MERENKULUN KYBERTURVALLISUUS – VARUSTAMOJEN PARHAAT KÄYTÄNNÖT

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuuskeskuksen yhteydessä toimii Huoltovarmuusneuvosto sekä pysyvinä yhteistyöeliminä komitean tapaan toimivia sektoreita ja pooleja. Nämä yhdessä muodostavat Huoltovarmuusorganisaation.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

Julkaisija:	Huoltovarmuusorganisaatio, Vesikuljetuspooli
Teksti:	Teksti perustuu Huoltovarmuusorganisaatioon kuuluvan Vesikuljetuspoolin ja Suomen Varustamot ry:n tilaamaan ja Deductive Labs Ab:n toteuttamaan selvitykseen
Kuvat:	Shutterstock
Taitto:	Up-to-Point Oy
Julkaisu-vuosi:	2021
ISBN:	978-952-7470-04-6

Sisältö

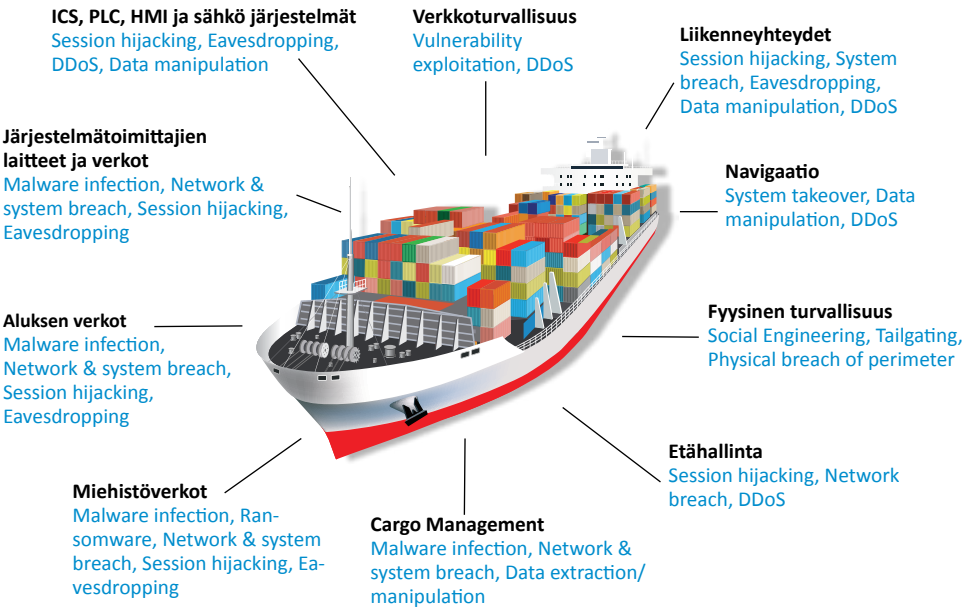
Varustamon kyberturvallisuuden eri osa-alueita ja parhaita käytäntöjä ehdotetaan ja esitetään tässä asiakirjassa seuraavasti:

TAUSTA JA ESITTELY

Merenkulkuala ja kauppa-alukset voivat tuntua epätodennäköisiltä kohteilta kyberhyökkäyksille, mutta merenkulkualan digitalisoitumisen lisääntyessä ja verkkoon liitetyn tietotekniikan (IT), operatiivisen tekniikan lisääntyessä (OT) -järjestelmät, meriteollisuuden ohjausjärjestelmät (ICS) ja mm satelliittiviestintä ovat alttiita verkkorikollisten ja muiden tietoturvallisuutta uhkaavien ryhmien hyökkäyksille. Siksi on kriittistä, että kyberturvallisuutta hallitaan asianmukaisesti merenkulkualalla alusten, miehistön ja rahdin suojaamiseksi mahdollisilta kyberturvallisuusuhkilta ja -hyökkäyksiltä.

Merenkulun kyberturvallisuus on käytäntöjen, menettelyjen, ohjeiden, toimenpiteiden, riskienhallintatoimien, koulutuksien, työkalujen ja tekniikoiden valintoja, joita käytetään koko merenkulkualan ja alusten suojaamiseen.

IT- ja OT-järjestelmiin liittyvät riskit ovat erilaiset siinä mielessä, että IT-järjestelmien riskit vaikuttavat pääasiassa talouteen ja maineeseen, kun taas OT-järjestelmien riskit voivat vaikuttaa turvallisuuteen ja uhata ihmishenkiä, omaisuutta ja ympäristöä, jos riskit toteutuvat.



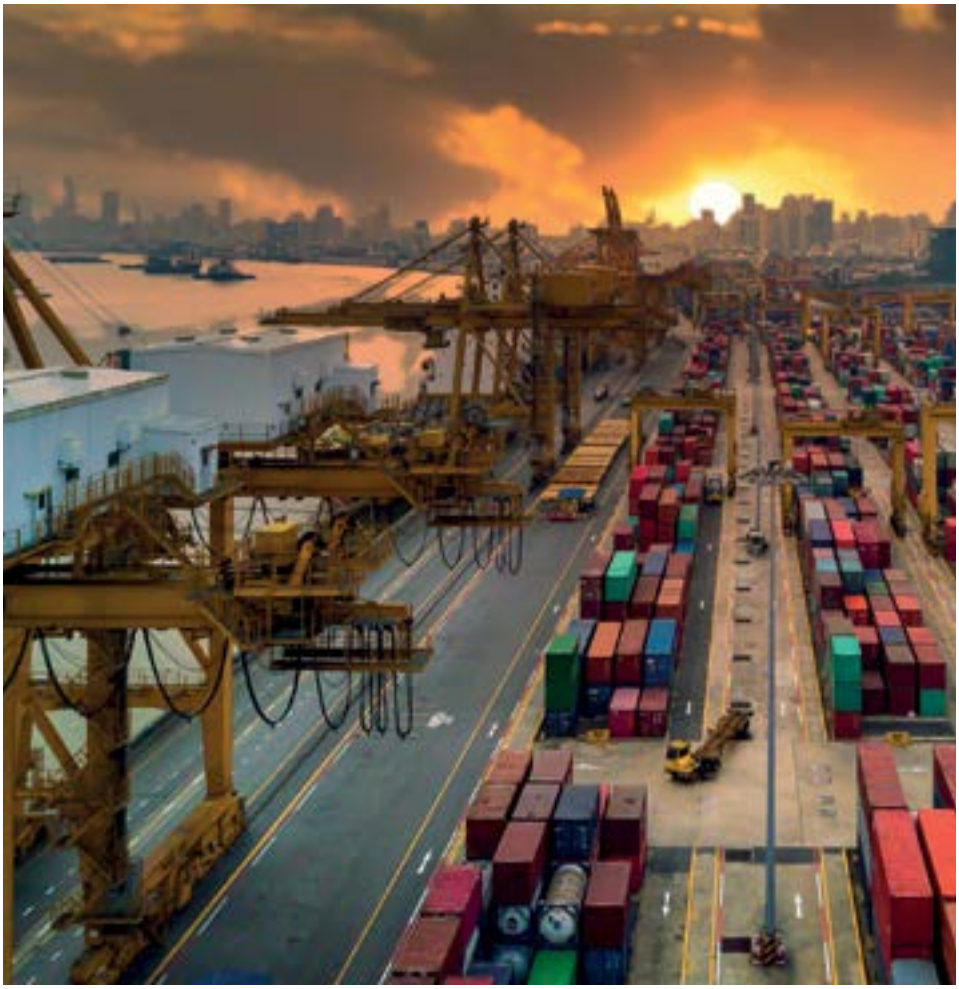
Tammikuussa 2021 Suomen Varustamot ry yhdessä Huoltovarmuuskeskuksen kanssa aloitti hankkeen merenkulkualan aluksien kyberturvallisuuden tilanteen kartoittamiseksi. Suomalainen merenkulun kyberturvallisuusasiantuntija Deductive Labs Ab valittiin toteuttamaan projektin.

Hankkeessa tuotettiin kolme erillistä asiakirjaa, jotka ovat saatavissa kieliversioineen (en, fi, sv) Suomen Varustamot r.y:n tai Huoltovarmuuskeskuksen julkaisu-sivujen kautta: *https://www.huoltovarmuuskeskus.fi/julkaisut* ja *https://shipowners.fi/vastuullisuus/turvallisuus/kyberturvallisuus/*

1. ***Merenkulun kyberturvallisuusraportti – Suomen kauppalaivaston kypsyys (ENG)***, kattava raportti Suomen merenkulkualan nykytilasta

2. ***Merenkulun kyberturvallisuus – Alusten parhaat käytännöt***, yhteenveto havainnoista ja esitys alusten parhaista käytännöistä

3. ***Merenkulun kyberturvallisuus – Varustamon parhaat käytännöt***, yhteenveto havainnoista ja esitys varustamojen parhaista käytännöistä



1. JOHDON TUKI

Ylimmän johdon tuki on ratkaisevan tärkeää organisaation kyberturvallisuuden kehittämisen kannalta. Nämä suositellut toimet auttavat saamaan ylin johto ymmärtämään paremmin ja kehittämään kyberturvallisuutta

Toimenpiteet:

1. Aloita keskustelu kyberturvallisuudesta ylimmän johdon kanssa ja sisällytä kyberturvallisuus johdon agendalle.
2. Sisällytä kyberturvallisuus johdon päätöksentekoprosessiin
3. Käytä riskienhallintaa työkaluna päätöksenteossa
4. Kouluta ylin johto kyberturvallisuudessa

Tavoite:

- Lisääntynyt ymmärrys kyberturvallisuudesta ja organisaation riskeistä
- Päätökset tehdään riskiarvioinneista saatujen tietojen perusteella
- Ylimmän johdon esimerkki ja sitoutuminen kyberturvallisuuden kehittämiseen on ensisijaisen tärkeää koko organisaation kannalta.

Vinkkejä:

Suomen kyberturvallisuuskeskus (NCSC-FI) on julkaissut ylimmän johdon kyberturvallisuusohjeet, joita voidaan käyttää ymmärryksen lisäämiseen

- *https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf*

2. KYBERTURVALLISUUSKOULUTUS

Kyberturvallisuuskoulutus ja tietoisuus ovat tärkeitä koko organisaatiolle ylimmästä johdosta työntekijöihin ja miehistöön.

Toimenpiteet:

1. Järjestä kyberturvallisuuskoulutuksia kaikille työntekijöille.
2. Suorita kyberturvallisuuskoulutuksia säännöllisesti
3. Järjestä kyberturvallisuuskoulutuksia jatkuvana osana yrityksen prosesseja ja kulttuuria

Tavoite:

- Lisääntynyt ymmärrys kyberturvallisuudesta kaikille työntekijöille
- Organisaatio noudattaa IMO: n kyberriskien hallintaa koskevia määräyksiä1
- Lisääntynyt kyberturvallisuuden tietoisuus organisaatiossa

Vinkkejä:

Organisaation kyberturvallisuuden avainhenkilöt voivat auttaa luomaan tarvittavat koulutusmateriaalit. Koulutukset voi tarpeen mukaan myös ulkoistaa kolmannelle osapuolelle. Kyberturvallisuuskoulutusta tulisi tarjota kaikille työntekijöille, myös ylimmälle johdolle.

Eri henkilöstöryhmien kyberturvallisuuteen liittyvät roolit tarvitsevat erilaisia lähestymistapoja ja erilaista koulutusta. Harkitse koulutuksen tarjoamista räätälöidysti tietyille rooleille ja heidän erityisille kyberturvallisuushaasteilleen ja -tarpeilleen.

Koulutuksissa voi käyttää ulkopuolisia kouluttajia ja verkkokoulutusta.

1) https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

3. KYBERTURVALLISUUSMENETTELYT JA OHJEET

Organisaation työntekijöillä ja alusten miehistöllä on oltava selkeät menettelytavat, jotka määrittelevät miten kyberturvallisuutta hallitaan organisaatiossa ja aluksilla.

Toimenpiteet:

Luo käytännölliset menettelytavat, ohjeet työntekijöille ja miehistölle:

1. Menettelytavat organisaation palveluiden ja järjestelmien käytöstä
2. Menettelytavat ulkoisten tietovälineiden käytöstä ja hallinnasta
3. Menettelytavat organisaation järjestelmien hallintaan ja päivityksiin
4. Menettelytavat henkilökohtaisten laitteiden, verkkojen ja Internetin käytöstä
5. Menettelytavat ulkoisten toimittajien etäyhteyksien käytöstä
6. Menettelytavat kyberturvallisuuspoikkeamien hallintaan
7. Menettelytavat kyberturvallisuusharjoituksien järjestämiseksi

Tavoite:

- Organisaation työntekijöillä on dokumentoidut menettelytavat mitä tehdä kyberturvallisuuden hallitsemiseksi.
- Organisaation ja aluksien menettelytavat tukevat ISM/ISPS koodien vaatimuksia

Vinkkejä:

Tee yhteistyötä miehistön, toimittajien ja muiden kolmansien osapuolten kanssa ymmärtääkseen heidän päivittäiset toimintansa ja miten heidän toimintansa vaikuttavat organisaation ja aluksien kyberturvallisuuteen. Sisällytä osapuolet käytännön menettelyjen kehittämiseen, jotka ovat helposti ymmärrettäviä ja noudatettavia. Varustamon kyberturvallisuuskulttuurin luominen on varustamon johdon vastuulla.

4. ORGANISAATION KRIITTISET PALVELUT JA TOIMINNOT

Organisaatiossa ja sen aluksissa käytettyjen kriittisten palveluiden ja toimintojen tunnistaminen ja ymmärtäminen on kriittistä kyberturvallisuuden ymmärtämiselle ja ylläpitämiselle. Organisaation on tunnistettava kaikki kriittiset palvelut ja toiminnot sekä niihin liittyvät IT- ja OT-järjestelmät, jotta voidaan tunnistaa riskit ja mahdolliset vaikutukset palvelujen toimintaan kyberturvallisuushäiriön sattuessa. Tämä sisältää kaikki organisaatiossa käytetyt palvelut ja toiminnot sekä maalla että aluksilla.

Toimenpiteet:

1. Tunnista ja dokumentoi kaikki organisaation kriittiset palvelut ja toiminnot
2. Tunnista ja dokumentoi kaikki kriittisten palvelujen ja toimintojen toimittamiseen liittyvät IT- ja OT-järjestelmät.
3. Aloita perustyökaluilla, kuten laskentataulukoilla ja asiakirjoilla, ja harkitse automaattisten työkalujen käyttöönottoa työn tehostamiseksi

Tavoite:

- Organisaation kriittiset palvelut ja toiminta on kartoitettu
- Organisaation IT- ja OT-järjestelmät on kartoitettu ja dokumentoitu
- Järjestelmäluetteloa käytetään riskienhallintaprosessissa

Vinkkejä:

Kriittisten palveluiden ja toimintojen ja niihin liittyvien IT- ja OT-järjestelmien kartoittaminen on haastavaa ja aikaa vaativa tehtävä. Suosittelemme käyttämän DCSA:n ”Asset Management and Risk Register Templates Reading Guide” -opasta, joka sisältää käyttökelpoisia malleja joita voi käyttää järjestelmäluetteloiden luomiseen ja riskienhallinnan organisoimiseen. Aloita tunnistamalla kriittiset järjestelmät, joilla on suuri vaikutus alusten turvallisuuteen ja toimintaan.

	Asset List							
	Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.							
Asset Serial	Asset	Type/Description	Version	Owner	Custodian	Location	Date of Last Chek	Criticality
1	Del Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

5. RISKIEN ARVIOINTI

Kun organisaation kriittiset palvelut ja niihin liittyvät IT- ja OT-järjestelmät on tunnistettu ja dokumentoitu, on tehtävä riskinarviointi mahdollisten uhkien, riskien ja haavoittuvuuksien tunnistamiseksi. Riskien arvioinnissa tulee ottaa huomioon kaikki mahdolliset tilanteet ja tapahtumat jotka voivat vaikuttaa organisaation ja alusten toimintaan ja turvallisuuteen.

Toimenpiteet:

1. Arvioi tunnistettujen palvelujen, toimintojen ja järjestelmien kyberturvallisuusriskit
2. Tunnista ja dokumentoi riskien korjaamiseen tarvittavat toimenpiteet.
3. Luo toimintasuunnitelma riskinarvioinnissa tunnistetuista toimenpiteistä
4. Huomioi kyberturvallisuus ja kyberriskien hallinta osana turvallisuusjohtamisjärjestelmää (SMS/ISM)

Tavoite:

- Organisaation kriittisiin palveluihin ja toimintoihin liittyvät riskit on tunnistettu ja dokumentoitu
- Toimintasuunnitelma tunnistettujen riskien korjaamiseksi on dokumentoitu
- Organisaation riskienhallintaprocessi noudattaa IMO:n vaatimuksia merenkulun kyberturvallisuusriskien hallinnasta

Vinkkejä:

Julkisesti saatavilla on monia erilaisia malleja ja laskentataulukoita, joiden avulla voidaan aloittaa kyberriskien hallintaan tarvittavat toimenpiteet. Suosittelemme käyttämään DCSAs "***Asset Management and Risk Register Templates Reading Guide***"[2] ohjeita jotka sisältävät malleja IT- ja OT-järjestelmien dokumentointiin ja riskienhallinnan tekoon. Riskienhallintaprosessin kypsyessä voidaan käyttää muita työkaluja.

2) https://dcsa.org/wp-content/uploads/2020/03/DCSA_Asset-Management-and-Risk-Register-Templates-Reading-Guide.pdf

6. RISKIEN HALLINTASUUNNITELMA

Kun kriittiset palvelut, toiminnot ja niihin liittyvät järjestelmät sekä niihin liittyvät riskit on tunnistettu, seuraava vaihe on toteuttaa riskienhallintasuunnitelma, joka sisältää toimenpiteitä ja korjauksia tunnistettujen riskien hallitsemiseksi.

Tämä vaihe perustuu riskinarviointiin, ja siinä hahmotellaan sekä menettelyt että tekniset toimenpiteet, jotka on toteutettava riskien minimoimiseksi ja korjaamiseksi.

Toimenpiteet:

1. Luo projektisuunnitelma riskienhallintasuunnitelman toimenpiteille.
2. Varmista että projektisuunnitelmassa yksilöidään riskin korjaamiseksi tarvittavat vaiheet ja toimet, mitä resursseja tarvitaan, kuka on vastuussa, mikä on aikataulu ja että budjetti on hyväksytty
3. Toteuta projektisuunnitelma

Tavoite:

- Projektisuunnitelma on dokumentoitu ja pantu täytäntöön
- Tunnistetut riskit on korjattu

Vinkkejä:

Käsittele toimenpiteitä projekteina, johon sisältyy dokumentoituja suunnitelmia ja tehtäviä, joita voidaan seurata. Sinun ei tarvitse keksiä pyörää uudelleen, käytä työn hallintaan yrityksen perustamia projektinhallinnan menetelmiä ja -työkaluja.

Riskienhallintaan voi käyttää ulkopuolisia asiantuntijoita työn tehostamiseksi.

7. KYBERTURVALLISUUSARKKITEHTUURI

Organisaation ja alusten dokumentoitu kyberturvallisuusarkkitehtuuri määrittelee kuinka kyberturvallisuus toteutetaan organisaatiossa ja aluksilla. Kyberturvallisuusarkkitehtuuri auttaa varmistamaan, että kyberturvallisuuden valvonta dokumentoidaan ja toteutetaan standardoidulla tavalla organisaatiossa ja aluksilla.

Toimenpiteet:

1. Määrittele kyberturvallisuusarkktehtuuri joka kuvaa miten kyberturvallisuus toteutetaan organisaatioissa ja aluksilla
2. Määrittele jokaiselle alukselle kybertruvallisuussunnitelma (CSP - Cybersecurity Plan), joka perustuu kyberturvallisuusarkkitehtuuriin ja aluksien tekniseen ympäristöön ja tarpeisiin
3. Jokaiselle alukselle joka perustuu dokumentoituun arkkitehtuuriin ja määrittelee miten aluksella käytetyt järjestelmät turvataan
4. Yhdistä kyberturvallisuussuunnitelma dokumentoituihin kyberturvallisuusmenettelyihin

Tavoite:

- Kyberturvallisuusarkkitehtuuri on dokumentoitu ja kuvaa kuinka kyberturvallisuus toteutetaan organisaatiossa ja aluksilla ja määrittelee tarvittavat toimenpiteet kyberturvallisuuden parantamiseksi
- Kyberturvallisuusarkkitehtuuria käytetään aluksien kyberturvallisuussunnitelmien määrittelyssä

Vinkkejä:

Aluksen kyberturvallisuussuunnitelma voidaan sisällyttää olemassa oleviin turvasuunnitelmiin (SSP), mutta suosittelemme erillisen kyberturvallisuussuunnitelman (CSP) luomista asiakirjojen pitämiseksi erillään, koska SSP keskittyy perinteisesti enemmän alusten fyysiseen turvallisuuteen. Kyberturvallisuuden lisääminen perinteiseen turvasuunnitelmaan(SSP) tekee siitä monimutkaisemman ja vaikeamman ymmärtää ja omaksua. Kyberturvallisuussuunnitelma on yhdistettävä dokumentoitujen kyberturvallisuusmenettelyjen kanssa.

8. TOIMITUSKETJUN KYBERTURVALLISUUS

Merenkulkuala on erittäin riippuvainen useista ulkoisista toimittajista ja kolmansista osapuolista, ja niillä on tärkeä rooli alusten hallinnassa ja toiminnassa. Toimittajilla on yleensä vastuu alusten kriittisten järjestelmien, kuten ECDIS-järjestelmien, moottoreiden ja virranhallinnan, lastinhallintajärjestelmien, GPS-järjestelmien, PLC:n, antureiden jne. hallinnasta ja valvonnasta.

Toimenpiteet:

1. Tunnista kaikki toimittajat
2. Suorita toimittajan riskinarviointi
3. Luo toimittajan kyberturvallisuusvaatimukset
4. Sisällytä kyberturvallisuusvaatimukset toimittajasopimuksiin
5. Varmista, että toimittajasopimuksiin sisältyy oikeus kyberturvallisuuden tarkastukseen

Tavoite:

- Toimittajat on tunnistettu ja dokumentoitu
- Toimittajien kyberturvallisuusvaatimukset on dokumentoitu
- Toimitusketjun kyberturvallisuus on hallittu

Vinkkejä:

Aloita tunnistamalla ja dokumentoimalla kaikki toimittajat, jotka tarjoavat järjestelmiä ja palveluita aluksille. Määritä tarvittavat kyberturvallisuusvaatimukset ja ohjeet riskinarviointien perusteella.

Hyvät ja käytännölliset ohjeet toimitusketjun turvallisuudesta löytyvät mm. UK NCSC:n toimitusketjun turvaohjeista[3].

3) https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

9. KYBERTURVALLISUUSTAPAHTUMIEN HALLINTA, REAGOINTI JA TOIPUMINEN

Tehokkaan kyberturvallisuustapahtumien hallinnan avulla organisaatiot voivat tunnistaa kyberturvallisuuspoikkeamat ja reagoida nopeasti tapahtumaan ja toipua siitä, jotta tapahtuman vaikutus ei vaikuta aluksen turvallisuuteen tai kulkuun.

Toimenpiteet:

1. Luo kyberturvallisuuden tapahtumien hallintamenettely. Menettelyssä tulisi kuvata, mitä toimia työntekijät ja miehistö tulisi tehdä kyberturvallisuuspoikkeamien sattuessa ja miten kriittisten järjestelmien lokeja analysoidaan ja seurataan.
2. Varmista, että ympäristöä seurataan ja tapahtumat kirjataan tapahtumien havaitsemisen helpottamiseksi
3. Järjestä kyberharjoituksia kouluttaaksesi työntekijöitä ja miehistöä reagoimaan kyberturvallisuustapahtumiin

Tavoite:

- Organisaatio havaitsee, reagoi ja toipuu kyberturvallisuustapahtumista
- Kyberturvallisuusharjoituksia tehdään säännöllisesti

Vinkkejä:

Aloita luomalla kyberturvallisuustapahtumien hallintamenettelyjä, jotka kuvaavat mitä työntekijät ja alusten miehistö tulisi tehdä kyberturvallisuustapahtuman sattuessa. Menettelyjen tulisi sisältää ohjeita miten kyberturvallisuustapahtumia havaitaan, miten niihin reagoidaan ja miten niistä toivutaan takaisin normaalitilaan.

Kyberturvallisuuskeskus on julkaissut ohjeet kyberharjoitusten järjestämiseen:

- *https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf*

Kyberharjoituksien järjestäminen on hyvä ja tehokas tapa kouluttaa työntekijöitä miehistöä reagoimaan kyberturvallisuustapahtumiin.

10. KYBERTURVALLISUUSSTANDARDIT JA KEHYKSET

ISO 27001 on yleinen standardi tietoturvan hallintajärjestelmän (ISMS) luomiseksi, mutta standardi ei ole täysin yhdenmukainen merenkulkualan vaatimuksien kanssa. Standardit, kuten NIST-kyberturvallisuuden kehys (NIST CSF) ja ISA / IEC 62443 Teollisuuden automaatio- ja ohjausjärjestelmien turvallisuus, ovat paremmin yhdenmukaistettuja ja niihin viitataan usein merialan kyberturvallisuuden säädöksissä ja ohjeistuksissa.

Toimenpiteet:

1. Valitse organisaatiollesi sopiva kyberturvallisuusstandardi tai -kehys
2. Käytä riskienhallintaa tarvittavien toimenpiteiden ja toimenpiteiden tunnistamiseen.
3. Määrittele kyberturvallisuuskäytännöt, -prosessit ja -menettelyt valitun kehyksen perusteella.

Tavoite:

- Organisaatio käyttää vakiintunutta kyberturvallisuuden standardia tai kehystä

Vinkkejä:

Saatavilla on monia erilaisia standardeja ja kehyksiä, joita voidaan käyttää ohjaamaan organisaation kyberturvallisuustoimia. Useimmin käytetyt ovat ISO 27001, ISA / IEC 62443 ja NIST-kyberturvallisuuskehys.

Suosittelemme, että organisaatio investoi aikaa tai ottaa yhteyttä ulkoisiin resursseihin ja asiantuntijoihin, saadakseen käsityksen erilaisista standardeista ja kehyksistä ja selvittääkseen, mikä niistä sopii parhaiten omaan ympäristöön ja tarpeisiin.

Käyttämällä vakiintuneita standardeja kyberturvallisuustoiminnasta tulee standardoitua ja helpompaa toteuttaa, ylläpitää ja tarkastaa.

Kyberturvallisuusstandardien toteutukseen voi käyttää ulkopuolisia asiantuntijoita työn tehostamiseksi.

11. YHTEISTYÖ ULKOISTEN OSAPUOLIEN KANSSA

Viimeinen suositus, jos se katsotaan tarpeelliseksi, on saada ulkopuolista apua alan järjestöiltä, varustamoilta, yhdistyksiltä tai kokeneilta kyberturvallisuuskumppaneilta, jotka voivat auttaa suunnittelemaan ja toteuttamaan kyberturvallisuustoimenpiteitä ympäristössäsi.

Esimerkkejä ulkoisista organisaatiot ovat:

- Merenkulkualan varustamot
- Merenkulkualan järjestöt ja yhdistykset
- Luokittelulaitokset
- Merivakuutusyhtiöt
- Kansalliset tietoturva-alan viranomaiset(esim. Kyberturvallisuuskeskus)
- Kyberturvallisuusyritykset

Kyberturvallisuus on monimutkainen prosessi, joka vaatii erityisosaamista, joka on vaikea löytää. IT- ja OT-tiimisi työskentelevät todennäköisesti kovasti säännöllisten tehtäviensä ja projektien parissa, ja voi olla helpompaa ja halvempaa saada apua ulkoisista resursseista, joilla on aikaisempaa tietoa merenkulun kyberturvallisuudesta sen sijaan, että palkattaisiin vaikeasti löydettäviä asiantuntijoita organisaatioosi.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI