Laura Salminen

INHIMILLISTEN TEKIJÖIDEN VAIKUTUS MERENKULUN KYBERTURVALLISUUTEEN ALUKSEN KONEOSASTOLLA

Opinnäytetyö

Merenkulun insinööri

2022

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Merenkulun insinööri
Tekijä/Tekijät	Laura Salminen
Työn nimi	Inhimillisten tekijöiden vaikutus merenkulun kyberturvallisuuteen aluksen koneosastolla
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu: Human Factor in Ship ECR Safety Management -hanke
Vuosi	2022
Sivut	72+1
Työn ohjaaja(t)	Joel Paananen

TIIVISTELMÄ

Tässä opinnäytetyössä tutkittiin, miten kyberturvallisuus näkyy aluksen koneosastolla ja kuinka inhimilliset tekijät vaikuttavat konehenkilöstön kyberhygieniataitoihin. Tutkimus koostuu HF Tool -koulutuksesta sekä kahdeksasta eri haastattelusta. Työn tavoitteena oli nähdä, kuinka konepäällystön kyberturvallisuuden hahmottaminen toteutuu aluksen rutiineissa ja työnkuvassa. Haastatteluiden tavoitteena oli myös saada selville, miten kyberturvallisuuteen on ylipäätään panostettu.

Opinnäytetyön teoriaosuus koostuu sekä PDF-dokumenteista että painetusta tekstistä, ja osa materiaalista on uutisia ja Internet-dokumentteja. Teoriaosuudessa tulkitaan asiantuntijahaastattelua ja selvitetään kyberturvallisuuden vaiheita sekä reflektoidaan sitä inhimillisen tekijän rooliin aluksen koneosastolla. Kyberturvallisuusosio selventää, mitä riskejä liittyy Internetin käyttöön ja kuinka erilaisiin uhkiin tulisi varautua. Turvallisuusajattelun perustana voidaan pitää ideologiaa, joka pohjautuu henkilöstön kouluttamiseen. Inhimillisen tekijän vaikutusta koneosaston työnkuvaan esitellään erilaisten skenaarioiden kautta. Tämä havainnollistaa konevalvomon tai -huoneen toimintaa sekä tilannetietoutta, ja demonstroi kuinka konehenkilöstö toimii erilaisten tilanteiden aikana. Kyberturvallisuudelle on joitakin määräyksiä laivaympäristöön, mitkä muodostuvat Kansainvälisen merenkulkujärjestön määräyksistä ja luokituslaitosten ohjeista.

Tutkimuksen ajankohtaisuus nostetaan esille, jonka seurauksena voidaan esittää johtopäätöksiä tämän hetken kyberturvallisuustaidoista. Aluksen koneosaston näkökulmasta voidaan todeta, että suurimmat haasteet liittyvät haittaohjelmiin ja viruksiin, jotka voivat uhata aluksen tietojärjestelmiä. Kyberturvallisuuskoulutuksien niukkuus herättää myös kysymyksiä, sillä niitä ei järjestetä säännöllisesti. Lisäksi suurin osa kyberturvallisuustaidoista on sidottu varustamoiden IT-tukeen, jolloin apu on harvoin fyysisesti laivalla.

Asiasanat: Merenkulku, konepäällystö, inhimillinen tekijä, kyberturvallisuus, kyberhygienia

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Laura Salminen
Thesis title	Impact of Human Factor on maritime cyber security in the engine department of the ship
Commissioned by	South-Eastern Finland University of Applied Sciences – Project on Human Factor in Ship ECR Safety Management
Time	2022
Pages	72 pages, 1 appendix page
Supervisor	Joel Paananen

ABSTRACT

This thesis aimed to established how cyber security is seen in the engine department of the vessel and how human factor affects the cyber hygiene skills. The objective of the thesis was to examine how the perception of cyber security among the licensed engineering crew is reflected in the routines and tasks on the vessel.

The theory section examines the layers between cyber security and studies the role of the human factor in the engine department of the vessel. The part focused on cyber security examines the risks in the Internet and presents available means for protecting against cyber threats. Interviews were made with marine engineers to define the investments that had already been made in cyber security. The impact of the human factor in the work of the engine crew is examined through different scenarios to illustrate the operation of the engine control room and engine room as well as the awareness and performance of the engine crew in different situations.

The thesis provides a picture of the current cyber security competence onboard vessels. From the engineering department's point of view, the main challenges are related to malware or viruses on computers and smart devices. The scarcity of cyber security training also raises concerns, and it should be more regularly organized. In addition, majority of cyber security competence is provided by the support of shipowners, which means that help is rarely physically available.

Keywords: marine engineering, cyber hygiene, cyber security, human factor

SISÄLLYS

1 JOHDANTO

Merenkulkuun kohdistuneiden kyberhyökkäysten on arvioitu kasvaneen koronapandemian aikana jopa nelinkertaiseksi, eivätkä varustamot ole halukkaita kertomaan julkisuuteen kaikista kiristysyrityksistä. Pandemia-aika on tehostanut rahdin kulkua merellä lentoliikenteen hiljennettyä kasvattaen kyberhyökkäyksiä. Suurin osa hyökkäyksistä jää vähälle huomiolle, koska joko varustamot maksavat kiristäjille tai ne eivät ylitä uutiskynnystä. (Tuomaala 2021.) Tästä voidaan johdonmukaisesti olettaa, että kyberhyökkäysten vaikutuksista saadaan vain osa selville ja ne vaikuttavat merkitsevästi merenkulun kokonaisturvallisuuteen. Tästä saatavan trendin perusteella entistä tuhoisampia hyökkäyksiä voidaan seurata jopa lähietäisyydeltä.

Suomeen kohdistuneet kyberuhkat ovat kasvaneet ja merkittävimpinä voidaan pitää poliittisia ratkaisuja tai suurien organisaatioiden päätöksiä, jotka saattavat aktivoida ja motivoida hyökkääjiä. Keskeisiä uhkia ovat kiristyshaittaohjelmat, joiden määrä kasvaa vauhdilla. Monet organisaatiot Suomessa ovat joutuneet näiden haittaohjelmien uhreiksi. Tämän takia elintärkeät toiminnot voivat vaarantua. (Kybersää 2022.) Koska suurin osa Suomeen saapuvasta tavarasta kulkee meriteitse, uhan alla on koko meriliikenne.

Merenkulussa alusten kriittisten järjestelmien suojeleminen ei ole yhtä hyvällä tasolla kuin yleinen turvallisuus, mikä pitäisi ottaa huomioon päätöksenteossa. Uudet alukset ovat täynnä automaatiota ja sähköisiä järjestelmiä, joten ne ovat täynnä verkkoon kytkettyjä IoT[1]-laitteita. (Latva-Teikari 2021.) Tosin automaation kasvattaminen aluksissa on auttanut vähentämään inhimillisten virheiden mahdollisuutta ja näin ollen parantanut aluksien turvallisuutta. (Nevalainen 2022).

Turvalliset työolot eivät ole ainoastaan lakisääteinen ja moraalinen velvollisuus, vaan niistä on tutkittua hyötyä taloudellisesti yritykselle. Investoimalla työpaikan turvallisuuteen, voidaan välttää ”läheltä piti” -tilanteita. Kyseiset investoinnit vaikuttavat myönteisesti työmotivaatioon, työn laatuun sekä yrityksen maineeseen. Tämän lisäksi ne vaikuttavat positiivisesti työntekijöiden ja

[1] Internet of Things eli esineet tai laitteet, jotka ovat kytkettyinä Internetiin.

asiakkaiden tyytyväisyyteen ja yrityksen taloudelliseen menestykseen. (ISSA 2017.)

2 TUTKIMUKSEN TAUSTA

Suomi on riippuvainen merenkulusta, sillä lähes 90 % viennistä ja tuonnista tapahtuu meriteitse ja lipun alla seilaa yli 100 alusta (Suomen varustamot s.a.). Koska suomalaisia merenkulkijoita matkustaa ympäri maailmaa jatkuvasti, tutkimuksen kohteena oli selvittää, miten inhimilliset tekijät vaikuttavat merenkulun kyberturvallisuuteen aluksen koneosastolla ja kuinka koulutuksen avulla voidaan lisätä kyberhygieniaa[2] suomalaisissa aluksissa koneinsinööreille.

Tutkimuksen lähtökohtana oli selventää aluksen päällystön ja miehistön tietoturvallisuustasoa ja miten inhimilliset syyt altistavat kyberuhkan mahdollisuudelle. Työn tarkoituksena oli pohtia inhimillisen toiminnan syy-seuraussuhdetta, ja kuinka se vaikuttaa aluksen operointiin koneosastolla. Lähtöoletamuksena voidaan kuitenkin pitää aluksen tietoturvatason olevan ainakin 10 vuotta jäljessä maaorganisaatioiden tietoturvatasosta, joista laajin syy perustuu koulutuksien vähyyteen. Tämä oli yksi tehtyjen haastatteluiden peruskysymyksistä.

Tämän opinnäytetyön tavoitteena on herättää sekä alusten miehistön ja aluksista vastaavien päälliköiden, omistajien, että varustamoiden mielenkiinto aihealueen kriittisyydelle ja henkilöstön kouluttamiselle. Työn toimeksiannosta vastasi Kaakkois-Suomen ammattikorkeakoulu Oy:n Human Factor in Ship ECR Safety Management -hanke, jota William ja Ester Otsakorven säätiö rahoittaa. Hanketta toteutettiin yhdessä Työterveyslaitoksen kanssa.

2.1 Menetelmät ja teoreettinen viitekehys

Keskeisenä menetelmänä tässä opinnäytetyössä ovat haastattelut, joilla on tarkoitus saada ymmärrys tämän hetken kyberturvallisuuden taitotasosta

[2] Kyberhygienialla tarkoitetaan toimenpiteitä, joilla tietokoneiden ja IoT-laitteiden käyttäjät voivat parantaa verkon puhtautta. Tällä pyritään turvallisuuskeskeiseen ajattelutavan muodostumiseen ja sen omaksumiseen. Keskeinen periaate on, että kyberhygieniasta tulee päivittäinen rutiini. (Kaspersky 2022).

aluksien koneosastolla ja kerätä tietoa tämän hetken aluksien päällystön ja miehistön tietoturvataidoista inhimillisen tekijän valossa. Haastateltavina ovat aluksien konemestarit ja konepäälliköt.

Kyberturvallisuuskulttuurin muutos tapahtuu tietoisella panostamisella. Käyttäjiä ja organisaatioita on ohjattava auttamaan asettamaan perusasiat kuntoon. Tällä viitataan mm. tietoturvaohjelmiin, salasanoihin ja yleisen huomion kiinnittämiseen kyberasioissa. Jatkuva muutos bittimaailmassa lisää tiedottamisen ja käyttäjien koulutettavuuden tarpeellisuutta. Kyberturvallisuus tarkoittaa bittien maailman turvallisuutta ja sitä on kyettävä johtamaan ja rakentamaan toivottuun suuntaan. (Limnell ym. 2014, 39–43.)

Turvallisuus on riippuvainen fyysisestä todellisuudesta sekä yhteisestä ymmärryksestä, miten asiat todellisuudessa ovat. Jotta tämä tunne vahvistuisi, on pystyttävä tekemään sellaisia toimenpiteitä, jotka parantavat turvallisuutta. Puutteellinen ymmärrys asioiden oikeasta tilasta voi johtaa illuusioon. Tästä syystä tunnemme itsemme turvatuiksi, koska emme tiedä asioiden oikeasta tilasta. (Limnell ym. 2014, 35.)

2.2 Tutkimustehtävän rajaus ja tutkimusongelmat

Tutkimuskysymys on kuvaileva ja sen pohjalta etsittiin vastauksia kysymykseen, miten inhimilliset tekijät vaikuttavat merenkulun kyberturvallisuuteen aluksen koneosastolla ja jatkokysymykseen, kuinka koulutuksen avulla voidaan lisätä kyberhygieniaa suomalaisissa aluksissa koneinsinööreille. Opinnäytetyössä pohdittiin, mitä inhimillinen tekijä ja kyberturvallisuus pitävät sisällään, ja miten aiheesta voidaan kerätä tietoa sekä ammentaa sitä tässä tutkimuksessa.

Tutkimuksen tarkoituksena on lisätä kaikkien laivahenkilöiden tietoutta kyberturvallisuusriskeistä omalla henkilökohtaisella toiminnallaan. Sen pohjalta saadaan kartoitettua ymmärrys kyberturvallisuustaitojen laajuudesta. Työ toteutettiin kvalitatiivisella eli laadullisella menetelmällä ja siinä käytettiin hyväksi humanistista ajattelutapaa. Tutkimusta lähdettiin toteuttamaan Survey- ja tapaustutkimuksen kautta. Survey-tutkimuksen pohjalta pyrittiin kerätyn aineiston avulla vertailemaan, kuvailemaan ja selittämään ilmiötä osana

haastattelujen vastauksien ja taustatutkimusta. Tapaustutkimuksen tavoitteena oli kuvailla ilmiötä ryhmän antaman vastauksen perusteella. (Hirsjärvi ym. 2009.)

Kvalitatiivinen menetelmä kuvaa todellista elämää, jolloin todellisuus toteutuu vaiherikkaana. Tutkimusmenetelmää hyödyntäen, pyrittiin tutkimaan alue mahdollisimman tarkasti ja kokonaisvaltaisesti. Tavoitteena oli kerätä tosiasioita haastattelujen seurauksena. Koska tutkimus perustuu lähes tutkimattomaan aiheeseen, joudutaan käyttämään myös joitakin kvantitatiivisen menetelmän perusteita ja luomaan ”tilastotietoa” tästä hetkestä. Ihmiset ovat kuitenkin tiedon keruun perusta ja suurin osa opinnäytetyöstä tultiin perustamaan vastauksien ja niiden päätelmien varaan, sillä tapaus on ainutlaatuinen. Haastattelujen kohdejoukko oli tarkoitusmukainen ja ennalta määrätty, vaikka mukaan mahtui muutamia ”yllätysvieraita”. (Hirsjärvi ym. 2009.)

Aineisto käsittää joukon yksilöhaastatteluita, joiden perusteella saatiin kuva vallitsevasta tiedon ja taidon tilasta. Ajatuksena: ”yksityisessä toistuu yleinen”, kuvaa aineiston luotettavuutta. Lisäksi yhdeksi isoksi osaksi opinnäytetyötä muodostui HF Tool™ -koulutus, joka järjestettiin Kotkassa, Kaakkois-Suomen ammattikorkeakoulun tiloissa 18.8.2022.

2.3 Haastattelut

Haastattelut toteutettiin teemahaastattelun turvin. Se on kahden ääripään (strukturoitu ja avoin haastattelu) välimuoto, mikä antoi joustavuutta haastatteluja tehdessä. Haastattelut suoritettiin joko puhelin-, Teams- tai sähköpostihaastatteluina. Referoivaa litterointia käytettiin kerätyn aineiston valikoimisessa ja yleistämisessä. Haastatteluissa esitettiin kysymyksiä pääasiassa konepäälliköille ja konemestareille sekä maissa työskentelevälle asiantuntijalle ja Vesikuljetuspoolille. Haastateltavat työskentelevät suomalaisilla aluksilla: matkustaja-, Ropax-, ja kuivarahtialuksella sekä tankkerilla, jäänmurtajalla ja erikoisaluksella. Anonymiteetin vuoksi alukset tullaan nimeämään alus A, alus B, alus C, alus D, alus E ja alus F.

Haastateltavien kokonaismäärä koostui kahdeksasta henkilöstä. Haastateltaviin otettiin yhteyttä sähköpostin kautta, jonka jälkeen sovittiin haastattelulle

sopiva ajankohta. Haastattelut nauhoitettiin ja niiden päätyttyä, ne kirjoitettiin puhtaaksi. Tämän jälkeen kaikista haastatteluista tehtiin yhteenveto ja niiden yhtymäkohtia pohdittiin, jotta tutkimusongelmaa saatiin purettua. Energia-alan turvallisuusasiantuntijan haastattelussa käytössä oli erilliset kysymykset ja niiden pääpaino oli inhimillisessä tekijässä. Tämä haastattelu toteutettiin sähköpostitse ja myöhemmin esitetyissä havainnoissa, referoidaan tätä haastattelua. Haastateltavan nimi ja yritys jää salassa pidettäviksi. Vesikuljetuspoolille oli myös omat kysymykset, jotka koostuivat neljästä kysymyksestä ja näitä vastauksia referoidaan tässä työssä osana johtopäätöksiä.

3 KYBERTURVA

Merenkulkuala sekä kauppa-alukset ovat alttiina tietoturvauhkille, ja lisääntyneen digitalisoitumisen ansiosta verkkoon liitetty tietotekniikka (IT)[3] ja operatiivinen tekniikka (OT)[4] ja meriteollisuuden ohjausjärjestelmät sekä satelliittiviestintä, ovat vaarassa kyberhyökkäyksille. Kyberturvallisuutta tulee hallita asianmukaisesti koko alalla sekä alusten, miehistön että rahdin suojaamiseksi. IT- ja OT-järjestelmiin yhdistyvät riskit eroavat toisistaan siinä mielessä, että IT-järjestelmien riskit vaikuttavat pääasiassa talouteen ja maineeseen, kun taas OT-järjestelmät voivat vaikuttaa turvallisuuteen uhaten ihmishenkiä, ympäristöä ja omaisuutta. (Huoltovarmuuskeskus 2021, 5.)

Hallintojen, varustamoiden sekä luokituslaitosten tulee huomioida riskienhallinta kyberturvallisuudelle osana ISM-säännöstön edellyttämiä tavoitteita ja vaatimuksia. Kyberriskienhallintajärjestelmä on yhdistävänä osana alusten ISM-turvallisuusjohtamisjärjestelmän riskienhallintaa. Kyberturvallisuus tulee ottaa huomioon varustamoiden toimesta riippumatta aluksien järjestelmien käyttöönottovuodesta tai alusten toiminta-alueesta. (Traficom 2020.)

Aluksien IoT-järjestelmät sisältävät lähes minkälaisia laitteita, jotka voidaan kytkeä verkkoon tuottamaan, vastaanottamaan tai jakamaan tietoa. IoT-laitteet yleistyvät, sillä ne vähentävät kustannuksia ja lisäävät tehokkuutta. Suuri reaaliaikainen tietomassa voidaan jalostaa käyttökelpoisiksi tunnusluvuiksi tai

[3] IT-järjestelmillä tarkoitetaan mm. työasemia, sähköpostia, Intranetiä ja kansioiden jakoa, liiketoimintaa ja rahoitusjärjestelmiä. (Huoltovarmuuskeskus 2021, 14.)
[4] OT-järjestelmistä puhuttaessa tarkoitetaan navigaatiolaitteita, yhteyksiä (Satcom, Wi-Fi ja 4G), tehonhallintaa ja päätelaitteita sekä sensoreita. (Huoltovarmuuskeskus 2021, 14.)

tilannekatsaukseksi aluksen kunnosta ja sen toiminnasta. Tietokoneiden määrä aluksilla riippuu pitkälti laivasta, sen tarkoituksesta ja iästä. Vanhemmissa aluksissa on usein PC-tietokone, kun taas uudemmissa aluksissa on käytössä useita tietokoneita erilaisiin käyttötarkoituksiin. Uusimmissa aluksissa on sadoittain sensoreita, jotka voivat olla yhteydessä verkkoon ja lähettää reaaliaikaista dataa aluksen kunnosta esim. varustamolle. (Latva-Teikari 2021.)

3.1 Kyberturvallisuuden tasot

Kyberturvallisuutta ei voida tarkastella pelkästään pintapuolisesti, sillä sitä ei välttämättä ymmärretä täydellisesti. Asiaa voidaan tarkastella kuitenkin tasoina, jolloin voidaan jakaa peruselementit ja haasteet osaksi puolustusta – millä tavalla ihminen, verkko, tietokone, järjestelmä, tieto ja pilvipalvelut vaikuttavat koko kyberturvallisuuteen. *Wilsonin mukaan ihmiset ovat suurin syy kyberuhkiin.* (Wilson 2021, 47–48.)

Kyberturvallisuustasojen ymmärtämiseksi, pohditaan asiaa tasoajattelun näkökulmasta, minkä seurauksena kyberhyökkäykset toistavat samaa kaavaa. Esimerkiksi kyberhyökkääjä tunnistaa työntekijän, joka toistuvasti ohittaa yrityksen kyberturvallisuuskoulutukset ja näkee tässä sisäänpääsymahdollisuuden yrityksen verkkoon. Hyökkääjä tekee väärennetyn sähköpostiosoitteen ja lähettää työntekijälle viestin väittäen sen olevan yrityksen IT-osastolta, missä olisi päivitys koneelle. Koska työntekijä ei osallistunut koulutuksiin, hän lukee viestin ajattelematta edes sen kontekstia. Kun ensimmäinen taso murretaan, hyökkäys pääsee verkkotason läpi ja samalla se linkittyy käyttöjärjestelmään. Tällöin hyökkäys voi kiinnittyä seuraavaan järjestelmään verkon sisällä, jolloin se voi levittäytyä itsestään myös muihin järjestelmiin ja valita kohteena olevan sovelluksen. (Wilson 2021, 47–48.)

3.1.1 Luottavainen ihminen

Kyberturvallisuudessa manipulointihyökkäykset tarkoittavat käyttäjien huijaamista suorittamaan tiettyjä toimia tai paljastamaan luottamuksellisia tietoja. Erään kyberturvallisuusyrityksen mukaan 98 prosenttia kyberhyökkäyksistä perustuu manipulointihyökkäyksiin, ja uudet työntekijät ovat eniten alttiina näille hyökkäyksille. 63 prosenttia onnistuneista iskuista tapahtuu Internet-

lähteessä ja johtuvat virheistä tai petoksista. Tilastot siis havainnollistavat *tasoajattelun alkavan ihmisistä,* jolloin kyberpuolustus on haasteellista: ihmiset usein valitsevat mukavuuden turvallisuuden sijaan ja ovat luonnostaan luottavaisia. (Wilson 2021, 49–52.)

Uusi teknologia tuo tullessaan mukavuutta ja mukavuus uusia käyttäjiä. Tämä johtaa siihen, että haavoittuvuudet lisääntyvät. Ihmiset mieluummin maksavat mukavuudesta kuin turvallisuudesta varsinkin, kun turvallisuusprotokollien hyödyt eivät ole selkeitä. Tästä voidaan päätellä, että *ihmiset ovat aina alttiina kyberuhkille*. Teknologiainnovaatiot kehittyvät vauhdilla, jolloin kyberturvallisuusasiantuntijat eivät aina pysy perässä. Parhaimmat kyberturvallisuusratkaisut ovat kuitenkin selkeitä ja helppokäyttöisiä. (Wilson 2021, 49–52.)

3.1.2 Verkon turvallisuus

Tasoajattelun seuraava vaihe on verkon turvallisuus. Tämä kohta voidaan ajatella esimerkiksi aidaksi. Tämän kautta voidaan pohtia kotiverkkoa, jota käytetään päivittäin: saatavilla on Internet-yhteys, jota hyödynnetään moneen eri tarkoitukseen, kuten TV:n katseluun tai musiikin kuunteluun. Kotona Wi-Fi-verkko on oma ja yksityinen, kun siihen liitytään. Asiaa voidaan tarkastella toisesta näkökulmasta: mitä jos naapurikin voisi liittyä tähän verkkoon? Silloin myös naapuri näkisi kaikki verkkoon kytketyt laitteet sekä niiden sisällön. Verkon toivotaan kuitenkin pysyvän usein yksityisenä. (Wilson 2021, 53–55.)

Kun ensimmäinen taso murretaan, tulee hyökkääjän läpäistä verkkotaso. Verkon suojaus tarkoittaa kaikkia niitä suojaustoimenpiteitä, joilla pyritään estämään ja havaitsemaan pääsyt sisäisiin järjestelmiin ja resursseihin. Toisen tason tasoajattelun tueksi voidaan ajatella asiaa OSI[5]-mallin avulla: järjestelmä mahdollistaa monipuoliset viestintäjärjestelmät hyödyntäen standardien ohjeita, jotka mahdollistavat eri tietokonejärjestelmien kommunikoinnin keskenään. (Wilson 2021, 53–55.)

Verkkoturvallisuuden takaamiseksi on olemassa ratkaisuja, jotka estävät vahinkojen eskaloitumisen: palomuurit, tunkeutumisen havaitsemisjärjestelmät,

[5] OSI-malli koostuu sanoista Open Systems Interconnection

IPS[6]-järjestelmät sekä tietoturva- ja tapahtumahallintajärjestelmät. Lähes kaikki verkkolaitteet pohjautuvat kyseisiin ratkaisuihin. *Palomuuri* on verkon suojauslaite, joka monitoroi ja säätelee sisään ja ulosmenevää verkkoliikennettä turvallisuussääntöjen mukaisesti. *Tunkeutumisen havaitsemisjärjestelmä* on ohjelmisto tai laitteisto, joka etsii verkkoliikenteestä epäilyttävää toimintaa ja tunnettuja uhkia. Tämä järjestelmä tuntee uhkat ja hälyttää heti, kun niitä havaitaan. *IPS-järjestelmä* sisältää kaksi yllä olevaa järjestelmää: kun järjestelmä huomaa tunkeutumisen verkossa, se voidaan pysäyttää automaattisesti. *Tietoturva- ja tapahtumien hallintajärjestelmä* on laite, joka tuo kaikkien tasojen, verkon, sovelluksien ja tietokonejärjestelmän tiedot yhteen. Hyökkääjän näkökulmasta on hyödyllisintä levitä nopeasti jokaisen tason läpi. (Wilson 2021, 53–55.)

3.1.3 Käyttöjärjestelmän turvallisuus

Kun hyökkääjä on päässyt ensimmäisen ja toisen tason läpi, hyökkääjä on tietokoneen käyttöjärjestelmä- tai isäntätasolla. Tämä taso on usein verrattavissa Microsoft Windowsiin, Applen OS X:n tai avoimen lähdekoodin Linux OS:ään. Modernit OS[7]-järjestelmät on suunniteltu toimimaan monikäyttäjäympäristössä ja toiminnoissa, mitkä vaativat useiden asioiden tehokasta ja yhtäaikaista käsittelyä. Näin ollen OS:n täytyy vähintään käsitellä lajittelua, muistin suojausta ja pääsynhallintaa. Lajittelun ideana on pitää yhden käyttäjän sisällöt erikseen muista käyttäjistä. Tämä viittaa käyttäjän digitaaliseen omaisuuteen, kuten tiedostoihin, kansioihin, lupiin/oikeuksiin tai muistiosaan. Muistin suojaus estää yhtä sovellusta korruptoimasta toista, kun ne ovat käynnissä samanaikaisesti. Pääsynhallinta on yksi kyberturvallisuuden periaatteista ja keskittyy estämään luvattomia pääsyjä olennaisiin resursseihin. (Wilson 2021, 55–58.)

Pääsynhallinta näyttäytyy erilaisissa muodoissa, kuten pakollisena, harkinnanvaraisena, rooli- ja sääntöpohjaisena. Käyttäjä ei voi muokata järjestelmävalvojan asettamia pakollisia pääsynhallinnan oikeuksia. Käyttäjä taas voi itse määritellä harkinnanvaraiset käyttöoikeudet, esimerkiksi luvat tiettyihin tiedostoihin. Käyttäjät voivat muuttaa, päivittää tai muokata lupia. Pakollinen tiedostojen valvonta ei tosin enää kuulu käyttäjälle, vaan se siirtyy esimerkiksi

[6] IPS-järjestelmällä tarkoitetaan murron estojärjestelmää
[7] OS-järjestelmät ovat tietokoneiden käyttöjärjestelmiä

järjestelmävalvojalle. Roolipohjainen pääsynhallinta keskittyy luokittelemaan pääsyn käyttäjämallin perusteella. Usein tämä on yleiskäytössä tai järjestelmävalvojalla. Sääntöpohjainen pääsynhallinta määrittelee ehdot pääsylle esimerkiksi kellonajan tai logististen pääsyrajoituksien mukaan. Esimerkiksi tiedostoon pääsee ainoastaan käsiksi tiettyyn kellonaikaan. (Wilson 2021, 55–58.)

3.1.4 Sovelluksen/ohjelmistojen turvallisuus

Usein hyökkääjän pääkohteena ovat sovellukset, sillä niitä on helpompi hyödyntää (rikolliseen toimintaan) kuin käyttöjärjestelmää. Yksi syy tähän on, että sovellukset ovat suunniteltu päivittymään useammin kuin käyttöjärjestelmät. Koska käyttöjärjestelmien komponentit ovat standardeja, niitä pitää harvoin korvata tai päivittää. Sovelluksissa sen sijaan on enemmän ominaisuuksia kuin käyttöjärjestelmissä. (Wilson 2021, 58–59.)

Esimerkiksi Microsoft Wordissa on yli sata ominaisuutta sekä mahdollisuus sisällyttää muita lisäosia sovellukseen esim. makrojen kautta. Tietojenkäsittelyssä makro on rajattu yksittäinen käsky, joka laajenee automaattisesti käskyjoukoksi tietyn tehtävän suorittamiseksi. Tyypillisesti makro toimii esimerkiksi, kun avataan Microsoft Word ja *asetetaan* sovelluksessa tekstin fontiksi Arial tai Times New Roman. Tämä tapahtuma johtaa takaisin ihmiseen ja ihmisen toimintaan. Kun on totuttu käyttämään tiettyä sovellusta tai fonttia, ei ajatella sen turvallisuutta. Tämä johtaa dilemmaan, jossa mukavuus voittaa turvallisuuden. (Wilson 2021, 58–59.)

Sovelluksien suojaukset, kuten virustorjunta tai haittaohjelmien torjuntaohjelmisto, suojelevat sovellushyökkäyksiltä. Usein sovelluksien suojausmenetelmät perustuvat tietoon, jolta hyökkäys mahdollisesti näyttää etukäteen. Kun hyökkäyksen ominaisuudet tunnetaan, voidaan kehittää suojaus, joka etsii ominaisuuksia ja pysäyttää hyökkäykset ennen kuin syntyy vahinkoa. Turvallisempien ohjelmistojen suunnittelun pitäisi olla sovellusturvallisuuden painopiste, sillä se on ennaltaehkäisyä. (Wilson 2021, 58–60.)

3.1.5 Tietojen turvaaminen

Salasana tai jokin muu henkilökohtainen tunniste on kyberhyökkääjien näkökulmasta arvokkainta omaisuutta. Tyypillisesti tämä tunniste piilee tilatiedossa: lepotilassa, jolloin se ei ole käytössä, matkalla, jolloin se on lähetetty toisesta kohteesta toiseen sekä käytössä, jolloin tieto on kirjaimellisesti käytössä. Luottamuksellisuuden, eheyden ja ensisijaisesti saatavuuden vuoksi, tiedot ja tunnisteet ovat suojattu kaikissa näissä tilatiedoissa ja suojamekanismi vaihtelee tilatiedottain. Lepotilatietojen suojaus näistä kolmesta on yksinkertaisin, sillä se saadaan aikaan joko salauksella, pääsynhallinnalla tai molempien yhdistelmällä. Tiedot on suojattu kaikissa tilatiedoissa usein erilaisilla salausavaimilla. Jokaisella tilatiedolla (lepo-, matka- ja käyttötila) on oma salausavaimensa. (Wilson 2021, 61–63.)

3.2 Määräykset

Aluksien kyberturvallisuus pohjautuu ensikädessä Solaksen määräyksien kautta ISM[8]- ja ISPS[9]-koodiin, jolloin turvallisuuteen ja turvalliseen työskentelyyn otetaan kantaa. Suomessa Traficom vartioi sääntöjen noudattamista ja luokituslaitokset tuovat omat näkökulmansa näkyviin erilaisilla ohjeilla, kiertokirjeillä ja suosituksilla. Luokituslaitokset puolestaan perustelevat suosituksensa erilaisilla standardeilla.

3.2.1 Kansainvälinen merenkulkujärjestö

IMO[10]:n vuonna 2017 ilmestynyt kiertokirje MSC-FAL.1/Circ.3, kertoo kiireellisestä tarpeesta lisätä kyberuhkien ja haavoittuvuuksien tietoisuutta merenkulussa. Ohjeessa annetaan korkean tason suosituksia kyberriskien hallintaan. Koska kyberteknologiasta on tullut olennainen osa merenkulkua, järjestelmien on oltava kansainvälisten standardien ja lippuhallintojen vaatimusten mukaisia. Pääsy järjestelmiin ja niiden yhteen liittäminen tai verkottamisen aiheuttamat haavoittuvuudet, voivat johtaa kyberriskeihin. Hakkerointi, haittaohjelmat

[8] ISM muodostuu sanoista: International Safety Management, joka on kansainvälisessä merenkulussa käytössä oleva turvallisuusjohtamisjärjestelmä. Turvallisuusjohtamisjärjestelmä on pakollinen jokaisessa aluksessa.
[9] ISPS muodostuu sanoista: International Ship and Port Facility Security, ja tämän koodin tavoitteena on lisätä turvallisuutta aluksilla ja satamissa.
[10] IMO muodostuu sanoista: International Maritime Organization, joka hallinnoi merenkulun turvallisuusasioita.

tai hyvälaatuisten tahattomat seuraukset, kuten ohjelmistojen huolto, aiheuttavat uhkia. Seuraavassa ohjeessa esitetään osat, jotka tukevat tehokasta kyberriskien hallintaa:

- Tunnistus: henkilöstön roolien ja vastuiden määrittäminen kyberriskien hallinnassa sekä järjestelmien, resurssien, tietojen ja ominaisuuksien tunnistus, jotka vikaantuessaan aiheuttavat riskin aluksien toiminnalle.

- Suojaus: riskienhallintaprosessien, toimenpiteiden, ja varasuunnitelmien käyttöönotto, jotta voidaan suojautua kybertapahtumilta ja varmistaa laivaustoimintojen jatkuvuus.

- Havaitseminen: kybertapahtumien havainnoinnin kehittäminen ja toteuttaminen ajoissa.

- Reagointi: toimintojen ja suunnitelmien kehittäminen ja toteuttaminen, joiden avulla turvataan ja palautetaan järjestelmät, jotka ovat välttämättömiä laivaustoiminnalle tai -palvelulle.

- Palauttaminen: toimenpiteiden tunnistaminen kyberjärjestelmien varmuuskopioimiseksi ja palauttamiseksi, jotka ovat välttämättömiä kybertapahtuman kannalta. (MSC-FAL.1/Circ.3, 1–3.)

3.2.2 Traficom

Traficom perustaa ajatuksensa merenkulun säännöstöille, mutta eivät ole vielä luoneet omia määräyksiään, lakejaan, tai muita ohjeita, jotka liittyisivät suoraan merenkulun kyberturvallisuuteen. Traficom käyttää ohjeissaan ENISAN[11] NIS-direktiivin lainsäädäntöä ja direktiivin tavoitteena on parantaa kyberturvallisuutta koko Euroopan alueella. Tämä lainsäädäntö käyttää tunnettuja standardeja ohjeissaan. Kyseinen NIS-direktiivi päivittyy kuitenkin loppuvuoden 2024 aikana, jolloin sen tilalle tulee NIS2-direktiivi. (Traficom s.a.; Council of the European Union 2022.)

Traficom kuitenkin ylläpitää kyberturvallisuuskeskusta, joka luo ohjeita ja määräyksiä kyberturvallisuudelle, mistä voidaan ottaa poimintoja merenkulkuun. Kyberturvallisuuskeskuksen Kybersää julkaisee kuukausittain havaintoja Suomessa tapahtuvista tai Suomeen kohdistuneista kyberuhkista. Huoltovarmuuskeskus sen sijaan on luonut ohjeet merenkulun kyberturvallisuudelle. (Traficom s.a.; Huoltovarmuuskeskus s.a.)

[11] European Union Agency for Cybersecurity

3.2.3 Luokituslaitokset IACS ja DNV

IACS[12]:n mukaan on tarpeellista laatia yhteinen toimintasuunnitelma, jotta alukset pysyvät kybersietokykyisinä. Vähimmäisvaatimukset, joita sovelletaan kyberuhkiin, perustuvat tavoitepohjaiseen lähestymistapaan kyberkestävien alusten tekemiseksi. (IACS UR E27: 2022.)

Vuonna 2024 voimaan astuvassa säädöksessä UR[13] E26 ja UR E27 on määritetty sinä vuonna valmistuvien aluksien kyberturvallisuusjärjestelmien vaatimukset. Tietokonepohjaisten järjestelmien käyttö aluksella ja sen soveltaminen sisältää vaatimukset tietokonepohjaisten järjestelmien suunnittelulle, rakentamiselle, käyttöönotolle ja ylläpidolle. Säädöksessä on lueteltu mm. kuinka käyttäjä voi tunnistautua päätelaitteelle, kuinka pitkä salasanan tulee olla tai, kuinka langatonta järjestelmää käytetään oikein. (IACS UR E27: 2022.) IACS käyttää pohjana ohjeistuksissaan turvallisuusstandardeja, kuten ISO/IEC 12207[14], ISO/IEC 27001[15] ja ISO/IEC 90003[16] sekä NIST[17]:n ohjeita. (IACS s.a.)

IACS:n UR E22 vaatimukset kohdistuvat ohjelmistojen toimivuuteen ja ohjelmistoa tukeviin laitteistoihin, mitkä tarjoavat luokitusvaatimusten alaisia ohjaus-, hälytys-, valvonta-, turvallisuus-, tai sisäisiä viestintätoimintoja. Säädös E22 on tällä hetkellä voimassa ja se sisältää tarkan kuvauksen, kuinka alukseen sijoitettuja tietokonepohjaisia järjestelmiä tulee testata ennen niiden asentamista. Kategoria III:n (kriittisimmät järjestelmät, joiden rikkoutumisen seurauksena on välitön vaara joko ihmiselle tai luonnolle) järjestelmät eivät saa käyttää langattomia datayhteyksiä, ellei siitä ole luokituslaitoksen hyväksyntää. Näitä järjestelmiä ovat mm. propulsiojärjestelmä, sähkönsyöttö sekä ohjausjärjestelmät. (IACS UR E22: 2016, 4.)

[12] International Association of Classification Societies
[13] Unified Requirements
[14] Standardi järjestelmä- ja ohjelmistosuunnittelulle – ohjelmiston elinkaariprosessit
[15] Standardi tietoturvallisuuden hallintajärjestelmän toteuttamisesta, ylläpitämisestä, luomisesta ja jatkuvasta parantamisesta
[16] Standardi ohjelmistosuunnittelusta ja soveltamisohjeet (ISO 9001:2008) tietokoneohjelmistoon
[17] National Institute of Standards and Technology

Aluksen sisäisen langattoman järjestelmän on täytettävä kansainvälisen teleliiton radiotaajuus- ja tehotasovaatimukset sekä lippuvaltion vaatimukset. Langattomille tietoliikennelaitteille on suoritettava testit satama- ja meriajon aikana, jotta voidaan todistaa radiotaajuuslähetyksen onnistuminen. Tämä ei kuitenkaan saa aiheuttaa missään laitteessa vikaa, eikä yhteys saa katketa itsestään sähkömagneettisten häiriöiden seurauksena käyttöolosuhteissa. (IACS UR E22: 2016, 10.)

IACS:n Suosituskirje 166 ohjeistaa selkeästi ja kattavasti, miten aluksien kyberturvallisuus tulisi rakentaa. Suosituskirje kertoo yksityiskohtaisesti, kuinka tietokonepohjaisia järjestelmiä käytetään, huolletaan ja testataan. Ennaltaehkäisy on tärkeää. Miehistön, päällystön ja omistajien (varustamo, telakka, ym.) tulee olla tietoisia kyberriskeistä ja pysyä niiden suhteen valppaina, sillä heikkoudet ja haavoittuvuudet kerääntyvät siihen asti, että alkuperäisestä ohjelmasta tulee tarpeeton. Osana kyberriskien hallintaa tulee omistajan tarjota asianmukaista koulutusta tietoturvaan liittyvistä riskeistä henkilöstölle, joka on valtuutettu olemaan vuorovaikutuksessa tämän suosituksen kattamien tietokonepohjaisten järjestelmien kanssa. (IACS No166: 2022, 2–54.)

DNV suosittelee arvioimaan aluksilla kaikkia kolmea ulottuvuutta: ihmisiä, prosesseja ja teknologiaa, mitkä ovat olennaisia kyberturvallisuuden sietokyvyn saavuttamiseksi aluksissa sekä organisaatiossa. DNV käyttää suosituksissaan IACS:n ja IMO:n vaatimuksia sekä tunnustettuja IEC-standardeja. Kyberturvallisuuden hallintajärjestelmä CSMS[18] koskee usein OT-järjestelmiä. IT-järjestelmä sen sijaan noudattaa standardia ISO/IEC27001. (DNV CG 0325: 2021.)

CSMS:n tulisi toimia yhdessä muiden aluksen hallintajärjestelmien kanssa, kuten turvallisuusjohtamisjärjestelmän ja tietoturvahallintajärjestelmän kanssa, että ne muodostavat yhtenäisen kokonaisuuden. CSMS ohjaa ihmisten käyttäytymistä sekä määrittelee periaatteet teknisten suojauksien toimivuudelle, koska käyttäjä ohjaa prosessia, prosessi ohjaa teknologiaa ja teknologia ohjaa käyttäjää. Kyseessä siis kyberturvallisuuden kolme peruspilaria, ja kaikki kolme asiaa tulisi huomioida yhdessä, että ne tukevat toisiaan ja luovat turvallisuutta. (DNV CG 0325: 2021.)

[18] Cyber Security Management System

Kyberturvallisuuden luokkamerkintä määritetään, kun suunnitteluasiakirjat ja järjestelmä- ja integrointitestit ovat hyväksyttyjä. Luokkamerkinnän ylläpitämiseksi DNV auditoi CSMS:n. Auditointi varmistaa, että CSMS koostuu vaaditusta sisällöstä, ja että sen käytäntöjä ja menettelyjä noudatetaan. Tämä tarkoittaa, että luodaan dokumentaatiota ja muita todisteita. (DNV CG 0325: 2021.)

CSMS-tarkastus suoritetaan vuosittain katsastuksen yhteydessä. CSMS sisältää käytäntöjä, toimintoja ja tallentamista. Kyberturvallisuusriskien hallitsemiseksi CSMS:n tulee sisältää tietynlainainen ohjenuora, joka on dokumentoitava ja sen tulee olla jäljitettävissä. (DNV CG 0325: 2021.)

Esimerkiksi laitteistot ja käyttöjärjestelmät, ohjelmistosovellukset ja -versiot sekä palomuurit ym. tulee pitää ajan tasalla yksityiskohtaisesti, ja turvallisuuteen liittyvät rakenteet ylläpidetään ja dokumentoidaan. Nämä luettelointitiedot arvioidaan päivitettyjen uhka- ja haavoittuvuustietojen perusteella yleensä kyberturvallisuusorganisaatioiden toimesta. Riskienarviointiin kuuluu seurausten vertailu vahvistettuihin hyväksymiskriteereihin. Riskeillä voi olla erilaisia seurauksia luottamuksellisuuteen, eheyteen ja saatavuuteen, ja näille kohteille voi olla erilaiset hyväksymiskriteerit. (DNV CG 0325: 2021.)

Käytäntöjä ja menettelyjä on kehitettävä ja määritettävä, jotta työntekijät ovat tarpeeksi päteviä turvallisuustavoitteiden ylläpitämiseksi. Kyseisten käytäntöjen tulee sisältää odotuksia, vastuita ja käsitellä kurinpitoprosesseja, jos periaatteita rikotaan. Ylläpidettäviin turvallisuusnäkökantoihin sijoittuu esimerkiksi sähköpostin ja web-palveluiden käyttö, pääsy salassa pidettävään informaatioon, työntekijöiden sopimusvelvoitteet työsuhteen päättymisen jälkeen ja yrityksen laitteiden käyttö yksityiseen tarkoitukseen. (DNV CG 0325: 2021.)

3.3 Kommunikaatio

Yhteydenpito aluksien välillä, sekä aluksien ja maiden välillä on toteutettu eri järjestelmien kautta. Yhteyksiä on paranneltu vuosien varrella, jotta tietoliikenne toimii sekä nopeasti että tehokkaasti. Tällöin data saadaan liikkumaan mahdollisimman ”suoraan”. Alusten viestintäjärjestelmiä käytetään täyttämään

useita erilaisia vaatimuksia sekä tarjoamaan yhteyksiä organisaatiolle, miehistölle tai matkustajille. Seuraavanlaisia järjestelmiä on käytössä:

- Satelliitti – useat eri sovellukset käyttävät satelliittiviestintää alusten väliseen viestintään, jotka kattavat sekä puhe- että datajärjestelmät.

- VHF/UHF – näitä taajuuskaistoja käyttävät viestintäjärjestelmät toimivat näköyhteys- tai yleislähetysalueviestinnässä ja sisältävät merenkulun VHF:n, joka toimii 156–162,025 MHz:n alueella aluksesta toiseen ja aluksesta maihin. Esimerkiksi VHF-kanava 70:tä käytetään digitaaliseen selektiiviseen kutsuun (DSC), jolla tarkoitetaan hakujärjestelmää, joka lähettää ja vastaanottaa datapuheluita hälytystarkoituksiin.

- S-taajuusalue, jossa paikallistetut järjestelmät hyödyntävät 2,4 GHz:n ja 5 GHz:n taajuuskaistojen yksityistä jakoa. Käytetään usein Wi-Fi-, ja Bluetooth-sovelluksissa.

- PABX/GSM, 3G, 4G ja 5G -järjestelmät, jotka voidaan tarjota joko paikallisesti tai etäyhteydellä, jos alukset ovat lähellä rantaa tai lauttoja. Paikallinen PABX- tai GSM-tukiasema voidaan ottaa käyttöön risteilyaluksilla, jotta niillä voidaan tarjota yhteys matkustajille Satcom-järjestelmän kautta maainfrastruktuuriin. Lautat saattavat myös käyttää 4G-yhteyksiä tarjotakseen digitaalista Internet-viestintää matkustajille.

Olennaista on, että kaikki viestintäjärjestelmät tunnistetaan yhdessä eri alijärjestelmien[19] kanssa, joihin ne voidaan liittää kaikissa tunnetuissa luokissa. (Boyes ym. 2017, 38.)

3.4 Lukitsemattoman oven takana seisoo rikollinen

Haittaohjelmien tarkoituksena on vahingoittaa tai hyödyntää ohjelmoitavaa laitetta, palvelua tai verkkoa. Niiden avulla kyberrikolliset keräävät usein dataa, joilla he mahdollisesti kiristävät uhreiltaan taloudellista hyötyä. Sähköpostit, salasanat, matkustajatiedot, miehistötiedot, raha-asiat tai muut vastaavat arkaluonteiset dokumentit, saattavat joutua vaaraan.

[19] Alijärjestelmällä tarkoitetaan palveluntarjoajaa, mikä on laite tai se osa suurempaa kokonaisuutta. Alijärjestelmä viittaa usein laitteistoon, tai jos puhutaan ohjelmistosta, viitataan aliohjelmaan tai johonkin sovelluksen osaan. (PCmag).

3.4.1 Haittaohjelmat

Hyökkäyksiä tukevat haittaohjelmistot ovat viime vuoden aikana kehittyneet. Niiden torjuntaan käytetään sekä innovatiivisia puolustusstrategioita että kestäviksi todettuja perinteisempiä puolustusstrategioita: monivaiheista todennusta tai kattavaa sovellusten tietoturvaa. Haittaohjelmien lopputulos vaihtelee vakoilusta, tunnistetietovarkauteen ja lunnaista tietojen menetykseen, ja niiden tavoitteena on päästä tunkeutumaan kohdeverkkoon. (Microsoft digitaalinen puolustus -raportti 2021, 34.)

Laillisen palvelun väärinkäyttö verkkoviestinnässä on johtanut pilvipalveluiden, kuten Google Driven ja Dropboxin, haittaohjelmiston alkuperäiseen toimitukseen, jolloin haittaohjelmistokampanjat käyttävät laillisia sivustoja lähes kaikkiin haittaohjelmaiskujen vaiheisiin. Haittaohjelmaa ei edes välttämättä tarvitse ladata erillisenä tiedostona. Hakukonetuloksien ja -mainonnan ansiosta haittaohjelmia leviää loppukäyttäjille tehokkaasti: yhdistelemällä laillisia hakukoneoptimointistrategioita ja olemassa olevien tartuntojen väärinkäyttöä, uhrin koneeseen asennetaan selainlaajennuksia, jotka muokkaavat hakutuloksia nostaen hyökkääjän materiaalin hakutulosten kärkeen. Hyökkääjät pystyvät manipuloimaan selaimen hakutuloksia omaksi edukseen. (Microsoft digitaalinen puolustus -raportti 2021, 35–36.)

3.4.2 Kiristyshaittaohjelma

Kyseessä on haittaohjelma, joka sieppaa tai salaa koneen tiedot vaatien hyökkääjälleen maksua usein kryptovaluutassa pitäen varastettuja tietoja hallussaan lunnaita vastaan. Syntyy tietomurto, jossa yrityksen sisäiseen verkkoon päästään käsiksi, ja jonka jälkeen kiristyshaittaohjelma leviää. Tämän seurauksena kaikki tiedot salataan, jotta esim. yritykseltä voidaan vaatia suuria summia rahaa tietojen palauttamista vastaan. Tyypillisesti hyökkääjä sieppaa uhrin arkaluonteiset tiedot ennen kuin aktivoi kiristyshaittaohjelman. Mahdolliset haitat uhrin maineelle kasvavat sitä mukaan, mitä kauemmin neuvotteluissa kestää. Hyökkääjä jättää uhrin tiedot salattuun tilaan ja saattaa paljastaa uhrin arkaluontoisia tietoja Internetissä. Hyökkääjät ovat myös mahdollisesti peukaloineet tietoja ennen niiden palauttamista uhrille. (Microsoft digitaalinen puolustus -raportti 2021, 10,15.)

Kiristyshaittaohjelmat tulevat usein organisaation verkkoon USB-tikkujen välityksellä. Kouluttamalla henkilöstöä vähennetään fyysisestä maailmasta saapuvaa uhkaa. Tällaisessa tilanteessa hyökkäystapahtumana voi olla, että matkustaja-aluksen käytävälle on pudotettu haittaohjelmaa sisältävä USB-tikku tai niitä jaetaan aluksella jonkin tapahtuman yhteydessä. Usein henkilöstö ei osaa ajatella niitä uhkina, ellei niistä ole mainittu organisaation koulutuksissa. *Sähköpostin kautta tulevat haitalliset liitteet tai erikoiset pyynnöt eivät välttämättä nouse mieleen, ellei siitä olla erikseen mainittu.* Organisaation vahvin lenkki verkkorikollisia vastaan on henkilö, joka on päivittänyt tietoturvaosaamisensa oikealle tasolle. (Inkinen 2022, 16.)

Koska verkkorikollisten taito on karttunut vuosien saatossa, kiristyshaittaohjelmista palautuminen on pääasiassa tietojen tallennus. Dataa ei saada enää takaisin, vaan sen tulee olla varmuuskopioitu turvalliseen paikkaan ennen kuin mahdollinen kiristyshaittaohjelma tapahtuu. Täten kiristyshaittaohjelmia vastaan ainoa selviytymiskeino on varmuuskopiointi esimerkiksi pilvipalveluun. Mitä isompi yritys kyseessä, sen isompia lunnaita vaaditaan. (Turvakäräjät -podcast 2021.)

Jos aluksen tietojärjestelmiin on levinnyt kiristyshaittaohjelma ja jälkimaininkeja käydään läpi, on alus täysin offline-tilassa. Kun tietoturvajärjestelmiä on muutettu sekä varmuuskopiot poistettu ja tiedot salattu, eivät käyttäjät pysty kirjautumaan sisään. Lunnaiden maksaminen ei takaa toiminnan palautumista, eikä estä mahdollisia tulevia hyökkäyksiä. Vaikka yksittäisen aluksen näkökulmasta olisi järkevää maksaa lunnaat järjestelmien palauttamiseksi, maksaminen tekee siitä vahingollista. Tämä edistää haittaohjelmien lisääntymisen ja palkitsee kiristäjän sekä kasvattaa kiristäjien liiketoimintamallin suosiota, mikä houkuttelee lisää toimijoita alalle. Kiristysohjelmatyökalujen automaatiotaso ja tehokkuus kasvavat ja tämä laajentaa sekä nopeuttaa hyökkäyksien onnistumista pienemmällä vaivalla. Organisaation on tunnettava maksujen laillisuus, sillä monessa valtiossa suunnitellaan lunnaiden määräämistä laittomiksi. (Microsoft digitaalinen puolustus -raportti 2021, 14–15.)

3.4.3 Tietojenkalastelu ja haitalliset sähköpostit

Vuonna 2020 tietojenkalastelu oli yleisin rikostyyppi FBI:n raportin mukaan. (Microsoft Digitaalinen puolustus -raportti 2021, 20). Kalastelua voi tapahtua monia eri reittejä pitkin, kuten sosiaalisen median, erilaisten linkkien, sähköpostien, tekstiviestien ja kryptattujen tiedostojen kautta: käy lataamassa tiedosto osoitteesta x ja lataa se tietokoneelle. Lisäksi haitallisia dokumentteja voidaan sarjalähettää sähköpostin liitteenä (mailspäm). Sähköpostit ovat vaarallisia, koska niiden kautta lähetetään eniten haitallista koodia käyttäjän tietokoneelle. Kalasteluviestit saapuvat yllättäen, joten niissä toimii nyrkkisääntönä: älä klikkaa, älä lataa. Kaksivaiheinen tunnistautuminen vähentää hyökkäyksen kohteeksi jäämisen. (Turvakäräjät -podcast 2021.)

Tietojenkalastelut ovat suunniteltu huijaamaan ihmisiä paljastamaan arkaluontoisia tietoja, kuten käyttäjätunnuksia tai salasanoja. Hyökkääjät osaavat luoda sähköpostiviestejä erilaisista aihepiireistä, kuten salasanojen vaihtamisesta tai tuottavuustyökaluista. Näiden tehtävänä on saada ihminen klikkaamaan linkkiä, sillä aihetta pidetään usein kiireellisenä. Hyökkäyksissä käytetyt kalastelusivut voivat toimia osana hyökkääjän ostamaa tai ylläpitämää valheellista verkkotunnusta, tai laillisen verkkosivun haavoittuvuutta on voitu hyötykäyttää haitalliseen isännöintiin. Tietojenkalastelusivustot ovat usein kopioita tunnettujen, kuten Googlen tai Office 365:n kaltaisten palveluiden aitoja kirjautumissivuja, jotta käyttäjät erehtyisivät syöttämään omat tunnistetietonsa verkkosivustolle. Kun tunnistetiedot ovat syötetty, käyttäjä ohjataan usein aidolle sivustolle, jonka takia käyttäjä ei osaa epäillä omien tunnistetietojen vaarantuneen. Syötetyt tunnistetiedot kuitenkin tallennetaan tai lähetetään hyökkääjälle myöhempää väärinkäyttöä varten. (Microsoft digitaalinen puolustus -raportti 2021, 21.)

Sähköpostia käytetään usein myös haittaohjelmien levittämiseen. Sähköpostiviestit saattavat sisältää haittaohjelmalinkin tai -liitteen, ja ne ovat usein päällekkäisiä viestejä tietojenkalasteluviestien kanssa. Sekä haittaohjelmien toimitukseen että tietojenkalastelua varten lähetetyt viestien linkit voivat johtaa siihen, että tietoturvateknikot eivät välttämättä havaitse huijausta. Haittaohjelmat eivät edellytä vuorovaikutusta käyttäjältä, joten niiden toimitus esimerkiksi sähköpostiin voidaan suunnitella pysymään käyttäjältä piilossa. Sähköpostin

liitteenä oleva dokumentti voi olla hämäystä, jolloin päätelaitteessa saattaa lähteä latautumaan haittaohjelma taustalla. Käyttäjä voi ajatella tiedoston olevan rikkinäinen tai, että se ei ollut tarkoitettu hänelle. Haittaohjelman käynnistymistä ei välttämättä huomata. Sähköpostin välityksellä jaetut haittaohjelmat muuttuvat kuitenkin säännöllisin väliajoin. Tämä johtuu haittaohjelmien poistamisesta tai hyökkääjien muuttuneiden tavoitteiden seurauksena. (Microsoft digitaalinen puolustus -raportti 2021, 22.)

Sähköpostin vaarantuminen on uhkakanava, koska lähes 70 prosenttia tietomurroista perustuu tietojenkalasteluun. Käyttämällä perustason tietoturvakäytäntöjä, voidaan estää tietomurtojen esiintyminen. Päivityksien suorittaminen, kaksivaiheinen todennus sekä asianmukaiset korjaustiedostot estävät tietomurtojen etenemisen. Organisaatio, joka ei noudata tai ylläpidä perustason käytäntöjä, altistuvat muita huomattavasti herkemmin hyökkäyksille. (Microsoft digitaalinen puolustus -raportti 2021, 89.)

3.4.4 Palvelunestohyökkäykset

Palvelunestohyökkäys tarkoittaa vahingollisen toimijan yritystä estää verkon tai palvelun käyttö häiritsemällä verkon toimintaa. Verkkoliikenne voidaan kuormittaa ylimääräisellä liikenteellä tai hyödyntää verkkolaitteessa olevaa haavoittuvuutta, mikä on seurausta toteutuneesta hyökkäyksestä. Suuri osa palvelunestohyökkäyksistä toteutuu hajautetulla järjestelmällä, jossa liikennettä lähetetään useasta eri lähteestä kuormittamaan kohdetta. Tämän taustalla on usein hyökkääjän hallitsema bottiverkko, joka koostuu useista IoT-laitteista, ja jotka ovat otettu haltuun hyökkäyskäyttöön laiteomistajien tietämättä. Kohdetta rasitetaan liian suurella liikennemäärällä tai kohteeseen lähetetään sellaista liikennettä, joka kuormittaa kohteen muisti- tai laskentaresursseja, jonka vuoksi kohdelaitteen käytön toiminta estyy. Sovellustasolla palvelunestohyökkäyksessä kohteeksi voidaan ottaa sovelluksen taustalla pyörivä tietokanta, jota voidaan rasittaa lähettämällä sinne suuria määriä kyselyitä. (Traficom: Toimintaohje–Palvelunestohyökkäys 2022, 2.)

Palvelunestohyökkäykset voidaan havaita esim. IDS[20]-ratkaisujen kautta. Tämän ratkaisun kautta havaitaan hyökkäykset ja sillä pyritään estämään

[20] IDS – Intrusion Detection System, hyökkäyksen havaitsemisjärjestelmä

hyökkäykset automaattisesti. (Traficom: Toimintaohje–Palvelunestohyökkäys 2022, 4.)

3.4.5 Teknisen tuen huijaukset ja Web-kameran käyttö

Tällä viitataan huijauspuheluihin, jossa henkilö saa soiton, usein heikolla englanninkielentaidon omaavalta soittajalta. Soittaja kertoo vastaajan tietokoneen olevan saastunut viruksesta. Ilmoitus tietokoneviruksesta on tullut soittajalle, joka ”työskentelee” Microsoft Windowsilla, ja soittaja on valmis sillä hetkellä auttamaan vastaajaa. Tämän jälkeen soittaja ”auttaa” poistamaan viruksen tietokoneesta luettelemalla numerosarjan, joka on usein sama kaikissa koneissa. Tämän jälkeen saadaan käyttöön etäkäyttöohjelma, jonka jälkeen vastaajan tili tyhjenee, kun kirjaudutaan pankkiin Internetin kautta. Puhelinnumero on usein väärennetty suomalaiseksi, koska ne voidaan toteuttaa ilman suurempaa panostusta. (Turvakäräjät -podcast 2021.)

Myös Web-kameroiden käyttö esimerkiksi aluksen ja varustamon välillä mahdollistaa uhkille. Kameroiden käyttö lisää riskiä, jossa tietokonekamera hakkeroidaan ja hyökkääjä näkee kameran takana näkyvät henkilöt, ja pääsee mahdollisesti käsiksi henkilöiden näytöllä jaettuun dataan tai henkilöllisyyteen. Kameran hakkerointi voi johtaa myös siihen, että sitä käytetään ns. Offline-tilassa, jolloin kukaan ei välttämättä ole kameran takana, mutta se tallentaa kuvamateriaalia esim. konevalvomosta hyökkääjän tilille. (Kaspersky s.a.).

3.5 Algoritmi

Kyseessä on koodi, joka antaa tietokoneelle listan sääntöjä ja ohjeita tietyn toiminnan suorittamiseen. Kehittyneemmät algoritmit voivat sisältää jopa miljoonia eri algoritmeja, jotka käyttävät menettelyssään koneoppimista. Algoritmi käyttäytyy kuten aivot: ne keräävät faktaa ja yhdistelevät sitä aiemmin opittuun sekä saavat palautetta tiedon soveltamisesta. Tunnetuimpia ovat erilaiset haku- ja suosittelualgoritmit. Niiden tarkoituksena on vastaanottaa tietoa ja muokata se hyödylliseen muotoon. Joka kerta, kun käyttäjä hyödyntää esimerkiksi Googlea tiedonhakuun, algoritmit pyörivät taustalla ja antavat personoituja suosituksia. Suositteluperiaate perustuu käyttäjästä löytyvän tiedon keräämiseen. (Riikonen 2022, 42.)

Osa sovelluksista on ahneita, että ne keräävät poikkeuksellisen paljon tietoa käyttäjästä. Sovellus saattaa etsiä tietoja yhdistetyistä sosiaalisen median palveluista, kolmansilta osapuolilta, muilta sovelluksen käyttäjiltä ja jopa puhelimesta. Se tallentaa tiedot, jotka käyttäjä on syöttänyt eri lomakkeisiin ja kerää tietoa mm. kommenteista, kuvista ja puhelimen kontakteista. Tällaiset sovellukset keräävät biomeristä dataa, kuten sormenjälkitietoja. Algoritmien avulla saadaan kerättyä käyttäjästä paljon tietoa, että käyttäjälle voidaan tarjota mittatilaustyönä käyttäjää kiinnostavaa dataa, kuten kissa- tai koiravideoita. Kerätyn datan loppusijoitusta ei sen sijaan kerrota. (Riikonen 2022, 43.)

Vaikka usein sivuutetaan riskit sosiaalisen median tai tietokoneen käytöstä, erilaiset kehittyneet palvelut mahdollistavat rikollisen toiminnan niissä. Palvelut mahdollistavat käyttäjän vainoamisen tai kiristämisen. Koska kuka tahansa voi ottaa julkisella paikalla toisesta kuvan, henkilön etsiminen palvelun kautta on mahdollista, jolloin kuva ja data voi joutua vääriin käsiin tai teknologiayritykset voivat tarjota tietojaan muille yhtiöille tai valtiolle. (Riikonen 2022, 43; Smith 2020).

3.6 IoT- ja OT-uhkaympäristö

IoT:n käyttöönotto sekä etäpalveluiden ripeä kasvu kotona että työpaikalla, lisäävät havainnollistamisen todennäköisyyttä, jonka seurauksena IoT-sovellukset yleistyvät kaikkialla. Alukset puolestaan ovat riippuvaisia OT-laitteistaan, joita käytetään erilaisiin säätöjärjestelmiin. Merkittävä osa OT-laitteista tulee kuitenkin jäljessä, mitä nykyaikaisten tietoturvallisuusstandardeihin käyttöönottoon ja hyödyntämiseen tulee. (Microsoft digitaalinen puolustus -raportti 2021, 70.)

Useimpien laitteiden perusta pohjautuu laiteohjelmistojen sekä ohjaimien taakse, jolloin niiden hakkerointi haittaohjelman upottamisella, aiheuttaa valtavan riskin laitteille ja sitä kautta organisaatiolle. Haittaohjelmat voivat tehdä laitteen käyttökelvottomaksi tai estää sen käynnistymisen. Organisaation tulisi varmistaa, että kaikkien palvelimiin tai loppukäyttäjien laitteisiin asennetut ohjelmistot ja ohjaimet täyttävät tietoturvavaatimukset, ja että niiden dokumentaatio on kunnossa. (Microsoft digitaalinen puolustus -raportti 2021, 74.)

IoT-ratkaisuissa yhdistyvät laitteistot, ohjelmistot sekä pilvipalvelut. Laitteet keräävät dataa ja sitä saadaan nopeasti ja tehokkaasti. Hyökkäykset ovat olleet kasvussa ja niiden vakavuus on herättänyt huomiota, jolloin hyökkäystulvan raadollisuus on lisännyt tietoa digitaalisen maailman kyberhyökkäyksien mahdollisuuksista vaikuttaa fyysiseen maailmaan. (Microsoft digitaalinen puolustus -raportti 2021, 76.)

Vanhan teknologian aiheuttamat uhkat eivät saa hidastaa nykyaikaisten digitaaliympäristön käyttöä, kun varmistetaan OT-järjestelmien käyttöä (Microsoft Digitaalinen puolustus -raportti 2021, 79). Spesiaalit hyökkäykset, jotka kohdistuvat suoraan OT-järjestelmiin, osoittavat näiden järjestelmien kiinnostavan erityisesti kyberrikollisia. Houkuttimena toimii *katkos* liiketoiminnalle (vienti–tuonti) tai ympäristövahinkojen ilmaantuminen. Merkittävänä osana on arvioida OT-järjestelmien tietoturva yhtä kattavasti kuin IT-järjestelmien tietoturva. Hyökkääjät osaavat valita vaivattomimman kohteen sisäänpääsyväyläkseen, jolloin kohdennetut tietojenkalastelu tai haittaohjelmahyökkäykset mahdollistavat pääsyn tietojärjestelmiin. Tämän jälkeen hyökkääjät voivat jatkaa toimintaansa OT-järjestelmiin. (Microsoft digitaalinen puolustus -raportti 2021, 83.)

3.7 Vaaratekijät

Vaaran aiheuttajat kyberturvallisuuden ja inhimillisen tekijän näkökulmasta voidaan määritellä listamuodossa. Uhkan vakavuus ja kehittyneisyys määräytyvät esimerkiksi yksilön kykyjen mukaan. Alla olevasta listasta käy ilmi mahdolliset vaaratekijät, jotka voivat olla kiinnostuneita laivajärjestelmistä:

- Välinpitämätön, huolimaton tai tietämätön työntekijä tai urakoitsija, joka ei välttämättä noudata hyväksyttyä toimintaa tai muita turvallisuuskäytäntöjä. Henkilö voi vaarantaa järjestelmän turvallisuuden virheen tai laiminlyönnin vuoksi.

- Tahattomat henkilöt, joiden tavoitteena ei ole järjestelmien tai tietojen vahingoittaminen, mutta voivat päästä niihin käsiksi ilman omistajan lupaa ja voivat aiheuttaa vahingossa vahinkoa. Tällaisten henkilöiden motiivina on yleensä tutkia järjestelmien heikkouksia ja haavoittuvuuksia.

- Tyytymätön työntekijä tai urakoitsija, jolla on rajalliset IT-taidot ja joiden motivaatiot vaihtelevat: tarkoituksena voi olla arkaluontoisten tietojen varastaminen tai niiden vuotaminen, aluksen toiminnan sabotointi tai häirintä. Vahingon määrä riippuu heidän roolistaan, järjestelmän

käyttöoikeuksista sekä aluksen järjestelmiin ja tietoihin liittyvien kyberturvatoimien tehokkuudesta.

- Tyytymätön työntekijä tai urakoitsija, jolla on merkittävät IT-taidot, mukaan lukien järjestelmävalvojat, joilla on mahdollisesti laajat käyttöoikeudet. Kyseiset henkilöt saattavat aiheuttaa huomattavaa vahinkoa varsinkin, jos heillä on käyttöoikeudet järjestelmänvalvojan oikeuksiin. Henkilöillä saattaa olla riittävästi tietoa ja kykyä ohittaa hallinta- ja suojatoimenpiteet ja he voivat olla taitavia poistamaan todisteita omista toimistaan, kuten muokkaamaan tai poistamaan merkintöjä järjestelmälokeista. Arkaluonteisissa rooleissa on harkittava organisaatiosta lähtevien tyytymättömien henkilöiden jatkotoimenpiteisiin, mikä perustuu sosiaalisen median syötteiden riskien arviointiin ja sen seurantaan.

- Merenkulusta kiinnostuneet henkilöt, jotka toimivat yksittäisinä hakkereina sekä kantavat rajallisesti tietoa että käyttävät muiden henkilöiden suunnittelemia ja kehittämiä työkaluja. Hakkerointi- ja palvelunestotyökalujen helppo saatavuus Internetistä tarkoittaa, että hyökkäyksen käynnistämiseen vaadittava tekninen ymmärrys on laskenut merkittävästi.

- Kybervandaalit, jotka ovat omaksuneet merenkulun tietoliikenteen- ja järjestelmät, voivat olla hyvin asiantuntevia, jolloin he saattavat kehittää tai laajentaa omia työkalujaan. Heidän motiivinsa eivät ole taloudellisia eivätkä ideologisia: he hakkeroivat tai kehittävät haittaohjelmia, koska heillä on potentiaalia suorittaa se. Esimerkiksi verkkosivuston turmeleminen tai murtautuminen palvelimelle tapahtuu käyttäjätunnuksia varastamalla, jotka myöhemmin voidaan julkaista julkisella verkkosivustolla, ovat heille ominaista. Tällä he haluavat osoittaa kykynsä.

- Merenkulkuorganisaation ulkopuolella työskentelevät erakot, jotka hallitsevat pitkälle kehittyneen teknisen tietämyksen. Ryhmä voi olla taitava poistamaan todisteita omista toimistaan: esimerkiksi muuttamaan tai poistamaan merkintöjä järjestelmälokeista. Heillä on myös todennäköisesti kykyä ohittaa valvonta- ja suojatoimenpiteet. (Boyes ym. 2017, 34.)

Vuonna 2017 Kaspersky Labin ja B2B Internationalin teettämässä tutkimuksessa selvisi, että 57 prosenttia yrityksistä (5000 eri yritystä mukana) olettaa heidän tietoturvansa olevan vaarassa, ja 52 prosenttia tutkimuksen yrityksistä myönsi, että työntekijät ovat suurin kyberturvallisuusuhka. Työntekijöiden huolimattomuus johtaa turvallisuusriskeihin. Yritykset ovat tietoisia, kuinka helposti työntekijän käytös tai inhimillinen erehdys vaikuttaa turvallisuuteen. (Kaspersky Daily 2017.)

Tutkimuksen mukaan yrityksiä huolettaa eniten työntekijöiden mobiililaitteiden käyttö, koska niiden kautta voidaan lähettää arkaluonteista tietoa tai

työntekijät saattavat käyttää sopimattomasti IT-resursseja. Henkilöstön pieni määrä saattaa lisätä joustavuutta siinä suhteessa, missä yritys jakaa työntekijöilleen IT-resursseja. Tutkimuksessa havaittiin myös, että työntekijät saattavat tehdä huolimattomuudessaan virheitä, tai sen takia, ettei heillä ollut riittävää tietoturvakoulutusta. (Kaspersky Daily 2017.)

Tietomurron sattuessa jopa 40 prosenttia työntekijöistä yrittävät piilottaa tapahtuman, eivätkä he välttämättä ota vastuuta tapauksesta. Usein työntekijät ovat koittaneet peitellä jälkiään tietovuodon sattumisen jälkeen. Tietovuodon peittämisellä voi olla laajamittaisia vaikutuksia, jotka usein pahentavat tietovuodon aiheuttamia vahinkoja. Tietovuodon havaitseminen tarpeeksi ajoissa edesauttaa tutkintaa. (Kaspersky Daily 2017.)

3.8 Kyberhygienia

Kyberhyökkäyksiltä voidaan suojautua 98 prosenttisesti, kun käytössä on perustason tietoturva. Ensimmäiseksi tulisi olla käytössä MFA[21], joka vaikeuttaa varastettujen tai kalasteltujen valtuustietojen käyttöä. Valtuutus ja todennus suoritetaan aina kaikkiin saatavilla oleviin datapisteisiin: käyttäjätiedot, sijainti, laitteen kunto, palvelu tai työkuorma, tietojen luokittelu ja poikkeavuudet, lukeutuvat näihin kohteisiin. MFA voi nimittäin jo alkumetreillä pysäyttää tunnistetietoihin perustuvan hyökkäyksen, koska ilman pääsyä hyökkääjä ei pääse käsiksi esim. tiliin tai suojattuun resurssiin. (Microsoft digitaalinen puolustus -raportti 2021, 124–126.)

Käytössä tulisi olla myös periaate, joka rajoittaa työntekijöiden mahdollisuuksia liikkua verkossa. Tämä rajoittaisi siis työntekijöiden käyttöoikeuksia laitteissa. Nämä teknologiat, jotka perustuvat riskinarvioinnin mukautuviin käytäntöihin sekä tietojen varmistuksen avulla, suojaavat tietoja ja tuottavuutta. (Microsoft digitaalinen puolustus -raportti 2021, 124–126.)

Kun organisaation laitteet ja sovellukset ovat ajan tasalla ja ne ovat oikein määritettyjä, vähenevät haavoittuvuuden riskit. Jotta järjestelmät käyttävät uusimpia versioita ja ne ovat määritetty oikein, mahdollistaa päätepisteiden

[21] Multi Factor Authentication – monivaiheinen todennus kirjauduttaessa tietokoneelle tai IoT-laitteelle.

hallintaratkaisut käytäntöjen lähetyksen esim. Push-syötteenä koneisiin. Olennainen osa kyberhygieniaa on laitteiden pito ajan tasalla ja niiden konfigurointi. Lisäksi käytetään myös päätepisteiden hallintaohjelmia ja varmistetaan niiden uusin käyttöversio. Jotta voidaan päivittää OT-järjestelmiä, on tehtävä kattava järjestelmäkartoitus. Tämän jälkeen voidaan ymmärtää, mitkä laitteistot ovat käytössä ja kuinka alttiina ne ovat tietynlaisille hyökkäyksille. (Microsoft digitaalinen puolustus -raportti 2021, 124–126.)

Jotta säästytään haittaohjelmilta päätepisteissä ja laitteissa, voidaan asentaa haittaohjelmien torjuntapalvelu. Lisäksi voidaan hyödyntää pilvipalveluiden haittaohjelmien torjuntapalveluita, koska ne ovat usein uusimpia ja tarkimpia. Tämä pitää sisällään myös OT- ja IoT-ympäristöt. Kaikissa pilvipalvelujärjestelmissä – virtuaalikoneista aina sovelluksiin – tulisi ottaa käyttöön työkuormasuojaus. (Microsoft digitaalinen puolustus -raportti 2021, 124–126.)

Datan turvaaminen vaatii sen, että tiedetään, mihin tiedot on tallennettu ja kenellä kaikilla on niihin käyttöoikeus. Mahdollisuuksien lomassa tietojen menetyksen estokäytännöt sekä arkaluonteisuusmerkinnät varmistavat käytäntöjä. Jos tietomurto tapahtuu, on tietoturvatiimin tiedettävä missä arkaluonteisimmat tiedot säilytetään ja missä niitä käytetään. Arkaluonteisen datan hallussapito organisaatiossa varmistaa niiden asianmukaiset toimenpiteet datan suojaamiseksi. Lisäksi organisaatioiden ymmärrys, mikä on arkaluonteista ja mikä ei, ja mihin saattaa kohdistua säädöksiä siirtyessä yhteistyökeskeisempää maailmaa: varmistus ja ymmärrys, mitä dataa on hallussa, ja miten se luokitellaan tarkasti sekä kuinka arkaluonteisuustunnisteita sovelletaan asianmukaisesti. Tällaiset käytännöt antavat valmiuksia hyödyntää tietoturvateknologioita. (Microsoft digitaalinen puolustus -raportti 2021, 124–126.)

Henkilöstön kouluttaminen ja omistautuneen työntekijän saaminen mukaan turvallisuuspolitiikkaan, vähentää työntekijän huolimattomuutta ja lisää motivaatiota kiinnittämään huomiota kyberturvaan. Tietoturvakoulutukset auttavat työntekijöitä ymmärtämään tietoturva-asioita paremmin. Pelkkä turvallisuuspolitiikan olemassaolo ei riitä, vaan on löydettävä tasapaino sitoutumisen ja turvallisuusajattelun välille. Päivitysten asentaminen, haittaohjelmasuojauksen varmistaminen ja henkilökohtaisten salasanojen tulisi olla rutiinia ja niitä tulisi

tarkkailla säännöllisin väliajoin. Kouluttaminen takaa myös sen, että työntekijä osaa toimia oikein, jos kyberhyökkäys tapahtuu. (Kaspersky Daily 2017.)

4 INHIMILLINEN TEKIJÄ

Turvallisuuden tunne lisääntyy, kun mahdollisimman moni asia sujuu ongelmitta. Turvallisuuden ylläpitämiseksi vaaditaan onnistumisia, ja sitä, että tapahtumia voidaan ennakoida ja tunnistaa. Ennakoivalla tavalla hyväksytään, että ihmisen toiminnassa ja suorituskyvyssä on vaihtelua ihmisten välillä. Tämän kautta voidaan luoda uusia tapoja toimia, välttyä virheiltä, lieventää seurauksia tai kompensoida puuttuvia resursseja. Näin varmistetaan työn sujuminen onnistuneena. Kun ihmiset nähdään voimavaroina, eikä ”heikoimpana lenkkinä”, järjestelmiin saadaan joustavuutta ja sietokykyä muuttuvissa tilanteissa (HF Tool™ 2022.) Jotta voidaan ymmärtää ihmisen käyttäytymistä erilaisissa työtilanteissa ja -ympäristössä, on ymmärrettävä, mitkä tekijät ajavat ihmiset näihin tilanteisiin. Pelkkä ulkopuolinen tarkastelu ei riitä, vaan pitää nähdä pintaa syvemmälle.

4.1 Ihminen ja digitalisaatio

Tapaturman tai ”läheltä piti” -tilanteen jälkeen usein ihmetellään, miten näin pääsi käymään. Usein tekniset ja uudet laitteet sekä järjestelmät, ovat tehokkaampia, nopeampia ja monimutkaisempia toimintatavoiltaan, mikä taas aiheuttaa sen, että ne ovat alttiimpia violle. Koska työelämä muuttuu jatkuvasti ja tieto vanhenee nopeasti, tulee työntekijöiden osaamista päivittää säännöllisesti. (ISSA 2017, 4,16.)

Teknologia ja digitalisaatio antavat uusia mahdollisuuksia työn organisointiin ja prosessien toteuttamiseen. Työ on hyvin verkottunutta, ja lähes jokainen vaikuttaa työssään useaan eri prosessiin erilaisten tietojärjestelmien ja työvaiheiden kautta. Koska pienet muutokset prosessissa voivat muuttaa koko prosessia, on tärkeää, että jokaisella on hyvä kokonaisnäkemys työstä ja sen toimintaperiaatteesta. Tietämys eri tekijöiden välisistä vuorovaikutuksista, syy-seuraussuhteista, välittömistä seurauksista, ja aikaa vievistä vaikutuksista, katsotaan jokaisen työntekijän eduksi. Aluksia on rakennettu ja niitä on ylläpidetty jopa vuosikymmenten ajan, jonka vuoksi uusia järjestelmiä ja erilaisia laite- ja osajärjestelmiä on tullut osaksi alusten toimintaa, ja ne edustavat eri-

ikäisiä teknologia ratkaisuja. Tästä seuraa, että työntekijöiden on hallittava sekä uudet että vanhemmat teknologiat. Työntekijät ikääntyvät ja jäävät eläkkeelle tai vaihtavat työpaikkaa, joten uusien työntekijöiden palkkaaminen ja huolellinen perehdyttäminen vaativaan tekniseen ja automatisoituun ympäristöön, on tärkeää. (Ala-Laurinaho ym. 2022, 6–7.)

Energia-alan turvallisuusasiantuntijan haastattelussa nousi esiin esimerkiksi se, että yksi merkittävimmistä inhimillisistä syistä vaaratilanteiden taustalla liittyy organisaation kykyyn oppia virheistä ja onnistumisista. Vaaratilanteiden tausta tulisi selvittää perusteellisesti ja tämän takia tulisi määritellä toimivat toimenpiteet asian korjaamiseksi. Vaaratilanteita aiheuttaa jatkuva kiire ja ripeä aikataulu, jolloin ihmisen työkapasiteetti venytetään äärimmilleen.

Lisääntynyt informaatiotulva vaikuttaa ihmisen tarkkaavaisuuteen ja yksityiskohtien havaitsemiseen. Laadukkaampaa työtä vaaditaan pienemmillä resursseilla, jonka seurauksena työsuhteen pituus lyhenee, mikä luo omalta osaltaan haasteita perehdytyksen laatuun. Ihmiset haluavat vaihtaa työpaikkoja useammin kuin aikaisemmin, mikä taas johtaa muuttuvaan työympäristöön ja uuteen perehdyttämiseen. Ikävään tilanteeseen joudutaan, kun organisaation ohjeista lipsutaan. Tämän seurauksena voi syntyä ajatusmalli, että tällä tavalla täällä toimitaan. Loppujen lopuksi ohjeita noudattaa vain harvat, ellei organisaatio itse pysty välittömästi vaikuttamaan tilanteeseen ja muuttamaan omaa toimintaa. (Energia-alan turvallisuusasiantuntija 2022.)

4.2 Näkökulmana turvallisuuden kehitys

Arkirealismi toteutuu usein työpaikalla, kun ajatellaan yksilö jo alun perin virhelähtöisesti eikä niinkään virheistä oppijana. Inhimilliset tekijät kuitenkin voivat joko tukea tai heikentää työjärjestelmän toimivuutta ja palveluiden turvallisuutta. Yksilön, ryhmän tai organisaation vaikutus työn piiriin on havaittavissa, mikä ilmenee työterveyslaitoksen HF Tool™ -koulutuksessa. Inhimillinen tekijä tarkoittaa eri asiaa kuin inhimillinen virhe, koska inhimillinen tekijä nähdään uudenlaisena tapana toteuttaa asioita, jolloin sen tarkoituksena on *kehittää turvallisuutta.* Ennakoiva tapa, jossa tunnistetaan riskit, vähentävät tutkitusti vaaratilanteiden syntyä. Tärkeää olisi tunnistaa ja ennakoida inhimilliset tekijät työn aikana, työpaikalla ja kollegoiden kesken. Lisäksi niiden raportoiminen

mahdollistaa tiedon kulkemisen johtoportaalle saakka, jolloin asioihin voidaan kiinnittää paremmin huomiota. Inhimillisten tekijöiden tutkiminen ja analysoiminen poikkeamissa, onnistumisissa sekä normaalitoiminnassa, avartavat turvallisuuden näkökantaa. (HF Tool™ 2022.)

Energia-alan turvallisuusasiantuntijan mukaan, töihin tulisi valmistautua päivittäin, jolloin siitä syntyisi rutiinia, joka taas vähentäisi inhimillistä riskiä. Kaikilla työntekijöillä tulisi olla yhdenmukaiset työkalut inhimillisten tekijöiden hallintaan, ja työntekijöitä tulisi kouluttaa säännöllisesti niiden käyttöön. Esimiesten ja johdon tulisi kannustaa työntekijöitä tällaiseen varmentavaan työskentelytapaan, jossa parityöskentely ja tarpeeksi selkeä viestintä, parantavat työstä suoriutumista. Työntekijöille tulisi tarjota riittävä osaaminen työpaikalla ja heidän osaamisestaan tulisi huolehtia. Inhimillisiä tekijöitä tukevat työkäytännöt, kuten aloituspalaverit tai briiffaukset sekä lopetuspalaverien käyttö, pitäisivät olla päivittäisiä rutiineja. Niitä käyttämällä tarkkavaisuus lisääntyy ja ammattiylpeys kohoaa. *Inhimillisten tekijöiden hallinnan tulisi olla osa työkäytäntöä ja jokapäiväistä tekemistä turvallisuuskriittisillä toimialoilla.* Muistinvaraan inhimillisten tekijöiden hallintaa ei voida rakentaa.

Ihmisen käyttäytymiseen työympäristössä voidaan vaikuttaa myönteisesti hyvällä esimiestyöllä ja johtamisella. Näin varmistetaan riittävät resurssit töiden tekemiseen ja laatuun. Työyhteisössä riittävä avoimuus ja luottamus muita työntekijöitä kohtaan vaikuttavat psykologisen turvallisuuden tuntuun: voidaan luottaa kollegan apuun. Huolehtimalla työntekijän motivaatiosta, työssä jaksamisesta sekä työhyvinvoinnista varmistutaan, että työntekijä pystyy suoriutumaan hänelle asetetuista työtehtävistä. Kun kaikkia työntekijöitä kuunnellaan ja annetaan mahdollisuus vaikuttaa omaan työhönsä, pystytään vaikuttamaan työntekijän oman toiminnan parantamiseen työpaikalla. Toistensa tunteminen on turvallisuustekijä. (Energia-alan turvallisuusasiantuntija 2022.)

4.3 Yksilön toiminta ja sen piirteet

Jokainen ihminen toimii omassa työssään ja työtilanteissa parhaimmalla mahdollisella tavallaan tai sen hetkisen kykynsä mukaan. Koska ihmisen toiminta on monien tilanteiden ja opittujen mallien summa, on mahdolliset riskitekijät

jatkuvasti läsnä. Vaihtelevilla inhimilliset tekijät -koulutuksilla voidaan varmistaa onnistuminen työskenneltäessä.

4.3.1 Tarkkaavaisuus

Keskeisenä vaatimuksena työtä tehdessä voidaan pitää tilannetietoutta: tarkkaavaisuutta, havainnointia, muistia, päätöksentekoa sekä reagointia. Jokaisessa työssä vaaditaan perustaitoja sekä erikoistaitoja, ja näiden pohjalta syntyy oman osaamisen tunnistaminen. Ihmisen tulisi tietää omat vahvuudet ja heikkoudet. Menetelmien ja ohjeiden oikea noudattaminen johtaa työn ja toiminnan oikeaan suorittamiseen. Tämän takia on keskeistä huomata, onko tilannetietous ollut ajan tasalla, ja ymmärtääkö henkilö ympärillä tapahtuvista asioista. Voidaan pohtia, onko häiriötilanteet otettu huomioon. (HF Tool™ 2022.)

Esimerkiksi aluksen konekorjaaja on aloittamassa sorvaamaan uutta akselia pienelle keskipakopumpulle. Konekorjaaja tarkistaa sorvauspaikan olevan siisti, varmistaa laitteen säädöt oikeiksi ja laittaa karan suojan eteen sekä huomioi muut verstaalla olijat, ettei metallikappaleita lennä toisia kohti, ja laittaa katosta roikkuvan hitsausverhon eteen. Hän laittaa suojalasit päähänsä sekä käyttää pitkähihaista työpaitaa ja -housuja, turvakenkiä ja hanskoja. Konekorjaaja ottaa huomioon merenkäynnistä johtuvan aallokon. Tämän jälkeen hän vielä varmistaa metallikappaleen olevan oikea ja ryhtyy sorvaamaan. Tilanteessa konekorjaaja *ottaa vastuun omasta työstään turvallisesti,* ja varmistaa, ettei hänen takiaan synny turhia riskejä.

Trial Error on tilanne, jossa koetaan oppiminen haasteellisuuden takia stressaavaksi. Tapahtuman seurauksena kokeillaan esimerkiksi uuden tietokonejärjestelmän käyttöä ja toimivuutta useaan kertaan, jolloin epäonnistuneen napin painalluksen jälkeen yritetään uudestaan ja yhä uudestaan, kunnes toivottu tapahtuma onnistuu ja oppiminen on saavutettu useiden virheellisten tai kyseenalaisten toimintojen kautta (HF Tool™ 2022.) Henkilö kokee tehtävässä onnistuneensa, vaikka virheiden mahdollisuus kasvoi jokaisen yrityksen jälkeen.

4.3.2 Representaatio

Kokonaistilanteen ymmärtämisen taustalla vaikuttaa vahvasti representaatio ja ihmisen sisäinen malli maailmasta. Taustalla tässä on ”big picture”, jonka pohjalta ennakoidaan, ymmärretään ja selitetään ympäristön piirteitä. Malli on usein epätarkka ja puutteellinen, mikä saattaa johtaa virhearviointeihin. (HF Tool™ 2022.)

Esimerkkitilanteessa aluksen konemestari perehdyttää alukselle saapuvaa moottorimiestä kyberturvallisuusasioissa. Konemestari on näyttänyt, kuinka aluksen tietokoneita saa käyttää. Moottorimies rakentaa opitusta järjestelmästä kuvan mieleensä aluksen tietokoneiden käytöstä, ja muistelee, kuinka tämä tapahtuu. Syntyy mielikuva tietokoneen käytöstä aluksella, johon yhdistetään jo aiemmin opittua tietoa. Uusi tieto suhteutetaan aikaisempaan tietoon ja järjestetään osaksi tietoperustaa. Kun moottorimies oppii uutta, hän pyrkii jatkuvasti suhteuttamaan havaittua informaatiota aikaisempaan kokemukseen. Moottorimiehen oppimisen pohjana toimii tieto, joka ohjaa toimintaa. Kun moottorimies haluaa oppia lisää aluksen kyberturvallisuudesta, hän lukee ja pohtii lukemaansa, ja huomaa asian olevan tuttua. Tämän havainnon perusteella, hän saattaa hypätä asian yli ja jatkaa lukemista, mikä voisi johtaa väärään käsitykseen aiheesta, vaikka luuli tietävänsä asian. Seurauksena tästä, hän todennäköisesti lukee asian uudelleen ja pyrkii ymmärtämään asian oikein sekä pyrkii selvittämään, miksi aikaisempi käsitys oli väärä.

4.3.3 Riskien arviointi ja oletus

Ennakoiva työote, jossa keskeisessä roolissa varmentava työskentelymalli, madaltavat työssä havaittavaa inhimillistä riskiä. Ennen työn aloittamista tulisi työhön liittyvät riskit tai vaarat arvioida ja prosessoida. Oikeanlaisella riskienarvioinnilla vältytään vahingoilta. (HF Tool™ 2022.)

Esimerkiksi aluksen konemestarilla on vahva käsitys, kuinka tietokoneen ruudulle ilmestyvää epämääräistä linkkiä tulisi käsitellä, ja tämän seurauksena sivuuttaa konepäällikön ohjeistuksen ja tekee oman ratkaisun oletuksen pohjalta, jolloin voi syntyä kyberturvallisuusriski. Oletusta käytetään oman epävarmuuden tai huolestuneisuuden vähentämiseen. Toiminta on oman oletuksen kautta niin vahva, että autenttinen informaatio jätetään huomiotta, koska

toiselta saatu ohjeistus on ristiriidassa oman olettamuksen kanssa. Myöhemmin ihmetellään, mikä meni väärin.

4.3.4 Työkuorma ja vigilanssi

Työkuorman jakautuneisuus kahteen ääripäähän (liian paljon informaatiota tai liian yksinkertaisia tehtäviä), vaikuttavat työntekijän suoritustasoon (HF Tool™ 2022). Tämä voi johtaa tilanteisiin, jossa henkilö joko esimerkiksi turhautuu tai stressaantuu.

Jos konemestari saa laivaa käynnistettäessä liian paljon ympäriltä informaatiota, kuten moottorimiehen antamia tilanneraportteja tietokoneella tapahtuvasta haittaohjelman aiheuttamasta ongelmasta tai pääkoneiden kierroslukujen heittelemisestä näytöllä, toimii konemestari suoritustason äärirajoilla. Tämä lisää tilannekohtaisen ja tehtävän aiheuttamaa kuormitusta hetkellisesti, mutta voi pitkällä aika välillä johtaa stressiin. Toisena ääripäänä työkuormaa voidaan pitää esimerkkiä, jossa moottorimies ei ole saanut pyynnöistään huolimatta konemestarilta muita töitä kuin verstaan luuttuamisen. Moottorimies turhautuu työhön, koska se ei välttämättä lisää mielenkiintoa päivärutiiniin. Sopiva vigilanssi työtehtävässä parantaa työn laatua ja mielekkyyttä tehdä työtä.

4.3.5 Väsymyksen vaikutus ja yleisen stressitaso

Väsymyksellä on suuria vaikutuksia työn tekemiseen ja siitä selviytymiseen. Väsyneenä ihmisen reagointiaika pitenee, jolloin ajoitusongelmia saattaa esiintyä. Usein myös huomioherkkyys alenee tai asioita jää huomaamatta. Muisti heikkenee ja keskittymiskykyä voi olla haastavaa hallita. (HF Tool™ 2022.)

Esimerkiksi konemestari on joutunut kollegoiden pitkittyneiden sairauslomien takia tekemään sekä 1.konemestarin että konekorjaajan töitä, jolloin yhtämittaista työjaksoa on kertynyt yli kahdeksan viikkoa. Konemestari on saanut keskimäärin unta viisi tuntia vuorokaudessa. Pitkittyneen univajeen seurauksena, konemestari ei ole huomannut ajoissa konevalvomon tietokoneella ilmanvaihtojärjestelmän sovelluksen ilmoituksia, jotka ovat seurausta sovelluksen hakkeroinnista. Myöhemmin tämän huomattuaan, konemestari kokee tilanteen erittäin stressaavaksi, kun ei pysty hoitamaan sekä häiriötilannetta

konehuoneessa että sovelluksen purkua, ettei siitä koituisi vahinkoa alukselle tai muulle miehistölle. Konemestarin mieltä vaivaa myös tapahtumahetkellä ennen työjakson aloittamista tapahtunut elämänmuutos, joka on lisännyt hänessä aggressiivisuuden määrää. Vihaisena, turhautuneena ja väsyneenä, konemestari käyttäytyy ikävästi alaisiaan kohtaan.

Jotta voitaisiin välttää tällaisten tilanteiden syntymistä, olisi konemestarin ollut tärkeää mainita ennen töihin lähtöä elämänmuutoksestaan aluksen päällikölle, ja päällikön suhtauduttava asiaan avoimesti ja huomioon ottaen. Väsyneenä ja stressaantuneena ihminen ei pysty työskentelemään täydellä kapasiteetillaan varsinkaan, että saisi hoidettua oman työnsä turvallisesti ja laadukkaasti loppuun. Väsymykseen ei auta muu kuin lepo, joten tässä tilanteessa päällikön olisi ollut tarpeellista lisätä resursseja aluksella ja päästää konemestari nukkumaan. (HF Tool™ 2022). Mahdollisuuksien salliessa, konemestari voisi erittäin stressaavan tilanteen hallintaan kokeilla asioiden listaamista paperille, ja priorisoida meneillään olevia töitä. Kun yksi työ on saatu tehtyä, se yliviivataan paperista, jonka jälkeen voidaan keskittyä seuraavaan asiaan (Energia-alan turvallisuusasiantuntija 2022). Tämän seurauksena konemestari voi tuntea asioiden olevan hallinnassa. (HF Tool™ 2022).

Pitkällä aikavälillä konemestari saattaa saada fyysisiä oireita, kuten sydämentykytyksiä tai lihaskramppeja, jos tilannetta ei pystytä purkamaan ja väsymys kestää liian kauan. Tilanne saattaa kärjistyä liian pitkälle, jos muutoksia työpaikalla ei tapahdu ja konemestarin on jäätävä pois töistä pitkälle sairaslomalle.

4.3.6 Motivaatio ja asenteet

Motivaatio ja asenteet vaikuttavat työn aloittamiseen, sen tekemiseen ja siitä suoriutumiseen, ja niihin viitataan usein joko myönteisenä tai kielteisenä suhtautumistapana. Motivaatioon ja asenteisiin voidaan vaikuttaa esimerkiksi lisäämällä työntekijän tietoa ja taitoa erilaisilla kursseilla tai palkinnoilla. Mahdollisia riskialttiita asenteita kuitenkin havaitaan usein työympäristössä. (Energia-alan turvallisuusasiantuntija 2022.)

Energia-alan turvallisuusasiantuntijan mukaan liiallinen itsevarmuus saattaa vähentää asioiden varmistamista muilta kollegoilta, jolloin esimerkiksi kyberturvallisuusasioissa henkilö ei kysy neuvoa, vaan toimii niin kuin hän parhaaksi näkee. Virheen mahdollisuus kasvaa, kun ego ei anna periksi. Yksi keino välttää tällaisen tilanteen kärjistyminen, on vaatia kaikilta työntekijöiltä yhdenmukaisen työkäytäntöjen noudattamista työpaikalla. Kokeneilla työntekijöillä voi myös olla tapana olettaa asioita, jos heillä on useiden vuosien työkokemus tehtävästä. Riskinä tässä on se, että päivitetyt säännöt jätetään huomiotta ja jatketaan työn tekemistä samoilla säännöillä kuin ne on tehty jo 20 vuotta. Johtamisen merkitys korostuu näissä tilanteissa.

HF Tool™ -koulutuksen pohjalta nousi esiin seuraavanlaisia skenaariota: Auktoriteetti-vastainen asenne voi johtaa siihen, että esimerkiksi moottorimies ei suostu ottamaan vastaan konemestarin ohjeita, vaan toimii oman kokemuksen pohjalta. Auktoriteetti-vastainen moottorimies ei hyväksy korkeammassa asemassa olevan konemestarin neuvoja ja saattaa ennen ohjeiden antamista lähteä tilanteesta pois. Vahva auktoriteetti vaikuttaa toimintaan.

Machoasenteen omaava ”alistaa” heikommassa asemassa olevia tai nuorempia henkilöitä. Machoasenne ei kysele, vaan suorittaa piittaamatta muiden mielipiteistä tai ehdotuksista. Vetäytymisen asenteella esimerkiksi konekorjaaja, ei usko omaan suoritukseen tai kykyyn saada hänelle määrättyä työtä tehtyä oikein. Hän epäilee, ja on valmiina ottamaan negatiivisen palautteen vastaan. Toisinaan hän saattaa vetäytyä kokonaan työnteosta siinä pelossa, ettei hänen osaamisensa ole riittävällä tasolla. Vetäytyvä ei koe välttämättä olevansa hyvä työntekijä, mikä voi johtua vähäisestä työkokemuksesta tai luottamuksesta itseensä. (HF Tool™ 2022.)

4.3.7 Tunnereaktiot

Pohjautuen HF Tool™ -koulutukseen voidaan nostaa esiin tilanteita, jossa tunnereaktiot ovat pääasiassa. Tunteet nousevat esiin erilaisten tapahtumien tai kanssakäymisten seurauksena, ja tunnereaktiot ovat seurausta mielialasta. Mielialaan taas voi vaikuttaa mm. työilmapiiri, uni, ihmissuhteet tai sää.

Esimerkiksi konemestari on uusi aluksella ja hän on saanut kahden päivän perehdytyksen konepäälliköltä sekä 1.konemestarilta. Konepäällikkö ilmoittaa konemestarille ennen työvuoron alkua, että konemestarin täytyy suorittaa kyberturvallisuuskoulutus työpäivän aikana. Konemestari ei ole joutunut suorittamaan tällaista koulutusta aikaisemmin, vaikka onkin työskennellyt tietokoneiden kanssa. Konemestari aloittaa koulutuksen tekemisen, mutta pelkää, ettei läpäise koulutusta. Koulutus on konemestarin mielestä haastava, eikä jännitykseltään läpäise sitä. Konemestari kertoo konepäällikölle koulutuksen tuloksen, eikä konepäällikkö ole tyytyväinen. Konemestari saa nuhteet konepäälliköltä, mutta saa yrittää koulutusta seuraavana päivänä uudelleen. Konemestari päättää viivytellä koulutuksen tekemistä vielä muutamalla päivällä, jotta ehtisi valmistautua siihen paremmin. Konepäällikkö kysyy koulutuksen suorituksesta, mutta konemestari vetoaa kiireeseen muissa töissä. Konepäällikkö hermostuu asiasta, ja tämä saa konemestarin pelkäämään konepäällikön reaktioita. Tämän takia konemestari ryhtyy pakoilemaan konepäällikköä, ja säikähtää joka kerta, kun näkee konepäällikön konevalvomossa.

Tilanteessa konemestari olisi voinut kysyä neuvoa muilta koulutuksen suorittaneita, tai ilmoittaa jo ensimmäisellä kerralla konepäällikölle, ettei ole suorittanut mitään vastaavanlaista koulutusta. Konepäällikön olisi myös ollut hyvä kysyä, onko uusi konemestari suorittanut mitään vastaavanlaista koulutusta. Pitkään jatkuneessa samankaltaisessa tilanteessa, konemestarista saattaa tulla säikähdysherkkä tai hän saattaa ryhtyä ylireagoimaan kaiken, mitä konepäällikkö konemestarille sanoo. Tämä taas voi johtaa virhearviointeihin.

Konepäällikön ja konemestarin on tärkeää tuntea alaisensa sillä tavalla, että he voivat muodostaa käsityksen työntekijän vahvuuksista ja kehityskohteista. Psykologinen turvallisuus korostuu näissä tilanteissa. Konepäällikön on tärkeää rakentaa konemiehistöstä toisiaan tukeva tiimi, jossa miehistö luottaa toisiinsa ja uskaltaa epäonnistua joutumatta negatiivisen kohtelun kohteeksi. Epäonnistuminen on miehistölle mahdollisuus oppia uutta ja auttaa menestymään jatkossa. (Energia-alan turvallisuusasiantuntija 2022.)

4.3.8 Sääntöjen noudattaminen

Energia-alan turvallisuusasiantuntijan mukaan lähtökohtana voidaan pitää sitä, että työpaikan sääntöjä noudatetaan. Sääntöjen käytöstä tulee rakentaa asia, mikä muodostuu osaksi jokaisen työntekijän ammattilaisuutta. Sääntöjen ja ohjeiden jatkuva kehittäminen ja ylläpito vaatii resursseja, mutta palkitsee lopulta. Tämän seurauksena organisaatio on saatava tilaan, jossa sääntöjä ja ohjeita kunnioitetaan aidosti. Jos kuitenkin ohjeet sivuutetaan, taustalla voidaan arvioida yksilön tai organisaation toimintaa. Yksilötasolla voidaan pohtia, onko työntekijä tietoinen noudattamatta jättämisestä, vai onko henkilöllä taipumusta piittaamattomuuteen.

4.4 Kiire

Kiire hallitsee aluksilla, kun puhutaan Human Factor -tilanteista. Nopeat käynnit satamissa, kuten lastin purun tai lastauksen takia, johtavat siihen tilanteeseen, että kaikkia kiireellisimpiäkään töitä ei välttämättä ehditä tekemään annetussa ajassa. Useiden päällekkäisten työtehtävien tai suoritusten määrä lisäävät työkuormaa ja stressitasot saattavat nousta. Käsiteltävää informaatiota ei ehditä prosessoida, jonka seurauksena voi aiheutua riskiarviointeja. Aikapaine voi syntyä, jolloin työntekijä saattaa ratkaista tärkeitä tehtäviä liian lyhyessä ajassa, mikä voi johtaa seuraaviin riskitilanteisiin. Kaksi kriittistä työtehtävää ei saisi mennä päällekkäin, eivätkä erilaiset työtehtävät saisi häiritä toisiaan, varsinkaan jos ne koetaan haasteellisiksi. (HF Tool™ 2022.)

Esimerkiksi konemestari harjoittelee konevalvomon yhdellä päätelaitteella päivitettyä uutta tietojärjestelmää, kun alus on saapumassa vaikeakulkuiseen satamaan ja apukone 2 tippuu verkosta. Konemestari yrittää saada puhelimella yhteyttä 1.konemestariin, mutta 1.konemestari ei vastaa. Konepäälliköstä ei ole apua, sillä hän on nukkumassa, ollen viime yönä korjaamassa 3. pääkoneen polttoainepumppua. Konevalvomon tietokonejärjestelmä on yli 14 vuotta vanha, eikä se tue nykyajan malleja. Apukoneiden järjestelmät ovat erillään pääkoneiden tietokonejärjestelmästä, sillä niitä ei ole vielä ehditty päivittää. Apukoneiden vanhahtava järjestelmä sisältää täten monimutkaista tietoa, jota on hidas tulkita ja niistä on haastava saada selkoa nopeasti. Yhtäaikainen kuormitus kasvattaa konemestarin stressitasot niin korkeiksi, että konemestari lamaantuu eikä pysty nousemaan konevalvomon penkistä. Jatkuva nopea

tahti satama-aikatauluissa, työaikapaine ja sääntö, ettei ylitöitä saa tehdä, on vähentänyt konemestarin aikaa opetella uusi, seuraavassa telakoinnissa kokonaan muuttuva tietojärjestelmä.

Laitteet eivät tukeneet konemestaria onnistumaan työssään, vaan sen sijaan laskivat hallinnan tunteen minimiin. Konemestari ei pystynyt vanhentuneelta järjestelmältä ottamaan selvää 2. apukoneen tilasta, eikä paikalle lähetetty moottorimies osannut vielä tutkia apukonetta, että siitä olisi ollut hyötyä konemestarin päätöksenteossa. (HF Tool™ 2022.)

4.5 Koulutus

Energia-alan turvallisuusasiantuntijan mukaan koulutuksia tulisi olla säännöllisin ajoin ja niiden tulisi olla käytännönläheisiä. Koulutuksien tulisi sisältää sekä teoreettista ymmärrystä aiheesta, että niitä pitäisi päästä syventämään erilaisten harjoituksien kautta, kuten harjoitusradoilla tai virtuaalitodellisuudessa. Jokaisessa harjoituksessa tulisi olla jokin aivoja stimuloiva osio, että harjoituksissa voidaan käsitellä monille vieraita aiheita. Tarkkaavaisuutta, muistia, havaitsemista, erilaisia sosiaalisen psykologian ilmiöitä ja kognitiivisen kapasiteetin rajoituksia, tulisi ottaa huomioon, kun suunnitellaan koulutuksia. Useissa maaorganisaatioissa on käytössä vuosittain vaihtelevia HF-koulutuksia, joissa ratkotaan tehtäviä joko ryhmätyönä tai parityöskentelynä mahdollisista riskitilanteista, mitä työpaikalla mahdollisesti voisi tapahtua. Yksittäinen pakollinen koulutus ei riitä, vaan niitä tulee kerrata ajoittain ja, että kouluttamisen on perustuttava vahvasti asiantuntijuuteen. Kun pystytään hallitsemaan omaa työtä, esimerkiksi uusien koulutuksien jälkeen, työtä on paljon mielekkäämpää tehdä.

5 TUTKIMUKSEN TULOKSET

Tutkimuksen tulokset perustuvat konemestareiden ja -päälliköiden vastauksiin. Tulokset ovat haastatteluiden nauhoitteista analysoitu sekä kirjoitettu, ja haastattelut on suoritettu syksyllä 2022. Tässä luvussa kerrotaan ensin haastattelukysymys, jota seuraa osittain pelkistetyt vastaukset aluskohtaisesti. Vastaukset esiintyvät luettelomaisena kokonaisuutena selkeyden vuoksi. Johtopäätöksissä sen sijaan pohditaan tutkimuksen tuloksia, sekä esitetään jatkotutkimusmahdollisuuksia ja mahdollisia parannusehdotuksia.

Miten kyberturvallisuus näkyy teidän aluksessanne?

Alus A: sähköpostiin saapuu satunnaisesti viestejä, joissa on ilmoituksia maailmalla liikkuvista huijausyrityksistä sekä viestejä, millaisia huijauksia yritykseen on saapunut aikaisemmin. Turvallisuusjohtamisjärjestelmässä on oma ohjeistus kyberturvallisuuden varalle, missä tietoa mm. Internetin käytöstä. Muistitikkuja ei saa kytkeä tietokoneisiin ja niissä on lukitut USB-portit. Salasanat vaihtuvat työkoneissa kolmen kuukauden välein. Salasanat saa jokainen itse valita, mutta ne eivät saa olla näkyvillä, eikä niitä saa jakaa ja ne tulee muistaa ulkoa.

Alus B: salasanoja on miljoonia eri järjestelmiin.

Alus C: Internetin käyttö ja aluksen verkkoon pääsy on rajoitettu. Laivan palvelimelle pääsee ainoastaan laivan päälliköt, komentosilta ja konevalvomo. Tämä on järjestetty erillisellä verkolla. Vaatii erikoisosaamista, jos halutaan yhdistyä muihin laitteisiin. Miehistölle on oma verkko, johon päästään lastitoimiston kautta. Tämä on haastateltavan mielestä heikoin lenkki.

Alus D: kaikki, jotka haluavat olla yhteydessä alukseen, ja ketkä saapuvat laivaan, joutuvat tekemään sopimuksen yhtiön kanssa. Tämä tarkoittaa sitä, että kaikilla on samat säännöt.

Alus E: työnantaja on nimennyt konttorilla ATK-vastuuhenkilöt. Ohjelmia päivitetään taukoamatta sekä sähköpostiviestejä tarkkaillaan, ja sähköpostiin saapuu ilmoituksia tulevista päivityksistä. Tehdään töitä sen eteen, ettei haittaohjelmia ilmenisi. Koneistoautomaatiojärjestelmän ollessa sisäänrakennettu ei sitä tarvitse päivittää jatkuvasti.

Alus F: aluksen Internet-yhteys on johdettu VPN-palvelimen kautta ja se on palomuurin takana. Tietokoneissa on salasanasuojattu tunnus. Ohjelmistojen asennus tai järjestelmäasennuksien muuttaminen tapahtuu ainoastaan päälliköiden toimesta. Tietokoneissa on virustorjuntaohjelmisto ja se pidetään ajan tasalla.

Kuinka paljon panostatte kyberturvallisuuteen ja mikä on varustamon rooli? Miten turvallisuus on ratkaistu kyberturvallisuuden osalta?

Alus A: varustamo on luonut kyberturvallisuusohjeet ja kerran kuukaudessa pidetään kokous koskien turvallisuusjohtamisjärjestelmää, missä ohjeistuksista muistutellaan. Ohjeistus on tarkka, eikä sitä ole tarvetta päivittää aktiivisesti, sillä ei ole tapahtunut vahinkoja. Ympärivuorokautinen turva on ulkopuolisen yrityksen kautta, jos sattuisi uhkaava kybertilanne aluksella tai olisi muuten haastava tilanne. Aluksen koneille ei saa asentaa tai kiinnittää mitään.

Alus B: varustamon kautta tehdään päivitykset ja pääsyt aluksen verkkoon. Varustamon IT-osasto huolehtii kolmansien osapuolien pääsemisestä aluksen verkkoon, jos sille on tarvetta. IoT-laitteita ei kytketä laivapalvelimelle, koska niillä on oma järjestelmä. Wi-Fi-verkko ei ole yhteydessä kriittisiin järjestelmiin tai laivapalvelimeen.

Alus C: vuosi sitten kaikille miehistön jäsenille tuli pakollisena suorittaa hyväksytysti kaksi kyberturvallisuuskurssia, josta jaettiin diplomit. Kurssi piti sisällään peruslaatuisia kysymyksiä kyberturvallisuudesta, ja perustui IMO:n suosituksiin. Kurssin pystyi suorittamaan Internetissä, jonka jokainen pystyi suorittamaan kotona.

Alus D: kaikki tietokoneiden käyttäjät joutuvat suorittamaan varustamon sisäisen kyberturvallisuuskurssin, ja kuukausittain järjestetään pienimuotoisia luentoja. Luennoissa käydään läpi kyberturvallisuusasioita, jonka seurauksena kaikkien tulisi olla tietoisia riskeistä. Näitä käydään läpi, jotta jokainen olisi tietoinen kyberturvallisuusuhkista. Tästä syystä epänormaali sähköposti huomataan ajoissa ja siitä kerrotaan eteenpäin. Kurssi on pakollinen kaikille, jotka käyttävät yhtiön koneita.

Alus E: varustamo on antanut kyberturvallisuusohjeet ja varustamo suorittaa tietokoneiden päivitykset ulkopuolisten uhkien torjumiseksi. Tämä takaa sen, että on riittävät edellytykset, eikä ulkopuolinen taho pääsisi hetkeksikään käsiksi järjestelmiin. Jokaisella on oma henkilökohtainen työsähköpostiosoite, jonka myötä on helpompi seurata, että viestit menevät työntekijöille. Sähköpostien päivitys tapahtuu automaattisesti. Salasanoissa tulee olla riittävä

määrä kirjaimia tai merkkejä, ja työkoneissa on vaatimuksena salasanojen päivittäminen tietyin väliajoin.

Alus F: varustamon vastuu tässä tapauksessa on huolehtia turvallisuudesta aluksen ja varustamon huolto-ohjelmien ja työaikakirjanpito-ohjelmien välillä. Aluksen omistaja on taas vastuussa muiden ohjelmistojen ylläpidosta. Miehistö pitää huolen, ettei laitteisiin tai järjestelmiin laiteta fyysisesti mitään sinne kuulumatonta.

Kuinka usein pidetään koulutuksia päällystölle ja miehistölle aiheesta? Entä ylläpidetäänkö näitä taitoja säännöllisesti? (Huolehtiiko varustamo/päällikkö/työntekijät itse näistä koulutusasioista?)

Alus A: kuukausittainen muistuttelu turvallisuusjohtamisjärjestelmän kautta, mutta myös silloinkin, jos on tarvetta aiheelle. Päällikkö päättää, koska kokouksia pidetään ja milloin turvallisuusjohtamisjärjestelmää (ja kyberturvallisuutta) läpikäydään.

Alus B: yksi seminaari on ollut reilu puolitoista vuotta sitten, kun varustamon DPA piti PowerPoint-esityksen. Ei ole varsin aktiivista toimintaa tämän puolesta.

Alus C: kyberturvallisuuskoulutuksia ei järjestetä erityisesti, paitsi ne aiemmin mainitut kaksi, jotka olivat pakollisia kaikille. Konttorissa on oma ATK, jonka puoleen voidaan kääntyä ongelmatilanteessa. Internetin ja verkon kanssa käytetään maalaisjärkeä. Lisäkoulutukset eivät olisi pahitteeksi.

Alus D: varustamon IT-osasto huolehtii kouluttamisesta ja he pitävät huolen, että taitoja ylläpidetään säännöllisesti. Viiden minuutin tehtäviä järjestetään viikoittain ja sen jälkeen vastataan kysymyksiin. Tehtävien tarkoituksena on muistuttaa asian tärkeydestä. Roskapostia saapuu paljon, varsinkin varustamolle, jonka vuoksi joudutaan olemaan jatkuvasti varpaillaan.

Alus E: kyberturvallisuuskoulutuksia ei pahemmin järjestetä, mutta muita koulutuksia järjestetään, ja ne ovat tarkoitettu pääsääntöisesti vastuuhenkilöille. Koulutukset järjestää työnantaja. Koulutukset ovat tarvittaessa opastuksia

erilaisiin tuntiohjelmiin, joiden jälkeen voidaan kertoa koulutuksen sisällöstä muille työntekijöille. Osa ohjelmista tosin työllistää liikaa, jolloin se lisää haastetta ja työmäärää. Tietyillä positioilla on enemmän vastuuta kuin toisilla (esim. konttorin ja aluksen viestintään liittyvät asiat). Sähkömestareilla on tässä suurempi vastuu.

Alus F: varustamo on pitänyt huolen, että koko aluksen henkilökunta on suorittanut kyberturvallisuusperuskurssin vuosi sitten. Taitojen ylläpitämisestä ei ole tietoa, sillä aihealue on uusi merenkulussa.

Kuinka perehdytätte uuden työntekijän aluksen tietojärjestelmiin? Mitä kaikkea työntekijät saavat tehdä päätelaitteilla ja muilla älylaitteilla?

Alus A: aluksen perehdytyskierrokseen sisältyy kyberturvallisuusosio, ja riippuu alukselle saapuvan henkilön positiosta, millaisen ohjeistuksen saa. Miehistötasolla asia koskee salasanojen käyttöä, USB-tikkujen käyttöä ja tietokoneiden käyttöä. Tämä sisältyy osastokohtaiseen perehdytykseen, joka on tehtävä kahden päivän aikana henkilön saapumisesta alukseen. Tietokonetta saa selailla ”järki päässä”, ja esimerkiksi viralliset asiat saa hoitaa tietokoneilla.

Alus B: uusille työntekijöille kerrotaan työkoneiden käytöstä ja heille mahdollisesti pidetään pienimuotoinen koulutus, kun saapuvat alukselle. Ohjeita ei noudateta orjallisesti, ja esimerkiksi omat pankkiasiat saa hoitaa valvomon erilliseltä tietokoneelta tai päivähuoneen tietokoneelta. Muistitikkuja tai kovalevyjä ei saa kytkeä yrityksen tietokoneisiin. IT-osasto valvoo tietokoneiden käyttöä jollakin tasolla.

Alus C: riippuu uuden työntekijän roolista: jos henkilö ei kuulu päällystöön, henkilön ei ole tarvetta päästä verkkoon kytketyille koneille. Konemiehiä ei perehdytetä aluksen kyberturvallisuustaitoihin. Joskus aikaisemmin verkkoon kytketystä tietokoneesta on jaettu (Windows 10) Wlan Internet, mikä aiheutti ongelmatilanteen. Henkilökunnalle on kuitenkin oma verkko.

Alus D: normaaliin käytäntöön kuuluu, että uusi henkilö perehdytetään aluksen tietokoneisiin ja -järjestelmiin. Aluksella on Wi-Fi-verkko (public network), jota miehistö voi käyttää. Aluksen konehuoneessa on laitteita, jotka on kytketty

laivan omaan verkkoyhteyteen, mutta se on palomuurien ja muiden suojauksien takana. Lisäksi IAS[22]-järjestelmä sekä muut tärkeät laitteet ja ohjelmat ovat omana järjestelmänään. Kaikki USB-portit ovat suljettu. Ainoastaan muutamassa koneessa USB-paikat ovat auki, ja ne ovat tarkoitettu muutamien laitteiden datan tiedonsiirtoa varten.

Alus E: riippuu henkilöstä ja positiosta, mutta henkilöt perehdytetään aina aluksen turvallisuuteen, joka sisältää palo- ja pelastautumisohjeistukset. Perehdytyslistat ovat alueittain ja henkilön postiosta riippuvaisia, esim. konemiehille tulevat perehdytyksen seurauksena laivan sisäiset järjestelmät tutuiksi. Henkilökunnan tiloissa on kansioita, jotka sisältävät käyttöturvallisuustiedotteet. Jokainen miehistön jäsen lukee ja kuittaa nämä kansiot suoritetuiksi. Kansioissa on luettavissa varustamon turvallisuusvaatimukset ja kyberturvallisuusosio (mm. sähköpostin käyttö ja Internet-sivujen käyttö). Miehistöllä on oma tietokone ja siinä on estot tietyille sivustoille. Konttorin kautta seurataan miehistön Internetin käyttöä, eikä aluksen oma Wi-Fi ole välttämättä kaikille saatavilla.

Alus F: konemiehistö on lähes sama kuin aina ennenkin, mutta jos alukselle saapuisi uusi työntekijä, hänet perehdytettäisiin työaikakirjanpito-ohjelmiston käyttöön. Jos uusi työntekijä olisi päällystön jäsen, hänet perehdytettäisiin myös aluksen huolto-ohjelman toimintaan. Työntekijät saavat käyttää toimistojen tietokoneita vapaa-ajallaan, kunhan se ei häiritse työntekoa tietokoneilla. Tietokoneiden ja älylaitteiden käyttö on suljettu satelliittiyhteyden omaavasta langattomasta verkosta, sillä ne eivät saa häiritä työntekoon tarkoitettua kaistaa.

Saako työntekijät pitää omia puhelimiaan mukana, kun he liikkuvat konehuoneessa? Onko kameran käytöstä ja kuvien jakamisesta rajoitettu? Onko älylaitteiden käyttöä rajoitettu?

Alus A: puhelimia saa käyttää konehuoneessa ja kuvia saa ottaa, mutta niiden jakamista sosiaaliseen mediaan tulee harkita tarkkaan, sillä se ei saa vaarantaa työnantajaa tai laivaa.

[22] Integrated Automation System – aluksien automaatiojärjestelmä, joka on usein kahdennettu.

Alus B: puhelimia käytetään, vaikka lähtökohtaisesti niiden käyttö on kielletty työaikana. Puhelimien käyttö ei saa häiritä työntekoa. Valokuvia saa ottaa, mutta niitä ei saa jakaa eteenpäin. Varustamo-ohjeessa ilmoitetaan, ettei kuvia saa jakaa sosiaaliseen mediaan tai niitä saa laittaa muuhun yleiseen jakeluun. Epäkohtia kuitenkin havaitaan, ja alukselta otettuja kuvia on jouduttu poistamaan sosiaalisesta mediasta.

Alus C: puhelimet saavat olla käytössä, mutta kuvia ei saa jakaa, vaikka sen tiedottaminen onkin ollut heikolla pohjalla. Sosiaalisesta mediasta saattaa erottua oma naama, vaikkei sitä haluaisi. Teknisistä laitteista ei saa ottaa kuvia, eikä aluksen konehuoneesta saa ottaa yhtään kuvaa, ellei varustamo anna siihen lupaa.

Alus D: työaikana ei saa käyttää puhelimia, mutta se on kuitenkin työntekijästä kiinni, miten hyvin ohjetta noudatetaan. Aina tämä ei ihan toteudu: puhelimia näkyy ja ”kännykkä kuuluu tämän päivän elämään”, joten sitä ei voida kokonaan vaatia poistettavaksi. Kuvia ei kuitenkaan saa jakaa sosiaaliseen mediaan, sillä siitä on mainittu jo työsopimuksessa.

Alus E: ulkona lipuvasta laivasta saa ottaa kuvan, mutta ei tunnistettavasti aluksen sisältä. Tämä on sen takia, ettei työntekijöitä tai aluksen laitteita tunnisteta. Kuvia ei saa lähettää muille henkilöille, eikä konehuoneesta tai -valvomosta myöskään saa ottaa kuvia tai jakaa niitä.

Alus F: puhelin saa olla mukana ja sillä voidaan ottaa kuvia korjattavasta kohteesta jatkoselvitystä varten. Kuvia ei saa tosin jakaa palveluihin tai sosiaaliseen mediaan ilman varustamon tai omistajan lupaa.

Onko rajoituksia mm. muistitikkujen käytöstä, puhelimien lataamisesta/ kytkemisestä aluksen tietokoneeseen? Miten tiedonsiirto (esim. kuvat tietokoneelle) on järjestetty?

Alus A: aluksen oma, miehistölle tarkoitettu Wlan on irrotettu työkoneverkosta. Miehistön Wlanista voidaan siirtää kuvia sähköpostin välityksellä eteenpäin. Muistitikut eivät ole sallittuja, ellei kyseessä ole työhön tarkoitettu muistitikku.

Työmuistitikut ovat varattuja laitekohtaisesti (laitteet, jotka eivät ole yhteydessä Internetiin), eli yksi tikku yhdelle laitteelle. Alihankkijat eivät saa laittaa muistitikkuja kiinni.

Alus B: omia puhelimia tai muistitikkuja ei saa kytkeä aluksen tietokoneisiin. Aluksella on kamera, jota käytetään ensisijaisesti, mutta jos kuva tulee ottaa nopeasti, voidaan käyttää omaa henkilökohtaista puhelinta. Otetut valokuvat lähetetään sähköpostin kautta tietokoneelle (jos jostain syystä aluksen kamera ei ole saatavilla ja joudutaan käyttämään omaa puhelinta esimerkiksi laiterikon takia nopeasti). Yrityksen puhelin on yhteydessä pilvipalveluun, mutta se toimii heikosti. Usein kuvat lähetetään koneelle sähköpostin kautta, mutta Internetin puuttuessa kuvat voidaan lähettää suorana siirtona 1.konemestarille, joka taas siirtää kuvat myöhemmin sähköpostin välityksellä tietokoneelle. Viimeisenä vaihtoehtona puhelin tai kamera kytketään tietokoneeseen johtimen kautta.

Alus C: kuvia otetaan paljon ja niille on omat kamerat. Muistikortilta jaetaan kuvat palvelimelle, eikä omia puhelimia saisi käyttää. Omaa puhelinta ei saisi kytkeä verkkoon, mutta ei sitä valvota. Palvelimen kautta kuvat lähetetään tekniselle osastolle maihin. USB-estot olisivat hyviä.

Alus D: kaikki USB-portit ovat lukittuina, eikä muistitikkuja saa käyttää. Jos niitä käytetään tiettyjen laitteiden takia tiedonsiirtoa varten, muistitikut menevät ”pesukoneen” kautta. (Tässä tarkoitetaan muistitikun virus- ja haittaohjelman tarkastuslaitetta, joka on erillisenä laitteena tietokoneista ja järjestelmistä.)

Alus E: virkapuhelimella tai työkameralla voidaan ottaa kuvia, jos esimerkiksi tarvitsee ottaa kuva laakerivauriosta. Kuva voidaan jakaa aluksen palvelimelle. Jos käytetään muistitikkua, se on ainoastaan laivan omaan käyttöön, mistä kerätään laitekohtaista tietoa. Henkilökohtaista tikkua ei saa käyttää, koska se on voinut käydä sellaisissa koneissa, jotka ovat saastuneet. Sähkömestarit usein varmistavat muistitikun sopivuuden. Huoltomiehillä saattaa olla omat muistitikut mukana, mutta he eivät saa käyttää niitä. Huoltomiehet joutuvat lähettämään kuvat tai tiedot sähköpostin kautta esim. konepäällikölle.

Alus F: aluksen omia muistitikkuja saa kytkeä ainoastaan tietokoneisiin. Muistitikut ovat periaatteessa laitekohtaisia, mistä data kerätään tai siirretään.

Tiedonsiirto onnistuu myös Bluetoothin välityksellä. Puhelimien lataamisesta tai kytkemisestä aluksen tietokoneeseen ei ole rajoituksia.

Kuinka konevalvomoon pääsy on rajoitettu? Onko kulkuluvat? Ketkä kaikki pääsevät?

Alus A: aluksella on laakonkivahti, joten kukaan ei tule kutsumatta sisälle. Aluksella ei ole omaa kulkulupajärjestelmää ja konehuoneessa voidaan pitää ovet auki, ellei erikseen määrätä niiden kiinnipitämisestä. Vierailijat saapuvat alukseen lastivalvomon kautta, ja heillä on aluksen työntekijä mukana vierailun ajan.

Alus B: valvomon ovet ovat lukossa, ja työntekijät kulkevat omilla kulkukorteilla ainoastaan sisään. Korsteenista pääsisi sisään, mutta nekin ovat lukittuina munalukoilla. Ulkopuolisilla urakoitsijoilla on omat kulkukortit.

Alus C: käytössä ei ole kulkulupia, lukkoja tai muuta kulunvalvontaa. Satamassa on käytössä ainoastaan laakonkivahti, ja sisäänkirjautuminen tapahtuu vierailijoiden tai urakoitsijoiden ollessa paikalla. Joku henkilö voisi livahtaa sisään, koska miehistöä on rajallisesti aluksella.

Alus D: konevalvomoon pääsee ainoastaan he, jotka työskentelevät siellä. Aluksen purseri antaa kulkuluvat laivalla liikkumiseen. Pääsy on rajattu alueellisesti, joten esimerkiksi laivasiivoojat eivät pääse konehuoneeseen. Ovia voi jäädä lukitsematta ja sen seurauksena voi syntyä vahinkoja. Ovet on pidettävä kuitenkin kiinni, sillä jos joku pahantekijä pääsee väärille alueille. Ovien kiinnipitämisestä on pidetty henkilöstölle puhutteluita.

Alus E: konevalvomon oven tekstikyltissä lukee laivan ollessa ajossa, että asiattomilta on pääsy kielletty. Vierailijoita otetaan vastaan, mutta heistä on oltava tieto etukäteen. Yleensä vierailijat ovat kuitenkin asiantuntijoita. Aluksen ja konehuoneen ovet ovat lukitsematta, jolloin olisi mahdollista päästä alukseen. Osa tietyistä alueista on lukittu. Aluksella on kuitenkin valvontakamerat, jotka seuraavat liikkumista. Aluksella tapahtuu jatkuvaa seurantaa ja valvontaa.

Alus F: konevalvomoon ei ole rajoitettua pääsyä merellä, eikä kulkulupajärjestelmää ole käytössä. Jos alukselle saapuu vierailijoita, heistä on usein tieto etukäteen ja konemestari tietää keitä konehuoneessa tai aluksella silloin liikkuu.

Millaisia kyberuhkia laivaanne voisi kohdistua?

Alus A: konehuoneen näkökulmasta tietokonevirus on pahin mahdollinen uhka, sillä se sekoittaisi koko tietoliikenteen. Mikään kriittinen laite ei kuitenkaan ole verkossa, joten se ei ehkä ole uhka tämän puolesta.

Alus B: jos tietokoneisiin pääsisi tunkeutumaan hakkeri, olisi se huolestuttavaa, vaikka järjestelmät ei ole suoranaisesti yhteydessä koneiden kriittisiin järjestelmiin. Ohjailujärjestelmiin olisi mahdollista päästä, jos kyseessä on taitava hakkeri. Tämän yhteydessä mahdollisia henkilötietoja voisi vuotaa. Vahinkoa ei koituisi pääkoneille, mutta ECDIS-järjestelmään pääsy olisi vaarallista. Ilmanvaihtotietokone, jossa on verkkokytkentäominaisuus, on myös alttiina hakkeroinnille. Virityksien kautta ilmanvaihtotietokone olisi Internet-yhteydessä jatkuvasti. Ilmanvaihtotietokoneelle pääsee laitevalmistaja (kolmas osapuoli) Internetin kautta, vaikka se vaatii heiltä erillisen sisäänkirjautumisen. Kolmannella osapuolella on käytössä MFA-todennus, jotta he voivat tarvittaessa ohjata aluksen ilmanvaihtoa.

Alus C: kyberuhka voisi tapahtua sähköpostin tai muistitikun kautta. Tietotekniikkaosaaminen on kuitenkin hyvällä tasolla: sähköpostien ylimääräisiä linkkejä ei klikkailla. Tietokoneissa on mahdollista asettaa muistitikku tai -kortti.

Alus D: se on merkittävä uhka, sillä suurin osa järjestelmistä on kytketty tietokoneisiin, ja tietokoneet ohjaavat kaikkea. Koko ohjaus tapahtuu konevalvomosta. On huomattava riski, jos joku esimerkiksi pääsee käsiksi tiettyyn ohjelmaan tai sähköjärjestelmään. Joillakin laitetoimittajilla on etäkäyttömahdollisuus, mutta heille tulee fyysisesti antaa lupa ohjelmien ja järjestelmien käyttöön.

Alus E: ohjelmat ovat kiinteitä, joten niihin ei pääse näppärästi käsiksi. Ulkopuolelta niitä ei voida ohjata, mutta ei tiedetä, voidaanko ohjata maista tätä

järjestelmää. Esimerkiksi osa sovelluksien päivityksistä tapahtuu parametrimuutoksien kautta, mutta sitä ei tiedetä, että voidaanko niitä muuttaa ulkopuolelta (etänä/maista). Tämä tosin herättää pohdintaa. Haittaohjelmat ja virukset ovat mahdollisia, jos päivityksiä tai virustorjuntaa ei ole suoritettu ajallaan.

Alus F: aluksen sähköpostiin voi saapua viesti, jonka liitetiedostossa on virus, tai sähköpostin kautta voidaan kalastella tietoja. Aluksen tärkeisiin järjestelmiin on mahdollista päästä sisään etäyhteyden kautta, ja tämä voisi mahdollisesti saada aluksen järjestelmät epäkuntoon, jos kyseistä väylää käytetään. Laivaverkkoon voidaan kytkeä henkilökohtainen tietokone, ja laite voidaan asettaa Wlan-hotspotiksi ilman salasanaa. Teoriassa tätä kautta ulkopuolinen voisi päästä kiinni laivaverkkoon.

Onko ollut uhkatilanteita? jos niin, minkä takia tilanne syntyi? Mikä oli sen aiheuttaja? Onko niistä raportoitu eteenpäin?

Alus A: spämmisähköpostit ovat olleet pahin uhkatilanne. Asiasta kerrottiin konttorille, jonka jälkeen ulkopuolinen yritys tarkasti asian. Tämän seurauksena virallinen tiedotus asiasta jaettiin laivahenkilöstölle. Haitallisesta sähköpostista otettiin kuva, ja sen jaettiin muiden varustamon aluksien kesken. Sähköposti liittyi lunnasvaatimuksiin. Ulkopuolinen yritys sai kuitenkin asian hoidettua kahdessa päivässä kiitettävästi.

Alus B: ei ole ollut uhkatilanteita, mutta erikoisia sähköpostiviestejä on saapunut. Sähköpostilinkkejä ei ole kuitenkaan klikattu auki. Kerran yhdestä hämärästä sähköpostista otettiin kuvakaappaus IT-osastolle, ja IT-osasto neuvoi, että se tulee poistaa.

Alus C: tietokoneisiin ei ole kohdistunut uhkatilanteita viimeisen kolmen vuoden aikana.

Alus D: ei ole ollut uhkatilanteita.

Alus E: varsinaisia tietoliikenteen uhkia ei ole ollut, koska käytössä on jatkuva seuranta ja se toimii hienosti. Uhkia pyritään estämään jatkuvasti. ”Yksikin tunkeutumisyritys on jo liikaa”.

Alus F: ei ole ollut uhkatilanteita.

Kyberhyökkäyksen kohdatessa miten toimisit? Tiedätkö mistä saat apua? (esim. laiva ei pääse lastaamaan, tai laiva on jumissa satamassa, tai ei ole puhelinyhteyttä/ Wi-Fiä?) (Onko suunnitelma paperisena?)

Alus A: ensiksi ilmoitetaan kollegalle, jos heillä olisi tietoa asiasta. Jos ollaan satamassa, otetaan yhteyttä konttoriin jollakin puhelimella, ja tämän jälkeen otetaan yhteyttä ulkopuoliseen yritykseen. Asiasta tiedotetaan kaikille kenelle pystytään, kuten turvahenkilölle. Jos tilanne vaatii, ryhdytään sammuttamaan järjestelmiä. Toimintaohje löytyy paperisena.

Alus B: satamassa otetaan yhteyttä satamaviranomaisiin tai ahtaajiin ja IT-osastolle. Kyberhyökkäyksen kohdatessa Internet ei silloin todennäköisesti toimi. Konehuoneessa on IP-puhelin, jonka kautta voidaan yrittää soittaa. Myös konttoriin ja DPA:han tulee ottaa yhteyttä. Yrityksen yleispuhelimella voidaan yrittää soittaa satamasta tai maista tai ulkokannelta apua. Valmiusryhmä on olemassa hätätilanteita varten. IT-osastolla on päivystys, johon voidaan laittaa sähköpostia tai soittaa, ja se toimii lähes 24/7. Alukselta löytyy Cyber Security Policy, jossa on määriteltynä riskianalyysit, jotka liittyvät aluksen ohjailuun kyberuhkassa.

Alus C: jos tavallinen puhelin ei toimi, otetaan yhteyttä konttoriin satelliittipuhelimen kautta. Konttorin kautta saa apua. Suunnitelmaa ei löydy paperisena.

Alus D: otetaan yhteyttä konttorin IT:hen. Jollain tavalla on päästävä heidän kanssaan yhteyteen. ”Paperisuunnitelma on varmaan niin salainen”, ettei haastateltavakaan tiedä.

Alus E: jotenkin on päästävä yhteyteen varustamon ja turvallisuuspäällikön kanssa, koska he kertoisivat ensimmäiset ohjeistukset. Tieto on ollut aina saatavilla, ja satelliitit toimivat hyvin, joten paljon saa tapahtua ennen kuin yhteys katoaa. Suezin kanava on tosin merirosvoaluetta, joten siellä pitäisi olla erittäin varuillaan. Hätäsignaalia voidaan lähettää hätätilanteessa ja lisäksi voidaan käyttää morsetusta osana pelastussignaalia. Pelastusraketti voisi olla

myös viimeinen keino. Automaattinen paikannusjärjestelmä toimisi, jos tilanteet eskaloituisivat suuriksi. Paperisuunnitelmasta ei ole tietoa.

Alus F: toimintasuunnitelmaa ei ole paperisena eikä asiasta ole ollut keskustelua aluksella. Satelliittipuhelimen kautta voisi ottaa yhteyttä varustamoon ja omistajaan, ja heidän neuvoillaan suorittaa tarvittavat toimenpiteet. Jos aluksen ohjailuun tai propulsioon liittyvät järjestelmät olisivat hyökkäyksen kohteena, otettaisiin yhteyttä myös laitevalmistajiin.

Onko teillä satelliittiyhteys varustamon/ muiden laivojenne kanssa? (Miten sen käyttö on suojattu?)

Alus A: löytyy, ja siinä on todennäköisesti ulkopuolisen yrityksen suojausjärjestelmä.

Alus B: löytyy satelliitti ja satelliittipuhelinyhteys, mutta sen suojauksesta ei ole tietoa.

Alus C: satelliitin kautta toimivat Internet ja puhelin, ja jos tarve vaatii, ja ollaan kaukana maista, voidaan käyttää satelliittiyhteyttä. Satelliitin suojauksesta ei ole tietoa.

Alus D: aluksella on satelliittiyhteys ja suojaus tapahtuu todennäköisesti varustamon IT:n kautta. Haastateltava ei ole perehtynyt satelliitin suojaukseen. Aluksella toimii myös 4G-yhteys.

Alus E: on satelliittiyhteys, jonka kautta saadaan viestintä toimimaan Alaskassakin.

Alus F: satelliitin kautta on toimiva verkkoyhteys, mutta sen suojauksesta pitäisi kysyä palveluntarjoajalta.

Miten vastuunjakaminen on huolehdittu? Onko kyberturvallisuus lisätty toimenkuvaan aluksella? / Onko tehtävälistalla henkilöä, joka tarkistaa laitteiden päivitykset, palomuurit, suojaukset, ja varmuuskopioinnin?

Alus A: työkoneiden puolesta ulkopuolinen yritys hoitaa asian, mutta aluksella tutkien ja karttojen yms. huolehtiminen on ykkösperämiehen vastuulla.

Alus B: IT-osasto hoitaa, ja osastolta käydään aluksella päivittämässä laitteita. IT-osastolla on oma tiimi, joka huolehtii palomuureista ja päivityksistä. Laivalla ei ole ketään IT-asiantuntijaa, mutta kapteeni toimii Safety/ Security Officerina, jolle tämä vastuu on todennäköisesti jaettu.

Alus C: konttorin etäyhteyden välityksellä huolehditaan laiteiden ja järjestelmien päivityksistä. Aluksella ei ole määrättyä henkilöä, joka on vastuussa laitteiden ja järjestelmien päivityksistä tai suojauksista.

Alus D: laivalla on kommunikointiteknikko, joka huolehtii päivittäisistä asioista ja hän on tarvittaessa yhteydessä varustamoon. Varustamo huolehtii päivityksistä etänä. Tämä ei koske kuitenkaan aluksen sisäistä järjestelmää, kuten IAS:ää tai koneenvalvontajärjestelmää.

Alus E: sähkömestarit huolehtivat laitteiston automaation toimivuudesta ja päivityksistä, sekä huolehtivat palvelimen turvajärjestelmien toiminnasta. Maista saadaan lisäapua tarvittaessa, ja jos laivan sähköposti kaatuu, ensisijaisesti soitetaan työnantajan ATK-tukeen. Aluksella on tarkkaan nimetyt henkilöt, jotka saavat hoitaa päivityksiä ja uudelleen käynnistyksiä. Perämiehille on myös osa vastuuta siirretty, jolloin he saavat esimerkiksi tietyistä komentosillan ohjelmista käynnistää uudelleen.

Alus F: omistajan ICT-osaston teknikot suorittavat tietokoneille päivityksiä ja varmuuskopiointeja, ja he huolehtivat myös palomuureista ja suojauksista joko aluksella tai etäyhteydellä. Laivahenkilökunta ei ota osaa asennuksiin.

Kuinka usein ulkoistatte osan työmäärästänne kolmannelle osapuolelle? Millaisiin asioihin kolmas osapuoli pääsee käsiksi ja millaiset oikeudet he saavat? Miten kolmas osapuoli tarkastetaan? Onko hän/he luotettavia ja vastuullisia?

Alus A: aluksella käytetään ainoastaan laitteiden valtuuttamia henkilöitä. Tiedossa on lista henkilöistä, joita saa käyttää alihankkijoina, sillä he tuntevat

laitteensa parhaiten. Urakoitsijoiden toimintaa valvotaan jatkuvasti, eikä heillä ole pääsymahdollisuutta verkkoihin tai työkoneille.

Alus B: urakoitsijat eivät saa käyttää aluksen laitteita tai Internetiä. Urakoitsijat saavat kuitenkin käyttää aluksen yleistä Wi-Fi-yhteyttä, jos vaativat pääsyä koneelle. Tiedot ja luvat ovat sovittu etukäteen urakoitsijoiden tilausvaiheessa, jos heillä on tarvetta kytkeytyä aluksen verkkoon. Alukselle saapuvat urakoitsijat varmennetaan IT-varaston kautta. Aluksella ei ole käytössä erityistä tarkistusproseduuria: jos esimerkiksi Wärtsilä tai Lyngso tulee alukselle, he tietävät, mitä tekevät ja tuovat mukanaan omat tietokoneensa. Luotetaan sokeasti alukselle saapuviin urakoitsijoihin, eikä heitä ole mahdollista tutkia paikan päällä.

Alus C: yritykset ja urakoitsijat on tarkastettu todennäköisesti konttorin kautta. Konttori tilaa huollot ja korjaukset alukselle. Jos urakoitsijoilla on tarve päästä teknisiin laitteisiin, heillä on omat tietokoneet ja Internet mukana.

Alus D: urakoitsijoilla ei ole pääsyä sisäiseen verkkoon. Urakoitsijoilla on samat verkko-oikeudet kuin matkustajillakin. Kaikki on eristetty toisistaan, ja urakoitsijoiden sopimukset menevät IT-osaston kautta. Urakoitsijat pääsevät Internetiin ainoastaan omien yhteyksien kautta. Jos urakoitsijoilla on tarve päästä aluksen järjestelmiin tai verkkoon, se on oma proseduurinsa IT-osaston kanssa.

Alus E: esim. ABB:llä työskentelevät ovat luotettavia, koska he hallitsevat omat ohjelmansa. Usein alukselle saapuvat urakoitsijat ovat luotettavia ja tunnustettujen yritysten henkilöitä. Urakoitsijat pääsevät ainoastaan omiin järjestelmiin käsiksi, ellei aiemmin erikseen ole sovittu, että tarvitsee huoltaa esim. painolastivedenkäsittely -ohjelmistoa. Urakoitsijat saavat käyttää ainoastaan omaan verkkoyhteyttään, ja suorittaa työn, mitä oli suunniteltu aiemmin.

Alus F: kolmannet osapuolet tulevat alukselle suoraan laitevalmistajalta suoritettavaa työtehtävää varten. Esimerkiksi Wärtsilältä saapuu pääkonehuoltajat ja Valmetilta asentajat konevalvontajärjestelmän huoltoa varten. Konevalvontajärjestelmien muutostöihin otetaan myös aina asiantuntija paikalle, koska he

kantavat vastuun tekemästään työstä ja raportoivat tekemänsä työt alushenkilökunnalle. Tämä takaa luotettavuuden.

Millaiset työajat teillä on? saako ylitöitä tehdä ja tehdäänkö niitä?

Alus A: ylitöitä vältetään, sillä niille on harvemmin tarvetta. Ainoastaan hätätilanteessa tai muissa poikkeustilanteissa saa tehdä ylitöitä. Jos satamaan tullaan tai lähdetään työajan ulkopuolella, silloin joustetaan. Töitä tehdään 8–17 välillä.

Alus B: ylitöitä tehdään hieman, jolloin työaika on 10,5 tunnista 12 tuntiin.

Alus C: jos aluksen ruumaa joudutaan puhdistamaan, silloin saattaa päivät venyä pitkiksi. Tämä huomioidaan lepoajassa työn suorittamisen jälkeen. Päälliköllä ja konepäälliköllä työaika on kahdeksan tuntia, mutta yllättävissä tilanteissa päivä saattaa myös venyä. Miehistö tekee pidempää päivää satunnaisesti, koska he tekevät vuorotyötä.

Alus D: vahdinajo tapahtuu 12 tunnin vuoroissa joka päivä, ja päivämiehet tekevät 10,5 tunnin päivää. Ylitöiden tekoa vältetään, mutta se teettää haastetta, sillä alus on uusi. Ylitöitä tehdään satunnaisesti. Uusien miehistön jäsenien saaminen alukselle on haasteellista. Riski on aina suurempi, kun on väsynyt.

Alus E: vahdeilla työajat ovat 12 tuntia töissä ja 12 tuntia vapaalla, silloin kun ollaan ajossa. Satama-aikana ei ole merivahtia. Ylitöitä tehdään satunnaisesti, kun merivahti on päällä.

Alus F: työaika on normaalisti 8–17. Ylitöitä ei synny kuin pakottavasta tarpeesta, esim. konerikon takia, jolloin korjaus ei voi odottaa.

Millainen työyhteisö teillä? tuleeko kaikki toimeen kaikkien kanssa? miten kulttuurierot on otettu huomioon?

Alus A: suomalainen miehistö, ja kaikki tulevat toimeen keskenään.

Alus B: kaikki eivät pidä toisistaan, mutta tulevat kuitenkin ihan hyvin toimeen keskenään. Alukselle on saapunut enemmän työntekijöitä, ja työmäärät ovat vähentyneet. Aikataulut ovat muuttuneet ja lähtöjä on nykyään enemmän kuin aikaisemmin.

Alus C: erittäin hyvä työporukka, vaikka aluksella työskenteleekin vaihtelevasti muita kuin suomalaisia. Jossain positioissa miehistön vaihtuvuus on näkyvämpää kuin toisessa. Kaikki tulevat hyvin toimeen keskenään. Vähäinen miehistö edesauttaa tuntemaan henkilöitä paremmin.

Alus D: aluksella on hyvä työyhteisö, eikä kulttuurieroja esiinny. Turvakielenä on ruotsi, mutta suomenkieliset pärjäävät hyvin.

Alus E: yllättävän hyvä työyhteisö, eikä aluksella ilmene työpaikkakiusaamista. Joskus joku henkilökunnasta tosin tuottaa välillä haastetta.

Alus F: työyhteisö on tiivis, jolloin yhteisöllisyyden tunne lisääntyy. Työtekijöiden vaihtuvuus on vähäistä. Kaikki tulevat toimeen keskenään, vaikka luonnollisesti, kitkaakin esiintyy. Tämä kuitenkin pyritään käsittelemään avoimin mielin työyhteisön kesken ja löytämään ratkaisu ongelmiin. Asioista vaikeneminen ei kuulu tapoihin.

Miten inhimilliset tekijät on otettu huomioon, jotta virheitä vältytään?

Alus A: perehdytyksiä on ajoittain. Aluksella on käyttäjäkohtaiset työpöydät, jonka seurauksena voidaan jäljittää työntekijään, jos on klikattu vääränlaista linkkiä koneella. Muistutetaan kyberturvallisuuden tärkeydestä.

Alus B: aluksen koneissa on virusvalvontaa, ja väärillä sivustoilla käynti johtaa huomautuksiin. Epäilyttävät sähköpostit antavat varoitusilmoituksen näytölle. Palomuuri valvoo. Inhimillistä tekijää ei ole huomioitu tässä, mutta aluksella on menty parempaan suuntaan työaikojen suhteen, jolloin työntekijät ovat olleet virkeämpiä.

Alus C: luottamuksella kollegaan ja esimerkillä, miten ei saa toimia.

Alus D: kaikille ei ole koulutusta. On vain koulutuksia, joita on viime vuosina pyörinyt. Tietokoneiden käyttäjät joutuvat olemaan kuitenkin hereillä asiasta, ja tiedostamaan kyberuhkat. Kyberuhkista pyritään muistuttamaan jatkuvasti.

Alus E: konepäällikön velvollisuutena on seurata inhimillistä tekijää, ettei kukaan ole esimerkiksi liian väsynyt työskentelemään. Aluksella on 0-toleranssi alkoholin suhteen, ja yksikin kerta riittää, jolloin työskentely aluksella loppuu. Aluksella huolehditaan toinen toisistaan. Väsyneenä voi tapahtua kaikenlaista, esimerkiksi kone voidaan vahingossa sammuttaa kesken ajon. Puhelimet tulee olla ladattuina töihin tullessa, koska tavoitettavuus ei saa katketa, eikä tietokatkoja saa esiintyä. Valvomo on miehitettynä jatkuvasti. Vahdit käyttävät Dect-puhelimia, joita kannetaan aina mukanaan. Vahtilistat tulee olla aina ajan tasalla, millä vältetään virheiden syntyminen.

Alus F: jos epähuomiossa avataan epämääräinen liitetiedosto sähköpostista, on virustorjuntaohjelmiston ja palomuurin tehtävänä suodattaa haitallinen materiaali pois loppukäyttäjältä, jottei turvallisuus vaarannu. Kyberturvallisuuskurssi toi näitä asioita esille, ja asioiden ymmärrys todettiin ennen sertifikaatin myöntämistä kokeella, jossa tarkistettiin asioiden sisäistäminen.

6 JOHTOPÄÄTÖKSET

Usein onnettomuuksien ja ”läheltä piti” -tilanteiden taustalla on ihmisen oma toiminta, jolloin ne aiheutetaan, eivätkä ne vain tapahdu itsestään. Perustana tässä voidaan pitää joko organisaation ohjeiden sivuuttamista, tai niiden heikkoa laatua, tai aluksen henkilöstön välinpitämättömyyttä tai tietämättömyyttä. Harvoin kyberuhkat suoranaisesti vaikuttavat ihmishenkiin, mutta ne vaikuttavat huomiota herättävästi aluksien ja varustamoiden maineeseen ja taloudelliseen tilanteeseen. Lisäksi kyberturvallisuuden varalle rakennettu hätätoimenpidesuunnitelman paperiversion puuttuminen, vaikeuttaa mahdollisesti kohtaavassa hyökkäyksessä toimimista. Aluksilla on kuitenkin toimenpidesuunnitelmat laminoituna tulipalon ja pelastusveneiden toimintaan, niin miksi ei kyberturvallisuudelle? Tuloksia tarkasteltaessa huomataan myös, että inhimillinen tekijä on läsnä tilanteissa.

6.1 Kyberturvallisuustaidot

Kyberturvallisuus ja sen hahmottaminen on alkanut näkyä alusten käyttöhenkilöiden rutiineissa, sekä mielenkiinto aihetta kohtaan on herännyt aluksilla ja varustamoissa. Vesikuljetuspoolin mukaan tietoisuus on herännyt kyberturvallisuutta kohtaan ja se kasvaa koko ajan mm. tapahtuneiden merenkulkuun kohdistuneiden tapausten takia. Lisäksi IMO:n päätöslauselman sekä kiertokirjeen (MSCFAL.1/Circ.3) mukaan hallintojen, varustamojen ja luokituslaitosten tulee huomioida kyberriskienhallinta yhtenä osana ISM-säännöstön edellyttämiä tavoitteita ja toiminnallisia vaatimuksia. Aiheesta on järjestetty myös runsaasti koulutuksia ja muita tilaisuuksia, joten kyberturvallisuuden merkityksestä ei ole voinut jäädä paitsi. Valitettavasti kyberturvallisuuden toimenpiteet jäävät osassa varustamoja aika vähäisiksi.

Verkkoon pääsyt ovat usein aluksilla rajoitettu, joten todennäköisyydet kyberuhkille vähenevät. Laivan palvelin on oma yksikkönsä, ja IAS-järjestelmä on kahdennettu, eikä se ole yhteydessä aluksien Wi-Fi-tai Wlan-järjestelmiin. Kriittisiin järjestelmiin pääsy on myös rajoitettu henkilötasolla. Kriittiset järjestelmät ovat myös kahdennettuja, ja usein laivapalvelimille pääsee ainoastaan valvomossa työskentelevät mestarit ja konepäällikkö.

Laitteiden päivityksiä suoritetaan etäyhteydellä, mutta laitteita, joita ei voi etäyhteydellä päivittää, varustamot usein lähettävät omia IT-henkilöitä tai varmistettuja laitehuoltajia paikalle. Muutamalla aluksella on nimettyjä henkilöitä, jotka suorittavat joitakin päivityksiä ja uudelleen käynnistyksiä paikan päällä. Yhdellä aluksella on kommunikointiteknikko huolehtimassa palvelimen ja laitteiden toimivuudesta. Urakoitsijoille tai kolmansille osapuolille ei anneta pääsyä laivaverkkoon, ellei kyseessä ole juuri laivaverkon testaukset tai päivitykset urakoitsijan toimesta. Varustamo huolehtii urakoitsijoiden saapumisesta aluksiin, jolloin heidän pätevyytensä on varmistettu varustamon kautta. Alukset tietävät, keitä urakoitsijoita heille saapuu, mutta eivät välttämättä tunne heitä entuudestaan. Urakoitsijoita ei usein uudelleen tarkisteta laivan päällä.

Omien muistitikkujen käyttö ja laitteiden kytkeminen aluksen verkkoon ovat vakaalla pohjalla, koska niiden käytöstä on määritetty. Osalla aluksista on lukitut USB-portit tai ne ovat kokonaan poistettu, mitkä vähentävät inhimillisestä

toiminnasta aiheutuvaa virheen mahdollisuutta kytkeä muistitikku tai -kortti verkkolaitteeseen. Aluksilla on kuitenkin muistitikkuja käytössä, mutta niiden käyttö on rajattu tiettyjen laitteiden datan tiedonsiirtoon. Alus D:llä on käytössä ”USB-pesukoneet”, joita käytetään ennen kuin muistitikku kytketään tietokoneeseen, mikä puolestaan varmistaa muistitikun olevan moitteeton. Osalla aluksista on käytössä laitekohtaisia muistitikkuja, mutta tikkujen virus- ja haittaohjelmista ei varmistuta ennen kuin ne kiinnitetään mittaustuloksia analysoivaan laitteeseen tai tietokoneeseen.

Aluksilla otettujen valokuvien siirto tapahtuu yleensä sähköpostin tai Bluetoothin kautta tietokoneelle ja palvelimelle. Tämä tapahtuma kertoo, että konepäällystöä on ohjeistettu toimimaan kyseisellä tavalla, ja mikä myös kertoo, että kyberhygieniaa on lisätty aluksilla. Jos omalla puhelimella otetaan kuitenkin kuvia, lisää se riskejä tiedonsiirtovaiheessa. Otetut kuvat saattavat yllättäen kadota puhelimen kansioista, puhelin saattaa hajota tai puhelimessa saattaa olla haittaohjelma tai virus, koska oma henkilökohtainen puhelin ei välttämättä ole suojattu virustorjuntaohjelmalla.

Oma sähköpostikaan ei välttämättä ole turvallisin vaihtoehto, koska niin kuin tietokoneissa niin älypuhelimissa, saattaa sovelluksissa piillä haittaohjelmia taustalla odottaen hyökkäyskäskyä. Bluetoothin välityksellä henkilökohtainen puhelin kytkeytyy aluksen tiettyyn tietokoneeseen kuvien lähetysvaiheessa, mikä altistaa aluksen tietokoneen uhkalle. Aluksilla käytetään pääsääntöisesti yrityksen kameroita kuvien ottamiseen, ja tämän jälkeen ne siirretään turvallisesti tietokoneelle joko muistikortin tai johtimen kautta. Alus B kuitenkin mainitsi, että viimeisenä vaihtoehtona kuvien siirtämistä varten henkilökohtainen puhelin voidaan kytkeä koneeseen, jotta kuvat saadaan tallennettua palvelimelle. Alus C mainitsi, että puhelimia tai kameroita ei saa kytkeä tietokoneisiin, mutta tätä toimintaa ei valvota. Alus F ilmoitti, että heillä ei ole rajoituksia lainkaan puhelimen tai kameran kytkemisestä tietokoneeseen. Tämä altistaa aluksien tietokoneet lukuisille uhkille.

Verkkorikollisuus muuttuu jatkuvasti, niin miksi koulutuksia pidetään harvoin tai niitä ei järjestetä lainkaan? Kyberturvallisuustaidot eivät voi karttua, jos niihin ei kiinnitetä tarpeeksi huomiota eikä henkilöstöä kouluteta sitä varten riittävän usein. Haastatteluiden perusteella voidaan todeta, että

kyberturvallisuuskoulutuksia järjestetään varsin heikosti ja niiden pääpaino on päällystön kouluttamisessa. Taustalla tässä voidaan tosin pitää, etteivät kaikki saa oikeuksia järjestelmiin, sillä se minimoi riskejä, mutta toisaalta kasvattaa päällystön ja miehistön välistä kuilua. Koulutuksia tulisi olla useammin ja niiden tulisi olla saatavilla jokaiselle laivahenkilölle, jotta jokainen voi päivittää osaamistaan ja pystyy tiedostamaan omaan alukseen kohdistuvat riskit.

Ainoastaan yhdellä aluksella kyberturvallisuuskoulutuksia järjestetään säännöllisesti, että niillä on jatkumo. Neljällä muulla aluksella koulutuksia on järjestetty kerran tai kaksi, mutta niitä taitoja ei ole ylläpidetty. Yhdellä aluksella koulutuksia ei järjestetä, mutta varustamo huolehtii kyberturvallisuuden tärkeydestä muistuttamalla henkilöstöä. Toisaalta aihe on suhteellisen uusi, joten aiheen kriittisyydelle ei olla vielä havahduttu, että sitä taitoa pitäisi ylläpitää. Kyberhygienia ei tässä vaiheessa toteudu varsin perusteellisesti, jos jokainen työntekijä saa toimia ”järki päässä”, kun virallisia ohjeita ei ole annettu. Maalaisjärjen käyttöä korostetaan tietokoneiden käytössä.

Haastatteluiden perusteella aluksille saapuvien uusien työntekijöiden perehdytykseen ei aina kuulu kyberturvallisuusosio, mikä puolestaan altistaa alukset kyberuhille, sillä uudet työntekijät ovat eniten alttiina kyberhyökkäyksille omalla toiminnallaan. Perehdytyksien laadukkuus ja siihen panostettu aika palvelee positiivisesti jokaista työntekijää ja harvemmin hyvästä perehdytyksestä kiistellään.

Jokainen haastatteluun osallistuneista vahvisti myös, että alus on erittäin riippuvainen varustamon omasta IT-tuesta. Tämä voi johtaa tilanteeseen, jossa alukset eivät kykene toimimaan itsenäisesti, vaan tarvitsevat kyberuhkan tapahtuessa IT-tuen neuvoja. Kaikki haastateltavista vastasivat ”miten toimisit kyberhyökkäyksen kohdatessa ja mistä saisit apua” -kysymykseen, että heidän tulisi olla ensimmäisenä yhteydessä varustamoon, turvallisuuspäällikköön sekä IT-tukeen. On hienoa, että apu löytyy varustamolta, mutta huolestuttavaa, ettei aluksilla osattaisi tilanteen sattuessa tehdä riittäviä toimenpiteitä itsenäisesti. Mitä tapahtuu, kun varustamon IT-tuki on palvelunestohyökkäyksen kohteena tai IT-tukeen ei saada yhteyttä satelliittien kautta?

Muutama haastateltava mainitsi alukselle saapuneen merkillisiä sähköposteja, jotka eivät loppupeleissä johtaneet suurempiin toimenpiteisiin. Tämä osoittaa, että sähköpostin kautta yritetään jatkuvasti päästä käsiksi tietoihin. Kaikki alukset kuitenkin kommentoivat, että sähköpostin välityksellä saapuvia linkkejä tai tiedostoja ei klikata. Riski kuitenkin on olemassa, jos sähköposti tai sen linkki osataan naamioida hyökkääjän puolesta ”varustamolta” tai ”IT-osastolta” saapuneeksi. Tämäkin johtaa tilanteeseen, jossa jokainen tulisi kouluttaa kyberturvallisuutta varten.

Vesikuljetuspoolin mukaan alusten turvallisuustaso vaihtelee nykyisin suhteessa alusten ikään. Usein vanhemmilla aluksilla ei ole verkkoon kytkettyjä laitteita, kun taas uudemmat alukset rakennetaan jo hyödyntämään tätä tekniikkaa. Tässä suhteessa vanhempia aluksia päivitetään jatkuvasti, ja eräs kriittinen paikka on nämä uudet asennukset ja päivitykset. Vesikuljetuspoolin selvityksen mukaan näiden päivitysten dokumentaatio jää usein vajaaksi. Uusien aluksien kyberturvallisuus on usein huomioitu jo järjestelmien rakennusvaiheessa ja käyttöönoton yhteydessä. Uudet alukset sisältävät runsaasti tekniikkaa, jotka mahdollistavat enemmän riskejä, ja vanhat alukset taas sisältävät vähemmän tekniikkaa, joten niistä koituu vähemmän riskejä. Toisaalta uusissa aluksissa osataan hallita paremmin riskejä. Henkilöstön iällä ei ole niin suurta merkitystä kuin innokkuudella tehdä ja kokeilla asioita ja tuoda alukselle esimerkiksi uusia laitteita. Nämä jälkiasennukset saattavat olla riski kyberturvallisuudelle. Vesikuljetuspoolin selvitystä tehdessä on sanottu, että suurin riski on uusi alus, jossa on paljon tekniikkaa, ja uudella aluksella oleva innokas bittinikkari, joka asentaa ja korjaa itse aluksen laitteita dokumentoimatta yhtäkään niistä.

Kyberuhkia ei välttämättä nähdä vielä tärkeänä asiana, että siihen puututtaisiin tai sitä ei nähdä vielä ongelmana, varsinkaan ”oman laivan” ongelmana. Mahdollista on myös, että aluksilla ei ole riittäviä resursseja investoida kyberturvallisuuden takaaviin laitteisiin tai koulutuksiin. ”Millaisia uhkia laivaanne voisi kohdistua konehuoneen näkökulmasta” -kysymys, keräsi vastauksia, jossa tiedostetaan todennäköisimmät uhkat. Lähes jokainen haastateltava kommentoi, että pahin mahdollinen tilanne olisi, jos aluksen koneissa havaittaisi virus tai haittaohjelma, jonka seurauksena tietoliikenne häiriintyisi.

6.2 Inhimillisen tekijän vaikutus

Vesikuljetuspoolin haastattelusta ilmeni, että inhimillinen tekijä korostuu jokaisella aluksella tekniikkaa käyttävien jokapäiväisissä työtavoissa. Tähän liittyvät mm. kirjautumisasetukset, salasanojen käyttö, omien muistivälineiden käyttö, virustarkistukset ja työkoneiden käyttö omiin tarkoituksiin. Näissä tavoissa on riski oikaista helppokäyttöisyyden nimissä. Tätä tosin korjaa hyvin laaditut varustamo-ohjeet, mutta jokaisella varustamolla niitä ei ole toteutettu asianmukaisesti. Asiaa voidaan parantaa jonkin verran jatkuvalla kyberturvallisuuskoulutuksella.

”Salasanoja on miljoonia eri järjestelmiin”, kuvaa tämän hetken tilannetta ja järjestelmien siirtymävaihetta kohti autonomisia aluksia. Tämä voi johtaa tilanteisiin, joissa salasanat kirjoitetaan lapuille, jottei niitä tarvitse muistaa. Tällöin salasanat ovat alinomaa myös sellaisessa paikassa, josta ne löydetään vaivatta tai ne ovat näkyvillä esim. Post-it -lapuilla. Salasanojen säilyttäminen esillä tai helposti löydettävässä paikassa, auttaa työntekijöitä vähentämään muistamisesta aiheutuvaa työkuormaa, mutta vaikuttaa negatiivisesti kyberturvallisuuteen. Vain kahdella aluksella mainittiin salasanojen merkkien pituudesta. Näillä aluksilla kaikkien salasanojen tulee olla riittävän pitkiä, ja niitä tulee päivittää tietyin määräajoin. Tietokoneen automaattinen muistutusviesti auttaa työntekijöitä muistamaan vaihtaa salasanat tarpeeksi usein.

Jokainen päällystöön kuuluva joutuu suorittamaan MRM[23]-kurssin osana koulutustaan. MRM-kurssilla käydään läpi inhimillistä tekijää, ja kurssin suoritettua hyväksytysti, siitä jaetaan sertifikaatti. Tämä on ainoa merenkulkijoille suunnattu koulutus, jossa inhimillistä tekijää painotetaan työnteossa. Koska koulutus on kertaluonteinen, koulutuksen jälkeen tulisi työntekijöitä muistuttaa asian kriittisyydestä. Inhimillisen tekijän mukaan ottaminen kyberturvallisuus-, palo- ja pelastusharjoituksiin, antaisi uutta perspektiiviä niitä suunniteltaessa ja suorittaessa.

Jos aluksella kommunikointi jää vähäiseksi, tai se painottuu ainoastaan työtehtävään, omasta tehdystä virheestä ei välttämättä uskalleta sanoa tai sitä

[23] Maritime Resource Management

yritetään piilottaa. Tällöin virheen tapahtuessa luotetaan sokeasti siihen, että kaikki järjestyy tai siitä ei jää kiinni.

Oletuksen määrä korostuu tilanteessa, jossa pidetään itsestään selvyytenä uuden työntekijän tietävän tietojärjestelmistä. Koska osan aluksista perehdytyskierrokseen ei kuulu kyberturvallisuusosio, eivät uudet työntekijät välttämättä tiedä, miten kyseisen aluksen tietokoneita tai älylaitteita saa käyttää. Jos työntekijälle ei tuoda ilmi, kuinka laitteita käytetään, ei voida olla varmoja osaako henkilö käyttää laitteita niin kuin niitä halutaan käytettävän. Tämäkin voi juontaa juurensa oletukseen, että nykypäivänä kaikki osaavat käyttää tietokoneita, ja todennäköisesti koulussa tai aiemmassa työpaikassa on suoritettu kurssi aiheesta. Lisäksi tietojärjestelmien haastavuutena voidaan pitää sitä, ettei kehdata sanoa hallitsevansa työssä käytettävää ohjelmaa. (Teperi 2022).

Omia puhelimia saa käyttää jokaisessa aluksessa, eikä konehuonetta ole rajattu tästä pois. Kuvia voidaan ottaa konehuoneessa, mutta niiden jakamisesta on ohjeita. Kuvia tosin saatetaan lähettää ottamisen jälkeen viestisovelluksien välityksellä ystäville, perheelle tai vahingossa jopa sosiaaliseen mediaan. Tämä ei välttämättä tarjoa alukselle mairittelevaa kuvaa, jos kriittinen kuva päätyy Internettiin. Monet haastateltavat mainitsivat, että puhelimia ei saisi käyttää työaikana, mutta niitä kuitenkin käytetään. Tämä johtaa tilanteeseen, jossa varustamon ohjeita ei noudateta. Tämä luo johtopäätöksen, että joko ohjeet ovat olleet heikkoja, tai niitä on ollut haasteellista suhteuttaa aluksen käyttöön. Vaihtoehtona tälle myös voidaan todeta, että aluksen henkilökunta ei välttämättä halua toimia tämän ohjeistuksen mukaan.

Nuorten keskuudessa suosittu Snapchat[24]-sovellus, sallii kuvan ottamisen missä ja milloin vain. Kuvan jakaminen sen sijaan tarvitsee Internet-yhteyden. Jos kuvan ottaja ei ole valppaana, omasta naamasta otettuun kuvaan saattaa mahtua osa myös kriittisestä laitteesta. Koska algoritmi saattaa ”haistella” otettua ja lähetettyä kuvaa, saattaa se tunnistaa kuvan taustalla kriittisen laitteen ja myöhemmin henkilön puhelin täyttyy kriittisen laitteen varaosista. Koska lähetetty kuva saattaa päätyä myös sellaisille henkilöille, joille kuva ei

[24] Viesti- ja kuvasovellus, jossa valokuva jaetaan usein ystävälle tai ystäväryhmälle. Jaettu kuva näkyy ystävän puhelimessa tietyn ajan, tai se voidaan tallentaa omaan puhelimeen tai pilvipalveluun.

kuulu, riskit vain jatkavat kasvuaan. Algoritmin käyttäytyminen myös aluksen tietokoneilla, esimerkiksi työkaluja tilatessa, voi tarjota erikoisia ratkaisuja tietokoneen käyttäjälle.

Kahdella aluksella on käytössä kulkulupajärjestelmä, ja muilla neljällä aluksella alukseen pääsy on rajoitettu laakonkivahdin ja/ tai videovalvonnan avulla. Tällä perusteella voidaan todeta, että alukseen pääsy on verrattain yksinkertaisesti järjestetty. Haastatteluissa kävi ilmi, että vaikka aluksella olisi kulkulupajärjestelmä, saattaa henkilökunnalta vahingossa tai helppokäyttöisyyden nimissä, jäädä ovia lukitsematta tai ne jäävät kokonaan auki, jolloin joko matkustajia tai urakoitsijoita saattaa päästä heiltä evätylle alueelle. Lähes kuka vain voi naamioitua esimerkiksi IT-asiantuntijaksi ja näyttää lupalappua laakonkivahdille, ja teeskennellä olevansa ”päällikön” toimesta aluksella, voivat riskit moninkertaistua. Mahdollisilla hakkereilla on vain mielikuvitus rajana, jos haluavat saada dataa käsiinsä aluksella. Ihmiset ovat sitä paitsi luottavaisia näkemäänsä ja kuulemaansa. Täytyy kuitenkin ottaa huomioon, että satamiin ja satama-alueelle pääsy on haastavaa ilman kulkulupaa.

Pääsääntöisesti aluksilla pyritään välttämään ylitöiden tekoa, mutta niitä joutuu toteuttamaan esimerkiksi konerikon tai ruuman pesun takia. Ylityöt eivät suoranaisesti vaikuta jokaisella työntekijällä väsymykseen, jos unesta pidetään huolta, mutta ylityöt saattavat vaikuttaa keskittymiseen ja työn laatuun. Pitkä ajanjakso vahdinajossa kuormittaa työntekijöitä, jolloin he voivat epähuomiossa klikata väärää linkkiä sähköpostissa tai Internet-sivuilla. Tästä voidaan luoda johtopäätös, että väsyneet ja kuormittuneet työntekijät ovat aina alttiina kyberuhkille ja saattavat päätöksiä tehdessä turvautua laiskoihin ratkaisuihin.

Suurin osa haastateltavista vastasi, että aluksella on miellyttävä työyhteisö. Työyhteisö tulee hyvin toimeen keskenään, mikä puolestaan lisää yhteenkuuluvuuden tunnetta ja sitä, että kollegaan voidaan luottaa. Tämä ei kuitenkaan takaa, ettei konflikteja syntyisi tai ikäviä kommentteja sanottaisi. Sen sijaan ongelmista todennäköisesti osataan puhua rakentavasti työpaikalla.

Haastattelun viimeisenä kysymyksenä oli: ”miten inhimillinen tekijä on otettu huomioon…”, tarjosi hajontaa vastauksissa. Monet haastateltavat vastasivat

asian liittyvän kyberturvallisuuteen, ja perustelivat vastausta tästä näkökulmasta. Sitä ei tiedetä, oliko kysymys liian epämääräinen haastateltavan näkökulmasta, vai oliko haastateltavalla käsitystä, mitä kysymyksellä tarkoitettiin. Toisena vaihtoehtona voidaan pitää, että haastattelija ei osannut esittää kysymystä tarpeeksi selkeästi, jotta siitä olisi syntynyt haluttu vastaus. Inhimillinen tekijä oli tilanteessa selvästi läsnä: haastattelija ei osannut selventää kysymyksen tarkoitusta, eikä haastateltava osannut kyseenalaistaa kysymystä, vaan haastateltava vastasi oman oletuksen kautta kysymykseen. Vaihtoehtona voidaan myös pitää sitä, että haastateltava ei tiennyt mitä inhimillinen tekijä tarkoittaa.

6.3 Kehitysideoita

Jokaisen aluksen tulisi panostaa kyberturvallisuuteen ja koulutuksiin. Koulutukset voisivat olla matalan kynnyksen harjoituksia, jonka jälkeen suoritetaan muutama tehtävä aiheeseen liittyen. Nämä koulutukset voisivat olla vuosittain toteutettavissa, ja lisäksi joka toisen vuoronvaihdon jälkeen/ joka neljäs vuoronvaihto, (esim. sama järjestelmä kuin palo- ja pelastuslautta koulutuksissa) voisi asioista keskustella ryhmässä tai henkilöt voisivat tutustua lyhyisiin kyberturvallisuusvideoihin. Näin ylläpidetään ajankohtaista asiaa tietoisuudessa. Lisäksi ”kyberhyökkäyksen kohdatessa miten toimisit” -tilanteen varalle olisi hyvä olla suunnitelma valmiina, ja kaikki tietokonekäyttäjät osaisivat suorittaa ensiavun tietojärjestelmälle tällaisessa tilanteessa.

Inhimilliset tekijät -harjoituksia tulisi painottaa laivatyössä enemmän. Nämä voisi ottaa yhdeksi kokonaisuudeksi esimerkiksi aluksen paloharjoituksia tai arkirutiineja, jolloin väsymystä, stressiä tai asenteita korostetaan. Aluksilla laitteiden merkintöjä voisi korostaa, ja ne voisivat olla jokaisessa paperissa ja kaaviossa samat. Tällä vältetään riskiä avata esim. väärä venttiili, jonka kautta pystytään todentamaan oikea laite ja avattava venttiili. Potentiaalisena vaihtoehtona voidaan inhimillistä tekijää suorittaa tietokone- tai virtuaaliympäristössä, jossa henkilön kapasiteettia seurataan paineen alla tai hätätilanteessa.

Alus E mainitsi, että: ”yksikin tunkeutumisyritys on liikaa”, tulisi olla jokaisen aluksen ja varustamon motto. Tällä pystytään varmistamaan kyberturvallisuuden kriittisyys koko alalla ja näkemään se yhteisenä ongelmana, eikä niinkään

jokaisen yksittäisenä esteenä. Varustamot voisivat suunnitella kyberturvallisuusohjeet yhdessä samankaltaisiksi, ja keskustella, millainen toimintasuunnitelma toimii ja millainen malli tulee sivuuttaa. Tämä auttaisi myös työpaikkaa vaihtavia työntekijöitä (varustamosta tai aluksesta toiseen) otaksumaan kyberturvallisuustaidot selkeämmin, kun kaikilla on samat ohjeet.

Jos kyberturvallisuusohjeet ovat luotu vuosi tai kaksi sitten, niiden paikkaansa pidettävyyttä ja ajankohtaisuutta olisi tärkeää tässä vaiheessa uudelleen arvioida. Kyberturvallisuus ja sen uhkat muuttuvat vauhdilla, joten ohjeiden tulee olla päivitettyjä tilanteiden tasalle. Alukset voisivat ottaa käytäntöön toiminnan, jossa varustamon IT-osasto tai varmistettu ulkopuolinen asiantuntija tulee viikoksi tai kahdeksi arvioimaan aluksen kyberhygieniataitoja, jonka perusteella voidaan varustamossa tehdä muutoksia, luoda uusia ohjeita tai päivityksiä rutiineihin. Tässä tilanteessa varustamon IT-asiantuntija tai varmistettu ulkopuolinen asiantuntija kertoisi parannusehdotuksia alukselle. Tämä olisi varustamon oma tilannekatsaus tilanteelle.

6.4 Opinnäytetyön jatkoideoita

Tietojärjestelmien haavoittuvuuksia joudutaan korjaamaan säännöllisesti päivittämällä järjestelmiä ja sovelluksia. Tutkimuksen aikana nousi esiin, että kulussa olevan aluksen järjestelmien päivittäminen ei ole yhtä yksinkertaista kuin maaorganisaation toimistokoneiden päivittäminen. Tämän prosessin kehittäminen edellyttäisi jatkotutkimuksia, jotka voisivat nostaa tutkimatonta tietoa esiin, että saadaan laajempi otos tämän hetken kyberturvallisuudesta ja sen taidoista aluksilla ja varustamoissa.

Voidaan tutkia esimerkiksi, millaisia päivityksiä aluksen IT-osasto suorittaa laitteille ja kuinka ne toteutetaan. Jatkokysymyksenä tähän voidaan sisällyttää, miten inhimillinen tekijä vaikuttaa IT-osaston päivityksiin, ja miten ne on otettu huomioon. Tämän kautta nähtäisiin, miten hyvin laitteet ovat ajan tasalla, ja kenellä kaikilla IT-osaston henkilöllä, on luvat laitteiden päivittämiseen. Tästä voidaan myös myöhemmin todeta, kuinka hyvin laitteet, sovellukset ja järjestelmät ovat uhkilta suojassa, ja kuinka hyvin päivityksien suorittajat ovat kyberhygieniataitoisia.

Vaihtoehtoisena tutkimuskysymyksenä voidaan esittää: Kuinka hyvin varustamo ja alukset kommunikoivat keskenään, ja kuinka paljon on hajontaa ohjeiden noudattamisessa ja toteutuksessa. Tähän voidaan vielä lisätä jatkokysymys: kuinka kattavia ovat varustamoiden järjestämät kyberturvallisuuskoulutukset? Tästä voidaan saada selville, miten varustamo ja alukset kommunikoivat keskenään, ja millainen on niiden keskinäinen vuorovaikutus. Tällä pystytään hahmottamaan, miten varustamon rooli näyttäytyy taustalla, kun aluksella noudatetaan ohjeita tai ne jätetään huomiotta. Kysymys peilaa myös inhimilliseen tekijään. Kun jokaisella aluksella alkaa olla kyberturvallisuuskoulutuksia, voidaan kysyä niiden laatua esimerkiksi kyselytutkimuksen kautta. Tämän kartoituksen jälkeen osataan suorittaa koulutuksia useammin tai koulutuksien laatuun voidaan vaikuttaa.

Kolmantena vaihtoehtona voidaan kysyä täysin kyberturvallisuuteen liittyvä tutkimuskysymys: Kuinka usein aluksen tietojärjestelmiin tehdään penetraatiotestauksia, jotka kertovat haavoittuvuuksista? Tämän jälkeen voidaan todeta, syntyykö haavoittuvuuksia liian usein ja millaisia ovat niiden heikkoudet. Tähän voidaan sijoittaa myös jatkokysymys: miten hyvin Zero Vulnerability näkyy aluksien ja varustamoiden toiminnassa, jonka jälkeen huomataan, onko nollapäivähaavoittuvuuksia nähtävillä, ja kuinka hyvin se toteutuu arkirutiineissa.

Miten inhimilliset tekijät näkyvät konemestareiden ja -päälliköiden työssä? Tällä tutkimuskysymyksellä voidaan haastatella sekä konepäälliköitä että konemestareita, jotta saadaan selvyys miten inhimilliset tekijät on otettu huomioon päällystön osalta. Kysymys ottaa kantaa yksilön toimintaan esimerkiksi konevalvomossa, ja johdattaa lukijan ihmisen toiminnan äärelle. Tästä huomataan myös, miten esimiesten työnteko ja työtehtävien anto vaikuttavat miehistön toimintaan. Tutkimuskysymys selvittää, kuinka tietoisia konepäälliköt ja -mestarit ovat inhimillisestä tekijästä.

6.5 Loppusanat

Kyberhygieniataitoja on lisätty aluksilla ja toimintaa kehitetään jatkuvasti eteenpäin. Asian kriittisyydestä ei sen sijaan painoteta tarpeeksi voimakkaasti. Vaikka uhkatilanteita ei ole aluksilla ollut, ei tarkoita, ettei niin voisi tapahtua. Kyberturvallisuuden riskit ovat tänä päivänä käsinkosketeltavia, ja lähes

päivittäin uutisissa käsitellään näitä uhkatilanteita. Maailmanlaajuisesti hyökkäyksiä tapahtuu tuhansia, ellei kymmeniä tuhansia päivittäin.

LÄHTEET

Ala-Laurinaho A., Asikainen I., Puro V., Teperi A. 2022. Työterveyslaitos. Helsinki. PDF-dokumentti. Saatavissa: https://www.julkari.fi/bitstream/handle/10024/143832/TTL-978-952-391-010-2.pdf?sequence=1&isAllowed=y [viitattu 11.4.2022.]

Boyes H., Isbell R. 2017. Code of Practice – Cyber security for ships. Institution of Engineering and Technology. Lontoo. PDF-dokumentti. Saatavissa: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-for-ships/ [viitattu 3.10.2022.]

Council of the European Union. 2022. EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation. WWW-sivu. Saatavissa: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/ [viitattu 7.12.2022.]

DNV CG. 2021. Class Guideline. Cyber Secure. WWW-sivu. Saatavissa: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html [viitattu 6.10.2022.]

Energia-alan turvallisuusasiantuntija (salassa pidettävä henkilöllisyys). 2022. Haastattelu.

Enisa. 2022. Euroopan Unionin kybertuvallisuusvirasto. WWW-sivu. Saatavissa: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new [viitattu 16.11.2022.]

Hirsjärvi S., Remes P., Sajavaara P. 2009. Tutki ja Kirjoita. 15. Uudistettu painos. Hämeenlinna: Kariston Kirjapaino Oy.

Huoltovarmuuskeskus. 2021. PDF-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/files/a3512a9ae47541a92f002c60c6fa3030dc5327d3/kyberturvallisuus-parhaat-kaytannot-aluksille.pdf [viitattu 8.4.2022.]

IACS. WWW-sivu. Saatavissa: https://iacs.org.uk/publications/unified-requirements/ur-e/ [viitattu 5.10.2022.]

IACS. 2022. Recommendation on Cyber Resilience. No 166. PDF-dokumentti. Saatavissa: https://iacs.org.uk/publications/unified-requirements/ur-e/[viitattu 10.10.2022.]

IACS. 2016. On Board Use and Application of Computer based Systems. E22. PDF-dokumentti. Saatavissa: https://iacs.org.uk/publications/unified-requirements/ur-e/ [viitattu 10.10.2022.]

IACS. 2022. Cyber resilience of ships. E26. PDF-dokumentti. Saatavissa: https://iacs.org.uk/publications/unified-requirements/ur-e/ [viitattu 10.10.2022.]

IACS. 2022. Cyber resilience of on-board systems and equipment. E27. PDF-dokumentti. Saatavissa: https://iacs.org.uk/publications/unified-requirements/ur-e/ [viitattu 10.10.2022.]

Inkinen M. 2022. Opas kiristyshaittaohjelmilta suojautumiseksi. PDF-dokumentti. [viitattu 12.9.2022.]

ISSA. 2017. Vision Zero opas. PDF-dokumentti. Saatavissa: https://vision-zero.global/sites/default/files/2022-04/FI-Vision%20Zero%20Guide-Web_0.pdf [viitattu 11.4.2022.]

Kaspersky Daily. 2017. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable Within. WWW-sivu. Saatavissa: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ [viitattu 10.10.2022.]

Kaspersky. Kyberhygienia. WWW-sivu. Saatavissa: https://www.kaspersky.fi/resource-center/preemptive-safety/cyber-hygiene-habits [viitattu 10.10.2022.]

Kaspersky. Webcam Hacking: Can Your Webcam Spy on You. Artikkeli. WWW-sivu. Saatavissa:https://www.kaspersky.com/resource-center/threats/webcam-hacking [viitattu 9.12.2022.]

Kurittu A., Kankaala L., Jauhiainen J. 2021. Spotify. Turvakäräjät–Kansalaisen kyberturvallisuus. Podcast. [viitattu 20.08.2022.]

Latva-Teikari, K. 2021. YLE. Uutinen. Saatavissa: https://yle.fi/uutiset/3-12026736 [viitattu 10.4.2022.]

Limnell J., Majewski K., Salminen M. 2014. Kyberturvallisuus. Docendo Oy.

Microsoftin Digitaalinen puolustusraportti. 2021. PDF-dokumentti. [viitattu 30.9.2022.]

Nevalainen, A. 2022. YLE. Uutinen. Saatavissa: https://yle.fi/uutiset/3-12292088 [viitattu 10.4.2022.]

Riikonen J. 2022. Algoritmi tietää sinusta kaiken. *Tiede.* 2/2022. Artikkeli. [viitattu 13.9.2022.]

Smith T. 2020. I got my file from Clearview AI, and it freaked me out. Artikkeli. Saatavissa: https://onezero.medium.com/i-got-my-file-from-clearview-ai-and-it-freaked-me-out-33ca28b5d6d4 [viitattu 13.9.2022.]

Subsystem. PC mag. WWW-sivu. Saatavissa: https://www.pcmag.com/encyclopedia/term/subsystem [viitattu 10.10.2022.]

Suomen Varustamot. WWW-sivu. Saatavissa: https://shipowners.fi [viitattu 12.10.2022.]

Teperi A., Puro V. 2022. HF-Tool™-koulutus. Sea safety II -projekti.

Traficom. 2022. Kybersää. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybersää%2C%20syyskuu%202022.pdf [viitattu 7.11.2022.]

Traficom. 2022. Toimintaohje–Palvelunestohyökkäys. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/PalvelunestohyökkäysToimintaohje.pdf [viitattu 6.11.2022.]

Traficom. 2020. WWW-sivusto. Saatavissa: https://www.traficom.fi/fi/liikenne/merenkulku/ism-turvallisuusjohtamisjarjestelma [viitattu 9.4.2022.]

Tuomaala, E. 2021.YLE. Uutinen. Saatavissa: https://yle.fi/uutiset/3-11894409 [viitattu 10.4.2022.]

Vesikuljetuspooli. 2022. Sähköpostihaastattelu.

Wilson D.C. 2021. Cybersecurity. Massachusetts Institute of Technology. The MIT Press.

LIITE1

Haastattelukysymykset konemestareille/-päälliköille

1. Miten kyberturvallisuus näkyy teidän aluksessanne?
2. Kuinka paljon panostatte kyberturvallisuuteen ja mikä on varustamon rooli? Miten turvallisuus on ratkaistu kyberturvallisuuden osalta?
3. Kuinka usein pidetään koulutuksia päällystölle ja miehistölle aiheesta? Entä ylläpidetäänkö näitä taitoja säännöllisesti? (Huolehtiiko varustamo/päällikkö/työntekijät itse näistä koulutusasioista?)
4. Kuinka perehdytätte uuden työntekijän aluksen tietojärjestelmiin? Mitä kaikkea työntekijät saavat tehdä päätelaitteella ja muilla älylaitteilla?
5. Saako työntekijät pitää omia puhelimiaan mukana, kun he liikkuvat konehuoneessa? Onko kameran käytöstä ja kuvien jakamisesta rajoitettu? Onko älylaitteiden käyttöä rajoitettu?
6. Onko rajoituksia mm. muistitikkujen käytöstä, puhelimien lataamisesta/kytkemisestä aluksen tietokoneeseen? Miten tiedonsiirto (esim. kuvat tietokoneelle) on järjestetty?
7. Kuinka konevalvomoon pääsy on rajoitettu? Onko kulkuluvat? Ketkä kaikki pääsevät?
8. Millaisia kyberuhkia laivaanne voisi kohdistua? (3)
9. Onko ollut uhkatilanteita? jos on niin, minkä takia tilanne syntyi? Mikä oli sen aiheuttaja? ja onko niistä raportoitu eteenpäin?
10. Kyberhyökkäyksen kohdatessa miten toimisit? Tiedätkö mistä saat apua? (esim. laiva ei pääse lastaamaan, tai laiva on jumissa satamassa, tai ei ole puhelinyhteyttä/wifiä) (Onko suunnitelma paperisena?)
11. Onko teillä satelliittiyhteys varustamon/laivojenne kanssa? Miten sen käyttö on suojattu?
12. (Miten vastuunjakaminen on huolehdittu? Onko kyberturvallisuus lisätty toimenkuvaan aluksella? / onko tehtävälistalla henkilöä, joka tarkistaa laitteiden päivitykset, palomuurit, suojaukset ja varmuuskopioinnin?)
13. (Kuinka usein ulkoistatte osan työmäärästänne kolmannelle osapuolelle? Millaisiin asioihin kolmas osapuoli pääsee käsiksi ja millaiset oikeudet he saavat? Miten kolmas osapuoli tarkastetaan? Onko hän/he luotettavia ja vastuullisia?)
14. Millaiset työajat teillä on? saako ylitöitä tehdä ja tehdäänkö niitä?
15. Millainen työyhteisö teillä? tuleeko kaikki toimeen kaikkien kanssa? miten kulttuurierot on otettu huomioon?
16. Miten inhimilliset tekijät on otettu huomioon, jotta virheitä vältytään?