen turvallisuuden kehitykseen. (Boström 2020.)

Laivojen kyberturvallisuus on herättänyt kasvavaa huomiota, kun tietotekniset uhat ovat monimutkaistuneet ja niiden vaikutukset laajentuneet. Yhä useammat laivat on varustettu älykkäillä järjestelmillä jotka liittyvät navigointiin, viestintään, konehuoneeseen ja muihin kriittisiin toimintoihin. Tämä tekee laivoista alttiimpia kyberhyökkäyksille jotka voivat vaarantaa sekä miehistön että ympäristön turvallisuuden. (Boström 2020.)

Tässä opinnäytetyössä käsitellään laivojen teknisen kyberturvallisuuden valvontaa ja tarkastellen sekä teknologisia että organisaatioon liittyviä näkökohtia. Opinnäytetyön tavoitteena on selvittää kyberturvallisuuden käytäntöjä laivoilla sekä varustamoilla, tunnistaa mahdollisia haavoittuvuuksia ja ehdottaa ratkaisuja kyberturvallisuuden varmistamiseksi meriliikenteessä.

Alusten digitalisoituminen ja autonomisten järjestelmien käyttöönotto lisäävät entisestään kyberuhkien monimuotoisuutta. Opinnäytetyössä tarkastellaan myös tulevaisuuden trendejä ja teknologisia kehityskulkuja, jotka voivat muokata laivojen kyberturvallisuuden valvontaa. Tavoitteena on selvittää, miten alan toimijat voivat varautua tietoturvallisuuden haasteisiin ja kehittää kyberturvallisuusratkaisuja.

Turvallisen merenkulun takaaminen vaatii laajaa yhteistyötä teollisuuden, viranomaisten ja turvallisuusratkaisujen kehittäjien välillä, jotta voidaan kehittää käytäntöjä ja innovatiivisia ratkaisuja laivojen kyberuhkiin vastaamiseksi.

2 Meriliikenteessä käytettävät järjestelmät

Laivojen digitalisoituessa jopa perinteisistä kalastus- tai purjeveneistä löytyy ECDIS- (Electronic Chart DISplay) ja GPS-järjestelmät, jotka ovat alttiita mahdollisille hyökkäyksille. Digitalisoituminen mahdollistaa alusten ja rannikon toimipisteiden infrastruktuurin toiminnan, joka takaa samalla alusten turvallisuuden. Digitalisoituminen tuo mukanaan kuitenkin lukuisia kyberhyökkäysvektoreita ja -skenaarioita. Digitalisoitumisen kasvaessa meriliikenteessä myös uhat tulevat kasvamaan. (Aslam ym. 2020.) Esimerkiksi jäänmurtajien avustaessa muita aluksia jäisten väylien läpi alusten välinen kommunikointi on tärkeää. Alusten täytyy pitää erittäin lyhyt etäisyys toisiinsa, kuitenkin niin että operaation aikana alukset eivät törmää. Esimerkiksi tällaisessa tilanteessa väliintulohyökkäys tai mahdollinen kommunikoinnin häirintä voi aiheuttaa mittavia vahinkoja niin aluksille, kuin niiden miehistölle. (Boström 2020.)

Meriliikenteen data kattaa monia lähteitä, esimerkiksi laivan ohjaamon dataverkot, automatisoidut tunnistusjärjestelmät kuten AIS (Automatic identification system) ja alusliikennepalvelut VTS (Vessel Traffic Service). Ohjaamossa käsitellään laivan toiminnan tietoja ja kommunikoidaan ulkopuolisten tahojen kanssa. Aluksella ohjaamon ulkopuolella käytettäviä IOT (Internet Of Things) järjestelmiä ovat esimerkiksi sensorit kuten valvontakamerat ja säätutkat, rahdin valvontajärjestelmät ja miehistön henkilökohtaiset elektroniset järjestelmät. (Aslam ym. 2020.) Edellä mainitut järjestelmät ovat alttiita kyberhyökkäyksille ja kybertietoisuus on yleisesti hyvin matala miehistöllä merenkulun järjestelmissä. Kyberturvallisuuden tutkinta on keskittynyt enimmäkseen etsimään järjestelmien heikkouksia, mutta turvallisuusratkaisut ja henkilöstön koulutus on usein sivuutettu. Laivasta ranta-asemiin ja ranta-asemista laivoille liikkuvan datan autenttisuuden varmistaminen on vaikeaa varsinkin aluksilla. (Frøystad ym. 2017.)

Merenkulussa tapahtuvat hyökkäykset aluksiin ja varustamoihin ovat kohdistamattomia tai kohdistettuja. Kohdistamattomat hyökkäykset käyttävät

tekniikoita ja järjestelmiä, jotka eivät välttämättä ole niin hienostuneita. Kohdistamattomia hyökkäyksiä toteuttavat yleisesti opportunistiset hakkerit, jotka pyrkivät saamaan rahallista hyötyä. Kohdistetut hyökkäykset ovat hienostuneempia ja saattavat käyttää järjestelmiä ja tekniikoita, jotka on luotu juuri kyseisiä aluksia tai varustamoja varten. Kohdistetut hyökkäykset ovat usein esimerkiksi valtiollisen tekijän tai mahdollisten rikollisryhmien tekemiä. Eräs esimerkki kohdistetusta kyberhyökkäyksestä oli hyökkäys Ukrainan voimalaitoksiin. (America's Cyber Defence Agency 2021.)

Meriliikenteen kommunikointijärjestelmät ovat muuttumassa merkittävästi lähitulevaisuudessa. Siirtyminen analogisista järjestelmistä kuten VHF-radiosta (Very High Frequency) VDES-järjestelmään (VHF Data Exchange System) ja satelliittijärjestelmiin tarkoittaa sitä, että uusia ominaisuuksia voidaan hyödyntää merenkulussa. (Frøystad ym. 2017.)

Radioiden käyttötarkoitukset ovat monipuolisia ja ne vaihtelevat laivan toiminta-alueen mukaan. VHF-radiota käytetään lyhyen kantaman kommunikointiin esimerkiksi luotsaustilanteissa muiden alusten kanssa. VHF:ään integroitu DSC (Digital Selective Calling) mahdollistaa ennalta sovittujen protokollalähetysten suoran lähetyksen ja vastaanoton ja on laajalti käytetty hätätilanteissa. (Actisense 1-5) MF (Medium Frequency) sekä HF (High Frequency) radioita käytetään pitkän kantaman kommunikointiin ja ne toimivat yleisesti esimerkiksi merenkulun varoitusten jaossa. MF, sekä HF radiotaajuuksien kuuluvuus ylittää nähtävän horisontin. Radioiden käyttö tulee jatkumaan merenkulussa niiden käyttövarmuuden takia. (Highland wireless 2023.)

AIS on pakollinen järjestelmä aluksilla joiden bruttovetoisuus on yli 300 GT (Gross Tonnage). AIS-järjestelmä suunniteltiin aluksi tutkan tueksi ja VTS:n (Vessel Traffic Services) avuksi, mutta nykyään sitä hyödynnetään laajemmin esimerkiksi alusten reittijaossa ja päästöjen seuraamisessa. (Svanberg ym. 2019.) AIS toimii pääsääntöisesti autonomisesti ja jatkuvasti aluksen sijainnista riippumatta. AIS käyttää kahta eri radiotaajuutta, jotka ovat 87B – 161.975 MHz ja 88B – 162.025 MHz. AIS lähettää ja vastaanottaa tietoa molemmilla taajuuksilla samaan aikaan välttääkseen mahdollisen häiriön. (All About AIS

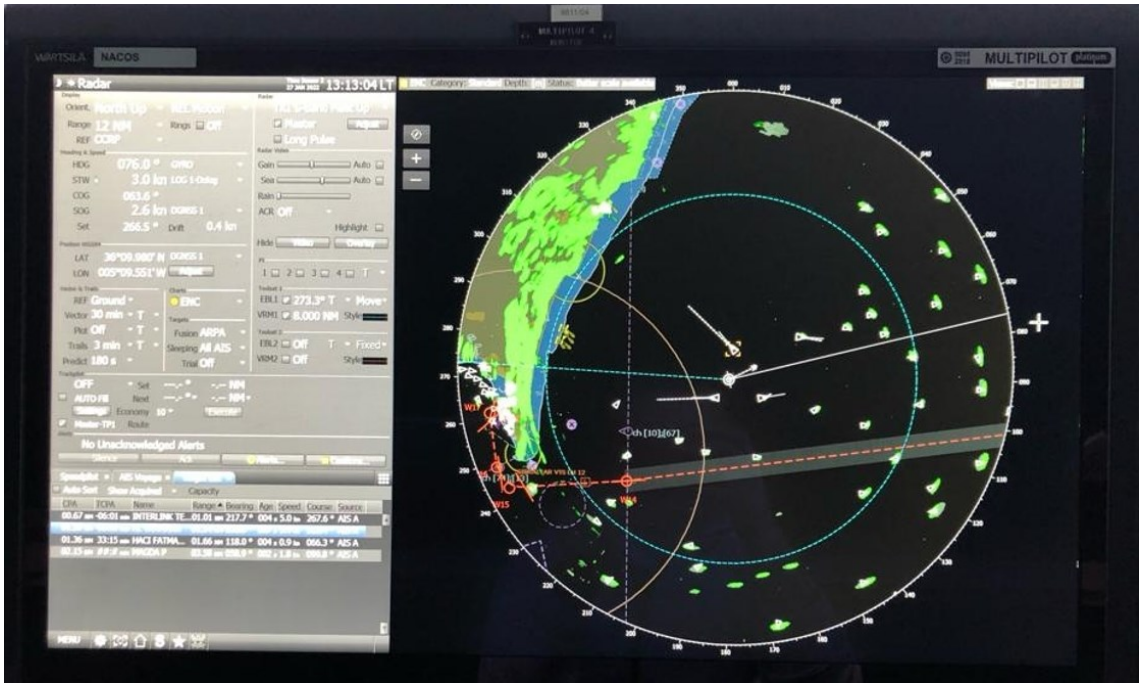
2012.) AIS lähettää 9 numeroista MMSI (Maritime Mobile Service Identity) numeroa, joka kertoo aluksen tunnisteen. AIS myös jakaa aluksen liiketekijät, lastin sekä kuljetun ja suunnitellun reitin. AIS toimii yhtenä merenkulun tärkeimpänä turvallisuusjärjestelmänä. (All About AIS 2012.)

Satelliittien käyttö on yleistynyt merkittävästi merenkulun toiminnassa sen kustannustehokkuuden ja helpon käytettävyyden johdosta. Satelliitteja käytetään merenkulun turvallisuuden, laittoman kalastuksen tai muun laittoman toiminnan valvontaan, pelastustoimiin ja sotilaalliseen käyttöön. Merenkulun turvallisuudessa satelliitti toimii GMDSS (Global Maritime Distress and Safety System), SART (Search and Rescue Transponders), S-AIS (Satellite AIS) ja muiden turvallisuusjärjestelmien kommunikointialustana. VSAT (Very-Small-Aperture Terminal) on lähetinvastaanotin, joka toimii alustana merenkulun internet-, data- ja puhelinverkkojen käytössä. Satelliitin tuottamaa kuvaa voidaan seurata reaaliaikaisesti, mikä mahdollistaa merialueiden valvonnan mahdollisten laittomien kalastajien tai esimerkiksi merirosvojen varalta. Satelliitin käyttö tulee kasvamaan huomattavasti merenkulun alalla. (INCAS 2016.)

Tutkaa käytetään merenkulussa laivan navigointiin, lähialueen tunnistamiseen ja pelastustoimiin. Tutkan vahvuutena on sen mahdollisuus seurata ja tunnistaa lähialue huonolla näkyvyydellä. Merenkulussa tutka toimii joko X- tai S-taajuudella. X-tutkan taajuus on 8 - 12 GHz ja S-tutkan taajuus on 2 - 4 GHz. X-tutkaa käytetään pääsääntöisesti navigointiin ja lähialueen seurantaan, mutta sen toimivuus on heikompi vaikeissa sääolosuhteissa kuten rankkasateella. S-tutkaa käytetään pidemmän kantaman seurantaan ja se toimii paremmin vaikeissa sääolosuhteissa. Kuten AIS, myös tutka on pakollinen järjestelmä kaikilla aluksille joiden bruttovetoisuus on yli 300. Järjestelmien kehittyessä, myös tutkan ohjelmisto on digitalisoitunut ja täten altis kyberhyökkäyksille. (Ward ym. 1990.)

ECDIS toimii aluksen elektronisena karttajärjestelmänä ja ohjaamossa käytettävien järjestelmien kuten tutkan ja AIS:in integraatiopisteenä. Käytännössä ECDIS visualisoi muiden ohjaamossa käytettävien järjestelmien

tuoman datan. Kuvassa 1 nähdään ECDIS-järjestelmän karttapohjassa vastaanottamaa dataa merenkulun tutkalta sekä AIS:ilta. Vihreät alueet kuvan sivuilla ovat tutkan luomia maaleja ja lähellä olevat kolmiot viivoilla ovat AIS-maaleja. Kuvassa 1 näkyy kuva karttapohjasta jossa tutka- ja AIS-tieto on integroitu.



Kuva 1. ECDIS, karttapohjajärjestelmän integroitu kuva. (Louhivuori 2023.)

Merenkulun ja navigoinnin järjestelmien ulkopuolella laivoissa on lukuisia tietokonejärjestelmiä, jotka automatisoivat ja helpottavat aluksen toimintoja. Näitä järjestelmiä ovat esimerkiksi lastin hallintajärjestelmät, kulunvalvontajärjestelmät, koneiston hallintajärjestelmät ja miehistön henkilökohtaiset elektroniikkajärjestelmät. Lastin hallintajärjestelmät vastaavat lastin lastaus- ja purkutoimista, kulunvalvontajärjestelmät laivan miehistön turvallisuudesta ja koneiston hallintajärjestelmät mekaanisten järjestelmien valvonnasta ja ohjauksesta. (Caprolu ym. 2020.) Kuvassa 2 näkyy miten aluksen verkot voidaan segmentoida. Kahdessa ylimmässä laatikossa kuvataan varustamoiden infrastruktuuria ja niiden alapuolella laivojen infrastruktuuria.

Kuva 2. Aluksen järjestelmien segmentointi esimerkki.

3 Laivojen kyberturvallisuuden ennakointi

3.1 Valmistautuminen, kyberkypsyys ja turvallisuuden tehostaminen

Yrityksen tietoturvatoiminnan perustana on ensisijaisesti ymmärrys sen toimintaympäristöstä ja digitaalisista järjestelmistä. Ilman tietoturvallisuuden perusteita ja oman kyberkypsyyden kartoitusta varustamot ja niiden laivat ovat haavoittuvaisia alkeellisillekin hyökkäyksille. Kyberkypsyydellä mitataan yrityksen valmiutta toimia tieto- ja kyberturvallisuusloukkauksissa. Kyberkypsyys mitataan käyttämällä eri uhkamallinnusrunkoja. (U.S. Department of Commerce. n.d.)

Uhkamallinnus toimii esimerkiksi seuraavan listan mukaan.

1. Uhkien tunnistus
2. Järjestelmien kovennus
3. Valvonta
4. Tilannereagointi
5. Analysointi

Toimivan yrityksen pitää tunnistaa heihin kohdistuvat uhkatekijät. Kartoittamalla hyökkääjät, uhat ja heikkoudet voidaan luoda ratkaisuja ja vastatoimenpiteitä. Aluksen ominaisuuksista ja varustamosta riippuen hyökkääjän motiivi ja osaaminen murtautua alusten järjestelmiin voi olla vaihteleva. Pienemmät varustamot voivat kokea korkeampaa uhkaa esimerkiksi opportunistisilta tai rahallista voittoa hakevilta hyökkääjiltä, joilla ei ole resursseja hienostuneempiin hyökkäyksiin. Isommilla varustamoilla hyökkääjän motiivi voi olla esimerkiksi poliittinen tai yritysvakoilu. Alusten yleisimpiä tieto- ja kyberturvallisuuteen vaikuttavia tekijöitä, motiiveja ja tavoitteita voivat olla taulukossa yksi luetellut profiilit. Taulukkoon 1 on listattu mahdollisia kyberhyökkäysten tekijöitä, heidän motiiveja ja tavoitteita.

Tekijät	Motiivit	Tavoite
Rikolliset	Rahallinen hyöty, vakoilu	Varastetun tiedon myynti tai kiristys. Heikkouksien myynti.
Opportunistit	Rahallinen hyöty, haaste, maine	Rahallinen hyöty, järjestelmien murtaminen
Valtiolliset tekijät	Poliittinen tai ideologinen hyöty, vakoilu	Tiedon saanti, valtiollisen tason infrastruktuurin heikennys.
Aktivistit	Huomio, maine, ideologinen hyöty	Tiedon tuhoaminen, jako tai siihen pääsyn esto, maine, huomio
Terroristit	Ideologinen hyöty, rahallinen hyöty, maine	Tiedon saanti, myynti, jakaminen, huomio
Vahingolliset tekijät	Eivät välttämättä aiheuta ongelmia tahallisesti, mutta toimivat hyökkääjinä esimerkiksi laittamalla vahingossa haittaohjelmallisen USB-tikun aluksen järjestelmään	

Taulukko 1 Kyberturvallisuuden tekijät, motiivit ja tavoitteet.
(Huoltovarmuuskeskus 2021a)

Tunnistamalla yleisimpiä hyökkäysmetodeja voidaan kouluttaa miehistöä ja parantaa alusten valmiutta vastata kyberuhkiin. Merenkulun organisaatiot ja niiden alukset ovat useinmiten alttiita seuraaville hyökkäyksille.

- Phishing

  Phishing eli kalastelu on yleisin hyökkäysvektori kyberturvallisuudessa. Kalastelua voidaan tehdä joko sosiaalisessa muodossa tai haittaohjelmien kautta. Sosiaalinen kalastelu pyrkii aiheuttamaan vahinkoa esiintymällä esimerkiksi organisaatioon kuuluvana henkilönä ja

näin pyrkiä saamaan pääsyn eri järjestelmiin. Haittaohjelmakalastelu taas pyrkii saamaan uhrin lataamaan haitallisia ohjelmia järjestelmäänsä. Aluksilla kalasteluhyökkäykset tehdään usein sähköpostin avulla. Sähköposti voi sisältää hyperlinkin tai mahdollisen tiedoston jonka uhri lataa tai siirtää käytettävään järjestelmään.

- Spear Phishing

  Spear Phishing eli kohdistettu kalastelu on hienostuneempi hyökkäysmetodi, jossa esimerkiksi hakkeri ottaa yhteyden aluksella toimivaan henkilöön ja esittelee itsensä “työkaverina”. Väärennetyillä sähköposteilla tai hyvin samankaltaisia tunnuksia käyttäen, voidaan pyrkiä huijaamaan yksittäistä henkilöä ja saamaan hänet lataamaan haittaohjelmia aluksen järjestelmiin.

- Henkilöllisyyden varastaminen ja huijaaminen.

  Kyberhyökkäykset voivat olla suunnattuja yksinomaan henkilöllisyyden varastamiseen ja sen käyttämiseksi edelleen rikollisiin tarkoituksiin. Henkilöllisyyden väärinkäyttöä tehdään yleisesti käyttäen eri haittaohjelmia.

- Kiristysohjelmat

  Kiristysohjelmat ovat haittaohjelmatyyppi, jotka pyrkivät rajoittamaan pääsyä järjestelmään, ellei uhri toimi kuten kiristäjä haluaa. Kiristysohjelmat voivat lukita järjestelmän esimerkiksi salasanan taakse ja vaatia lähettämään tietoa tai rahaa, luovuttaakseen salasanan ja pääsyn järjestelmään.

- MITM (Man In The Middle)

  Väliintulohyökkäys on tekniikka jossa hakkeri sieppaa järjestelmien välisen kommunikaation ja manipuloi sitä saavuttaakseen tavoitteensa.

- Tietovarkaudet

  Tietovarkaudet pyrkivät varastamaan aluksilla olevaa tietoa käyttäen aikaisempia metodeja. (Mraković, I. ym. 2019.)

Seuraavat alusten järjestelmät ja tekijät ovat alttiita kyberhyökkäyksille ja niiden heikkouksia voidaan hyödyntää ja käyttää hyväksi.

- GPS

  GPS-paikkatietoa voidaan häiritä tai sen vastaanotto voidaan estää. Hienostuneet hyökkäykset voivat myös luoda väärennettyä GPS-signaaleja antaen aluksille virheellistä tietoa.
- AIS

  AIS-järjestelmää, kuten GPS:ääkin voidaan häiritä tai sille voidaan lähettää väärennettyä tietoa. AIS:illa vastaanotettu virheellinen tieto voi aiheuttaa navigointi virheitä tai muita turvallisuusriskejä.
- ECDIS

  ECDIS-järjestelmät toimivat usein vanhoilla tietokoneilla ilman turvallisuusjärjestelyjä ja kartat ladataan suoraan internetistä tai muistitikulta, joka mahdollistaa haittaohjelmien sisäänpääsyn. Haittaohjelmat voivat esimerkiksi muokata karttatietoa ja täten aiheuttaa turvallisuusriskejä.
- IOT-järjestelmät (Internet Of Things)

  Alusten IOT-järjestelmät kuten valvontakamerat toimivat hyökkäys vektoreina haittaohjelmille.
- Standardoimattomat satelliittiprotokollat

  Satelliittiprotokollat toimivat hyökkäysvektorina MITM, palvelunesto tai haavoittuvien protokollien hyökkäyksissä.
- Elektroninen vaikuttaminen

  Elektronisessa vaikuttamisessa pyritään estämään alusten kokonaisvaltaista kommunikointia muiden alusten ja ranta-asemien kanssa.

- Inhimillinen tekijä

  Inhimillinen tekijä voi toimia tieto- ja kyberturvallisuudessa vaikuttavana tekijänä tai mahdollisesti katalyyttinä lopputulokselle. (Caprolu ym. 2020.)

3.2 Kyberturvallisuuden parantaminen yrityksissä

Yritysten tutkiessa järjestelmiensä heikkouksia, ensimmäinen askel on niiden tunnistaminen ja korjaaminen. Järjestelmien kovennuksessa pyritään käyttämään monikerroksista puolustustautumista, jossa käytännössä pyritään luomaan useampi kuin yksi turvallisuustoimenpide estämään hakkerien pääsyä järjestelmiin. Mikäli yksi mekanismeista pettää, muiden on tarkoitus jatkaa toimintaansa ja taata järjestelmän turvallisuus. Käyttöjärjestelmien kovennus on prosessi, jossa poistetaan haavoittuvuuksia esimerkiksi muokkaamalla järjestelmien oletussalasanoja, suorittamalla ohjelmistopäivityksiä sekä palomuurikonfiguraatioilla.

Kovennus aloitetaan luomalla turvallisuuskäytännöt. Toimivilla turvallisuuskäytännöillä voidaan aloittaa vastatoimet, sekä luoda puolustus järjestelmällisesti kyberhyökkäykseen. Luomalla pelikirjoja eli tarkistuslistoja tiettyihin hyökkäystyyppeihin saadaan runko, jolla voidaan tunnistaa hyökkäysvektori. Kun hyökkäysvektori on tunnistettu, voidaan kohteena olevat järjestelmät eristää ja suojata. Kovennusta voidaan jatkaa turvallisuustarkastuksella. Tarkastamalla järjestelmien suorituskykyjä ja haavoittuvuuksia, voidaan tunnistaa tekniset heikkoudet. Haavoittuvuuksia voidaan tarkistaa esimerkiksi eri haavoittuvuuskannereilla. (Clemente, N. 2008)

Aluksen järjestelmien heikkouksien tunnistaminen on edellytys koventamiselle ja kyberturvallisuuden parantamiselle. Seuraavalla toimilla voidaan koventaa alusten kyberturvallisuutta.

- Tunnistautuminen

  Käyttäjän todennus salasanalla on yksi perinteisimmistä tavoista suojella järjestelmiä. Moni käyttöönotettava järjestelmä saapuu oletussalasanoilla, jotka tulee vaihtaa. Tunnistautumisen tulisi olla salasanan lisäksi kaksivaiheista. Korkeavaiheisempi tunnistautuminen tarkoittaa pakollisia eri tunnistautumistapoja jotka pitää suorittaa, päästäkseen käyttämään järjestelmää. Tunnistautumismenetelmiä ovat salasanojen lisäksi esimerkiksi fyysinen ja biologinen tunnistautuminen. Fyysinen tunnistautuminen voi olla esimerkiksi henkilö- tai varmennekortti. Biologinen tunnistautuminen voi olla tunnistautuminen sormenjäljen tai iriksen avulla. (Kato, K ym. 2013.)

- Palomuurit

  Palomuurien tehtävä on tutkia jokainen saapuva ja lähtevä datapaketti ja joko hyväksyä tai hylätä se. Palomuurit toimivat tavallisesti aluksilla sovelluspalvelimien suojana langattoman verkon ja VSAT:in ympärillä. Aluksen sovelluspalvelimet eli DMZ:t (Demilitarized zone) on suojattu sekä front- että backend-palomuureilla. Frontend-palomuurilla valvotaan aluksen tiettyyn DMZ:een saapuvaa liikennettä ja backend-palomuurin tehtävänä on puolestaan käsitellä liikennettä, joka liikkuu DMZ:sta sisäverkkoon. (Enoch, S ym. 2021.)

- Ohjelmistopäivitykset

  Haavoittuvuusskannereilla löydetyt heikkoudet voidaan joskus korjata yksinkertaisesti hakemalla järjestelmän valmistajan uusin päivitys järjestelmään. (Clemente, N. 2008.)

- Antivirus

  Antivirusohjelmiston tehtävä on skannata järjestelmiä mahdollisten virusten löytämiseksi. Antivirus etsii järjestelmistä tiettyä osaa viruksen koodissa, jonka avulla se tunnistetaan haittaohjelmaksi. Antiviruksen

tehokkuus laskee, mikäli sitä ei pidetä ajan tasalla päivityksillä. (Clemente, N. 2008.)

- IDS/IPS

  IDS (Intrusion Detection System) on kyberturvallisuuden valvontajärjestelmä. IDS tarkkailee järjestelmän verkkoliikennettä ja pyrkii tunnistamaan haitalliset toiminnot. IPS (Intrusion Prevention System), joka on kehittyneempi versio IDS:stä, pyrkii sekä havaitsemaan että estämään haitallisen toiminnon esimerkiksi eristämällä hyökkäyksen kohteena olevan järjestelmän. IPS:n heikkouksia ovat kuitenkin muun muassa vaadittu kaistanleveys, väärät tunnistukset ja rajoitettu tietokanta. Vaadittavat resurssit IPS:n käyttöön voivat olla ongelma, järjestelmä voi luoda vääriä hälytyksiä ja jättää huomioimatta hienostuneempia hyökkäyksiä. (Clemente, N. 2008.)

- Segmentointi

  Järjestelmien jakaminen omiin lohkoihin tai aliverkkoihin mahdollistaa niiden eristämisen tarvittaessa. Tämä estää aluksiin kohdistuvien hyökkäysten leviämisen yksittäisistä järjestelmistä koko laivaan. (Clemente, N. 2008.)

- Salaus

  Järjestelmien ja niiden liikenteen salaus on vahva tapa suojautua välihyökkäyksiltä. Käytännössä järjestelmä vaatii tiettyä tunnistautumista vastaanottakseen sille lähetetyn datan. (Shmueli, E. ym 2010.)

- Varmuuskopiointi ja vaihtoehtoiset toimintatavat

  Tiedostojen, sekä ohjelmistoversioiden varmuuskopiointi mahdollistaa niiden palauttamisen aikaisempaan versioon, mikäli ne ovat haavoittuvaisia tai jo haittaohjelman vaikutuksen alla. Alusten on myös oltava valmiita toimimaan kyberhyökkäyksen alla ja ilman elektronisia

järjestelmiä esimerkiksi korvaten ECDIS-karttaohjelman perinteisellä paperikartalla. (Clemente, N. 2008.)

Organisaatioilla on käytössä usein rajallinen budjetti kyberturvallisuuteen, joten kaikkien toimintojen ja absoluuttisen turvallisuuden saavuttaminen ei ole aina mahdollista. Kyberturvallisuuden laiminlyönti voi kuitenkin aiheuttaa korkeampia kustannuksia vahinkojen kautta, kuin siihen investointi. (Huoltovarmuuskeskus 2021a)

3.3 Kyberturvallisuuden valvontajärjestelmät ja analysointi.

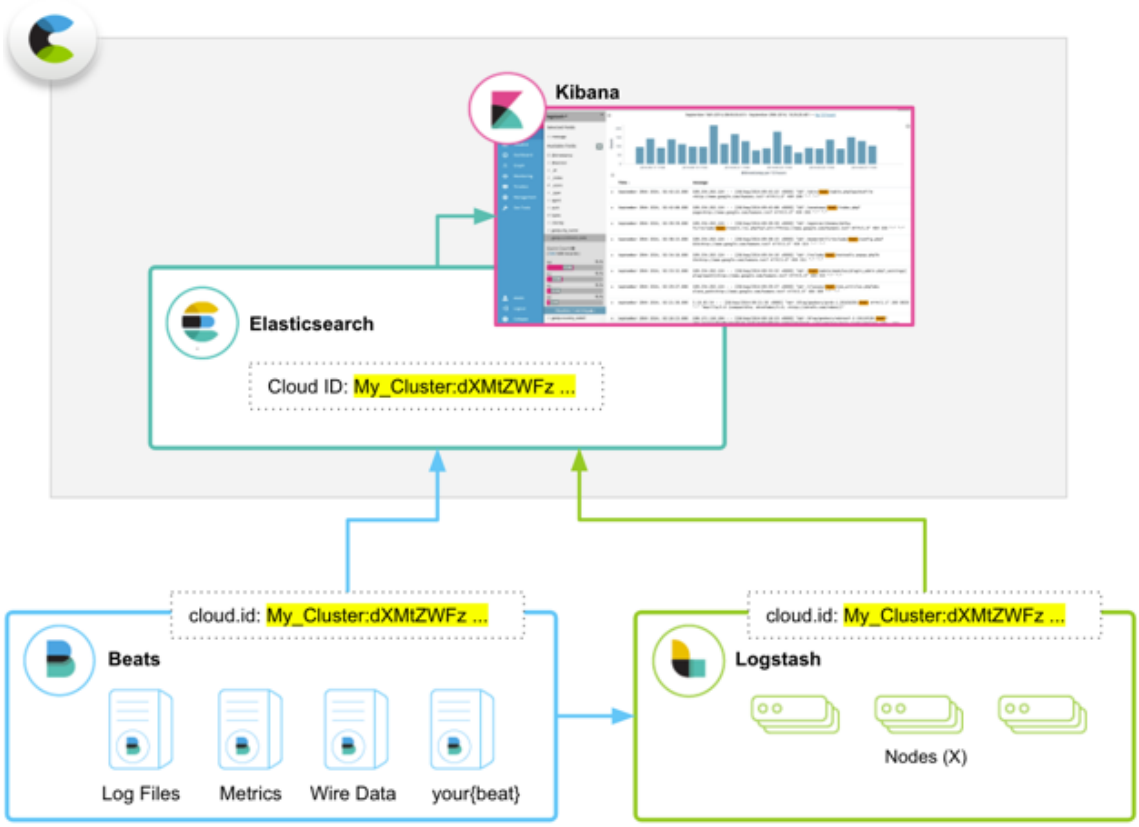
Yksittäisten lokitiedostojen, datan eheyden ja liikkuvuuden seuraaminen voidaan automatisoida ja prosessia voidaan nopeuttaa käyttämällä SIEM-järjestelmiä (Security Information and Event Management). SIEM-järjestelmät analysoivat dataa reaaliaikaisesti ja ilmoittavat poikkeamista määritettyjen vaatimusten mukaan. Käytettäviä SIEM-järjestelmiä ovat esimerkiksi Elasticsearch ja Splunk. SIEM-järjestelmät voidaan jakaa kahteen käyttötoimintoon. SIM (Security Info Management) kerää lokitiedot, raportoi ja analysoi datan aluksen järjestelmistä. SEM (Security Event Management) käsittelee SIM:in kautta vastaanotetut lokitiedot ja mahdollistaa tietoturvallisuuden seurannan. Jotta järjestelmien turvallisuutta voidaan valvoa, pitää tarvittava data siirtää aluksen järjestelmistä käytettävään SIEM:iin. Data siirretään valvottavaksi mobiiliverkon tai satelliitin välityksellä.

Valittaessa valvontajärjestelmä merenkulun kyberturvallisuuteen tulisi varmistaa, että seuraavia asioita kyetään valvomaan: (Montesino, R. ym. 2012.)

- verkko- ja puhelinliikenne
- palomuurien läpi kulkevat yhteydet
- kaikki käytössä olevat käyttöjärjestelmät
- tiedon eheys
- lokit
- prosessit
- haittaohjelmat käytettävissä järjestelmissä

Valittaessa aluksella käytettävää valvontajärjestelmää, Elasticsearch on avoimeen lähdekoodiin perustuva datan visualisointi- ja valvontajärjestelmä. Elasticsearch tallentaa datan JSON (JavaScript Object Notation) dokumenteiksi ja kykenee käsittelemään ja hallinnoimaan vastaanotetun datan tietoturvallisuuden valvojalle käytettäväksi. Elasticsearch kuuluu laajempaan kokonaisuuteen, joka pitää sisällään analytiikka- ja visualisointityökaluja, kuten Kibana ja Logstash. Kibana on Elasticsearchin GUI (Graphical User Interface)-työkalu, joka mahdollistaa itse käytettävän datan visualisoinnin. Logstash on datan prosessointityökalu, joka suodattaa vastaanotettua tietoa. (Zamfir, V-A. ym. 2019.)

Datan siirto visualisoitavaksi tapahtuu käytännössä siirtämällä lokitiedosto käyttäen eri beat-ohjelmia. Beat-ohjelmia ovat esimerkiksi Filebeat, jonka tarkoitus on lähettää tiedostoja Elasticsearchiin joko Logstashin kautta tai suoraan. Kuvassa 3 nähdään prosessi, miten käsiteltävä data saadaan visualisoitua Elasticsearchilla.



Kuva 3. Elasticsearch datan siirto visualisoitavaksi.(Elasticsearch n.d.)

Käytännössä vastaanotettuaan datan käyttäjä asettaa säännöt, joista järjestelmä luo pohjan Elasticsearchin valvonnalle. Seuraamalla järjestelmän luomia hälytyksiä voidaan suorittaa aluksen kyberturvallisuuden valvontaa Elasticsearchilla. (Zamfir, V-A. ym. 2019.)

4 Kyberturvallisuuden valvonta aluksilla ja maissa

4.1 Kyberturvallisuuden valvonta maissa

Kyberturvallisuuden valvonta maissa suoritetaan kyberturvallisuusvalvomoissa eli SOC:ssä (Security Operations Center). Varustamoiden SOC-toiminnan käyttöönotto on aloitettu, jotta saadaan täytettyä kyberturvallisuuden standardien vaatimat normit. Käytännössä SOC:in päätehtävä on valvoa laivan tieto- ja kyberturvallisuutta maista käsin niin IT (Information Technology) kuin OT-järjestelmissä (Operational Technology). Tavallisesti SOC:in toimintaa ei rajoita yhteydet valvottavaan kohteeseen, mutta merenkulkualalla vaihtelevasti toimivat yhteydet luovat rajoitteita alusten kyberturvallisuuden valvontaan. Alusten pitkä käyttöikä ja vanhat käyttöjärjestelmät pakottavat tieto- ja kyberturvallisuuden valvojat luomaan kompromisseja. SOC:ien pitää siis varautua esimerkiksi kaistanleveyden rajoituksiin ja toimimaan ympäristössä, joka on laajalti poikkeava normaalista SOC-toiminnasta. Varustamoiden kannattaa luoda käytännön menettelytavat työntekijöille niin aluksilla kuin rannassakin.

SOC:n reagointi ja toimintamahdollisuudet ovat rajalliset merenkulun toiminnassa, mutta jo tieto kyberhyökkäyksestä on erittäin tärkeä. SOC:n huomatessa aluksen olevassa kyberhyökkäyksen kohteena se voi käynnistää vastatoimet puolustautumiseen. Tiedonanto alukselle järjestelmien murrosta on erittäin tärkeää, sillä se mahdollistaa miehistön reagoinnin. SOC voi kyberhyökkäyksen aikana ohjeistaa aluksen miehistöä tarvittaviin toimenpiteisiin, sekä mahdollisesti esimerkiksi eristää saastuneet järjestelmät. Kyberhyökkäysten laajasta kirjosta johtuen, SOC:in pitää olla valmis toimimaan laajalti muuttuvassa ympäristössä reaaliaikaisesti. Monia hyökkäyksiä voidaan ehkäistä seuraamalla maailmanlaajuista kybersäätä sekä kyberturvallisuuden tilannetta ja pitämällä alusten järjestelmät suojattuna reaaliaikaisesti esimerkiksi etäpäivityksillä. (Nganga, A. ym. 2023.)

Kyberhyökkäyksen päätyttyä, SOC:in tehtävä on tutkia ja analysoida hyökkäys ja sen aiheuttamat ongelmat. Paikantamalla hyökkäysvektori, haavoittuvainen järjestelmä ja syy murrolle voidaan aloittaa korjaustoimenpiteet. Omien toimintatapojen sekä reagoinnin analysointi kyberhyökkäyksen aikana mahdollistaa SOC:ssä sekä aluksella toimivien henkilöiden valmiuden kehittymisen. Viimeiseksi yrityksen pitää tiedottaa sidosryhmiä mahdollisista vaikutuksista ja hyökkäyksen vakavuudesta. (Manco, D. 2022)

4.2 Kyberturvallisuuden valvonta aluksilla

Aluksella tärkeintä on valmistautuminen. Haasteita varautumiseen tuovat esimerkiksi aluksen fyysinen tila, sekä ylimääräisten valvontajärjestelmien tuomat tarpeet kuten virta. Aikaisemmin mainitut järjestelmien kovennukset sekä henkilöstön koulutus ovat suuressa roolissa. Poiketen normaalista SOC-toiminnasta, valvottavan aluksen heikko yhteys voi toimia myös valvojan eduksi. Alusta ei pystytä välttämättä valvomaan maalta koko ajan, mutta tämä korostaa aluksen miehistön kyberkypsyyttä sekä heidän kykyään valvoa omaa turvallisuuttaan. (Nganga, A. ym. 2023.) Alusten kyberturvallisuutta voidaan valvoa Elasticsearchin tapaisilla lokien hallintajärjestelmillä rannan lisäksi itse aluksella. Tärkeimmässä roolissa aluksella kyberturvallisuushyökkäyksen vaikutusten ehkäisemiseen on henkilöstön valmius toimia hyökkäyksen alaisena. Miehistön osaaminen tunnistaa, että laiva on kyberhyökkäyksen alla on erittäin tärkeää. Varustamoiden tulisi tarjota miehistölle koulutusta, jonka kannattaa räätälöidä erikseen aluksen henkilöstöryhmille. (Huoltovarmuuskeskus 2021b)

Automatisoidut valvontajärjestelmät, kuten EDR (Endpoint Detection and Response) ja XDR (Extended Detection and Response) voivat suojella aluksen järjestelmiä ilman miehistön panosta. EDR - ja XDR-järjestelmät seuraavat aluksen verkkojen liikennettä ja suorittavat tarvittavat toimenpiteet kyberhyökkäyksen estämiseksi. Henkilöstö voi kyberhyökkäyksen aikana myös pyrkiä eristämään hyökkäyksen kohteena olevia järjestelmiä. Kuvan 2 mukaisen segmentoinnin avulla voidaan varmistaa, että hyökkäys esimerkiksi ohjaamon

järjestelmien kautta ei leviä aluksen muihin järjestelmiin ja aiheuta enempää vahinkoa. Miehistö voi tarvittaessa itse eristää järjestelmiä enemmän ja täten jatkaa normaalia toimintaa. (Wurzenberger, M. ym. 2024.)

Ongelmana yrityksille kyberturvallisuuden valvonnassa on resurssit. Mahdollisuus siirtää ja tallentaa tieto aluksilta järjestelmille ja pitää se siellä on kallista. Myös henkilöstö ja sen koulutus sekä fyysinen laitteisto maksaa. Käytettävät ohjelmistot ovat usein ilmaisia mutta voivat tarvita erillisiä maksuja, jotta niistä saa täyden hyödyn irti. Yrityksen koon mukaan analysointia vaativaa dataa voi olla suuria määriä, joka vaikeuttaa sen käsittelyä. Yritys voi myös ulkoistaa kyberturvallisuuden valvonnan. (Serckumecka, A. ym. 2019)

5 Pohdinta

Laivojen kyberturvallisuus on nousemassa ongelmaksi nykyaikaisessa merenkulussa. Digitalisoituminen merenkulussa on avannut uusia mahdollisuuksia turvallisempaan toimintaan merellä, mutta samalla se on tuonut mukanaan haasteita kyberturvallisuuden näkökulmasta. Laivat ovat yhä enemmän riippuvaisia automaatiosta, tietojärjestelmistä ja internet-yhteyksistä, joka alistaa ne uusille uhille. Kyberturvallisuusuhat kehittyvät jatkuvasti ja ne voivat vaihdella haittaohjelmista ja tietomurroista fyysiseen manipulaatioon. Varustamoiden on tärkeää valmistautua ja tarkastella, miten suojata tietojärjestelmiään ja autonomisia järjestelmiään. Tieto- ja kyberturvallisuusongelmien tunnistaminen ja niiden korjaaminen on erittäin tärkeää. Tulevaisuudessa onkin tärkeää kehittää ennakoivia turvallisuusratkaisuja, jotka kykenevät vastaamaan nopeasti ja autonomisesti uhkiin.

Tässä opinnäytetyössä tavoitteena oli tarjota käytännön näkökulmia laivojen tietoturvan hallintaan ja selvittää miten laivalla voidaan toimia turvallisesti ja luotettavasti digitalisoituvassa ympäristössä. Keskeinen osa laivojen kyberturvallisuutta on alusten miehistön ja varustamoiden kybertietoisuuden lisääminen. Merenkulun ammattilaiset tarvitsevat kohdistettua koulutusta kyberuhkien tunnistamiseen, turvallisuuskäytäntöjen ymmärtämiseen ja kyberhyökkäystilanteissa reagointiin. Kybertietoisuuden kehittäminen voi vähentää inhimillisten virheiden aiheuttamia riskitekijöitä ja parantaa laivojen yleistä turvallisuutta.

Suositukset ja toimintaohjeet joita tässä opinnäytetyössä on annettu, perustuvat käytettyyn kirjallisuuteen. Jotta yksittäinen varustamo tai laivan miehistö saisi parhaan hyödyn ja ohjeet kyberturvallisuuden tehostamiseksi, tulisi tehdä varustamo- tai aluskohtainen selvitys nykytilanteesta kohdennettujen suositusten laatimiseksi.

Tulevaisuudessa olisi mielenkiintoista selvittää, millaisia valmiuksia henkilöstöllä tällä hetkellä on toimia kyberhyökkäyksen alla ja millaista koulutusta he ovat

saaneet. Onko henkilöstölle sopivin koulutus kohdistettua vai yleispätevää. Autonomisten alusten yleistyessä tarve kyberturvallisuuden henkilöstölle tulee nousemaan. Olisi myös mielenkiintoista selvittää suomalaisten ja muissa maissa toimivien varustamoiden eroja kyberturvallisuuskoulutuksissa. Voisiko tulevaisuudessa kyberturvallisuusosaaminen olla yksi merenkulun pätevyyksistä, jota ylläpidetään jatkuvalla kouluttautumisella.

Yhteenvetona voidaan todeta, että laivojen kyberturvallisuus on vielä kehittyvä ala joka vaatii aikaa. Tällä hetkellä on tärkeää keskittyä tunnistamaan ja korjaamaan nykyiset haasteet ja tutkia mitä uhkia tulevaisuudessa voi olla. Henkilöstön kybertietoisuuden nostaminen on olennainen osa tätä prosessia, jotta koko organisaatio voi vastata tehokkaasti mahdollisiin kyberuhkiin.

Lähteet

Actisense. Digital Selective Calling (DSC) – What you need to know. Viitattu 23.11.2023 https://actisense.com/news/digital-selective-calling-dsc-what-you-need-to-know/#:~:text=What%20is%20DSC%3F,other%20vessels%20and%20shore%20systems.

All About AIS 2012. Frequency. Viitattu 23.11.2023 http://www.allaboutais.com/index.php/en/technical-info/technical-fundamentals/109-ais-technicals/various-ais-technologies/158-frequency.

America's Cyber Security Agency 2022. Cyber-Attack Against Ukrainian Critical Infrastructure. Viitattu 22.11.2023 https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

Aslam, S. Michaelides, M. Herodotou, H. 2020. Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges.

Boström, M. 2020. Mind the Gap! A quantitative comparison between ship-to-ship communication and intended communication protocol. Safety Science.

Caprolu, M. Di Pietro, R. Raponi, S. Sciancalepore, S. Tedeschi, P. 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead

Clemente, N. 2007 System Hardening, Journal of Security Education, 2:4, 89-118. Viitattu 16.1.2024

Elasticsearch. Configure Beats and Logstash with Cloud ID. https://www.elastic.co/guide/en/cloud/current/ec-cloud-id.html Viitattu 4.2.2024

Enoch, S. Lee, J. Kim, D. 2021 Novel security models, metrics and security assessment for maritime vessel networks. Viitattu 17.1 2024.

Frøystad, C. Bernsmed, K. Meland P. 2017. Protecting Future Maritime Communication.

Highland wireless 2023. Marine Communication Systems Used in the Maritime Industry. Viitattu 23.11.2023 https://www.highlandwireless.com/marine-communication-systems-used-in-the-maritime-industry/.

Huoltovarmuuskeskus. 2021a. Maritime cybersecurity report – finnish maritime cybersecurity maturity. Viitattu 4.1.2024 https://www.huoltovarmuuskeskus.fi/files/d60cfd87d66aa5321cfc9e48dc76f8b5789603b3/maritime-cybersecurity-report.pdf

Huoltovarmuuskeskus. 2021b. Merenkulun kyberturvallisuus – alusten parhaat käytännöt Viitattu 28.1.2024 https://shipowners.fi/wp-content/uploads/2021/09/WWW_Parhaat_ka%CC%88yta%CC%88nno%CC%88t_aluksille_SU.pdf

INCAS 2016. The Use of Satellite Technologies for Maritime Surveillance: An Overview of EU Initiatives Viitattu 29.11.2023 https://bulletin.incas.ro/files/bosilca_r__vol_8_iss_1__f.pdf

Kato, K. Klyuev, V. 2013. Strong Passwords: Practical Issues

Louhivuori, L. 2023. ECDIS, karttapohjajärjestelmän integroitu kuva.

Manco, D. 2022. Automation in the Cybersecurity Incident Handling Proces

Montesino, R. Fenz, S. BalujaInformation, W. 2012. Management & Computer Security Emerald Article: SIEM-based framework for security controls automation

Mraković, I. Vujinoć, R. 2019. Maritime Cyber Security Analysis – How to Reduce Threats? Viitattu 17.1.2024

Nganga, A. Nganya, G. Lützhöft, M. Mallam, S. Scanlan, J. 2023. Bridging the Gap: Enhancing Maritime Vessel Cyber Resilience through Security Operation Centers

U.S. Department of Commerce. Cyber security basics, Understanding the NIST framework.Viitattu 4.1.2023

https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

Serckumecka, A. Medeiros, I. Bessani, A. 2019 Low-cost Serverless SIEM in the Cloud

Shmueli, E. Vaisenberg, R. Elovici, Y. Glezer, C. 2010. Database encryption: an overview of contemporary challenges and design considerations Viitattu 17.1.2024

Svanberg, M. Santén, V. Hörteborn, A. Holm, H. Finnsgård, C. 2019. AIS in maritime research.

Ward, K.D. Baker, C.J. Watts, S. 1990. Maritime surveillance radar Part 1 : Radar scattering from the ocean surface. Viitattu 3.1.2024

Wurzenberger, M. Höld, G. Landauer, M. Skopik, F. 2024. Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security

Zamfir, V-A. Carabas, M. Carabas, C. Tapus, N. 2019. Systems monitoring and big data analysis using the Elasticsearch system.