Pia Satopää,
Olli Soininen &
Jarkko Paavola

Fintraffic TURKU AMK

Meriklusteritoimijoiden tieto- ja kyberturvallisuuden hallintamalli OT-ympäristöille

303
Raportteja

TURKU AMK

Pia Satopää, Olli Soininen & Jarkko Paavola

Meriklusteritoimijoiden tieto- ja kyberturvallisuuden hallintamalli OT-ympäristöille

Fintraffic

Turun ammattikorkeakoulun raportteja 303
Turun ammattikorkeakoulu
Turku 2024

Kirjoittajat:
Pia Satopää Turun ammattikorkeakoulu
Olli Soininen Fintraffic
Jarkko Paavola Turun ammattikorkeakoulu

ISBN 978-952-216-879-5 (painettu)
ISSN 1457–7925 (painettu)
Painopaikka: Kari Media Group Oy, Printworks, Turku 2024

ISBN 978-952-216-878-8 (pdf)
ISSN 1459-7764 (elektroninen)

https://urn.fi/URN:ISBN: 978-952-216-878-8

Turun AMK:n sarjajulkaisut: turkuamk.fi/julkaisut

Sisältö

Johdanto

Meriklusteri käsittää laajan joukon toimijoita, jotka yhdessä muodostavat merenkulun ekosysteemin, mukaan lukien merenkulun, telakat, laivanrakennus, meripalvelut, satamaoperaatiot, logistiikan ja meriliikenteen hallinnan. Meriklusterin keskeisiä toimijoita ovat mm.

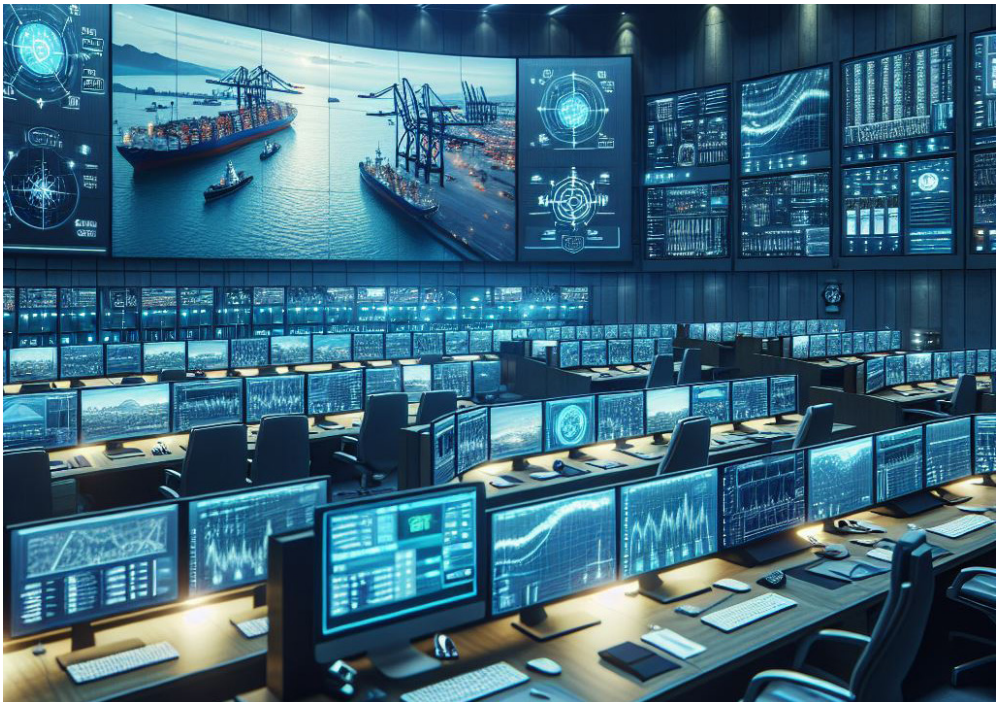
- varustamot: vastaavat laivojen operoinnista, huollosta ja reittien suunnittelusta
- satamat: toimivat merenkulun solmukohtina, tarjoten infrastruktuuria ja palveluita laivaliikenteelle
- satamaoperaattorit: huolehtivat lastin käsittelystä ja varastoinnista satamissa
- meriteollisuus: käsittää laivanrakennuksen, korjaustoiminnan ja meriteknologian kehittämisen
- luokituslaitokset: tarjoavat teknistä arviointia ja sertifiointia alusten turvallisuuden varmistamiseksi
- rahoitus- ja vakuutuspalvelut: tukevat merenkulun taloudellisia toimintoja
- julkiset toimijat: sisältävät viranomaiset, jotka säätelevät ja valvovat merenkulkua.

Meriklusterin turvallisuus on olennainen osa kansallista ja kansainvälistä turvallisuutta, sillä se on kriittinen infrastruktuuri, joka tukee globaalia kauppaa, taloudellista vakautta ja ympäristön hyvinvointia. Se on myös elintärkeä Suomen huoltovarmuudelle mahdollistaen ulkomaankaupan ja rahtiliikenteen sekä tukien puolustusvoimien toimintaa. Meriklusteri edistää Suomen kilpailukykyä ja kansainvälistymistä, sillä se tarjoaa korkealaatuisia tuotteita ja palveluita maailmanmarkkinoille sekä houkuttelee ulkomaisia investointeja ja osaamista Suomeen.

Merenkulun tai meriklusteritoimijoiden Operational Technology governance (OT governance) viittaa käytäntöihin ja menettelyihin, joilla hallinnoidaan ja valvotaan operatiivista teknologiaa merenkulkualalla. OT viittaa teollisuus- ja operatiivisiin prosesseihin, laitteisiin ja järjestelmiin, jotka ovat keskeisiä toiminnan ja infrastruktuurin hallinnassa, mukaan lukien laivojen navigointi, lastinkäsittely, energianhallinta ja muut kriittiset operatiiviset tehtävät.

Information Technology governance (IT governance) keskittyy organisaation tietoteknisten järjestelmien hallintaan. Tämä kattaa liiketoimintajärjestelmät, tietokannat ja sovellukset, ja sen pääpaino on datan suojaamisessa, tietosuojaan liittyvissä vaatimuksissa, järjestelmien käytettävyydessä ja liiketoimintaprosessien tehokkuudessa. IT governance varmistaa, että organisaation tietojärjestelmät toimivat tehokkaasti ja turvallisesti noudattaen lainsäädäntöä ja standardeja, kuten GDPR, NIS2 ja ISO 27001.

Tieto- ja kyberturvallisuus ovat nykyaikaisen meriklusterin toiminnan kulmakiviä. Niillä suojataan tärkeitä tietojärjestelmiä ja infrastruktuuria kyberuhkilta, jotka voivat aiheuttaa vakavia häiriöitä, toiminnan keskeytymistä, taloudellisia menetyksiä, ympäristöhaittoja tai jopa uhata ihmishenkiä. Tämän käsikirjan tavoitteena on tarjota lukijalle ymmärrys tieto- ja kyberturvallisuuden toimintakentästä, uhkaympäristöstä ja siitä, miten näitä riskejä voidaan hallita tehokkaasti.



1

Tieto ja kyber-turvallisuuden merkitys organisaatiolle ja liiketoiminnalle

Tieto- ja kyberturvallisuuden jatkuvuudella ja sen suunnittelulla on suuri merkitys liiketoiminnan jatkamiselle häiriötilanteissa. ISO/IEC27001-standardi tarjoaa siihen hyvät valmiudet, sillä se tarjoaa viitekehyksen ja puitteet, joiden avulla yritys voi suojata tietonsa ja tietojärjestelmänsä kyberuhilta ja varmistaa toiminnan jatkuvuuden.

Fyysisen omaisuuden, kuten rakennuksen tai auton vakuuttaminen on ymmärrettävästi tärkeää – se antaa turvaa odottamattomien vahinkojen varalta. Tieto- ja kyberturvallisuus toimivat samalla periaatteella, mutta niiden kohteena ovat yrityksen tiedot ja tietojärjestelmät. Aivan kuten vakuutus suojaa fyysistä omaisuutta, tieto- ja kyberturvallisuus suojaavat digitaalista omaisuutta, joka on yhä arvokkaampaa nykypäivän liiketoiminnassa.

Koska tieto on nykypäivän liiketoiminnassa yksi yrityksen arvokkain omaisuus ja resurssi, sen suojaaminen ja toiminnan jatkuvuus parantavat myös asiakkaiden ja yhteistyökumppaneiden luottamusta. Tämä analogia auttaa ymmärtämään, miksi kyberturvallisuuden merkitys on yhtä suuri kuin perinteisen vakuuttamisen.

Esimerkiksi satamaoperaattorit voivat hyödyntää reaaliaikaisia tietojärjestelmiä, jotka seuraavat alusten sijainteja ja lastinkäsittelyn edistymistä. Tämä tieto mahdollistaa tehokkaan satamaoperaatioiden hallinnan, vähentää odotusaikoja ja parantaa aikataulujen noudattamista. Eheään ja saavutettavaan tietoon perustuva päätöksenteko auttaa myös varmistamaan, että kaikki sääntö- ja turvallisuusvaatimukset täyttyvät.

1 Riskienhallinta ja suojatoimet:

a) Fyysinen omaisuus: vakuutusyhtiö edellyttää usein, että yritys toteuttaa tiettyjä suojatoimia, kuten hälytysjärjestelmiä ja turvakameroita, jotta omaisuus pysyy turvassa.

b) Tieto ja järjestelmät: ISO/IEC 27001 tarjoaa ohjeet ja suositukset, kuten vahvat salasanakäytännöt, tiedon salaus ja pääsynhallinta, jotka auttavat suojaamaan yrityksen tietoja ja järjestelmiä.

2 Jatkuva parantaminen ja valvonta:

a) Fyysinen omaisuus: vakuutusyhtiö saattaa vaatia säännöllisiä tarkastuksia ja päivityksiä suojajärjestelmiin.

b) Tieto ja järjestelmät: ISO/IEC 27001 -mukainen jatkuva parantaminen tarkoittaa säännöllistä riskien arviointia, suojaustoimien tarkastamista ja päivittämistä sekä tietoturvakäytäntöjen kehittämistä. Tämä varmistaa, että yrityksen tietoturva on ajan tasalla ja pystyy vastaamaan uusiin uhkiin.

3 Liiketoiminnan jatkuvuus:

a) Fyysinen omaisuus: vakuutus auttaa yritystä toipumaan fyysisistä vahingoista, kuten tulipalosta tai varkaudesta, ja jatkamaan toimintaansa.

b) Tieto ja järjestelmät: ISO/IEC 27001 auttaa yritystä varautumaan tietomurtoihin, palvelunestohyökkäyksiin ja muihin kyberuhkiin. Varautumissuunnitelmat ja varmuuskopiot takaavat, että yritys voi palauttaa tiedot ja jatkaa toimintaansa mahdollisimman nopeasti häiriön jälkeen.

Jos yritys on valmis panostamaan fyysisen omaisuuden vakuuttamiseen, samanlainen panostus kyberturvallisuuteen on aivan yhtä tärkeää. Fyysinen omaisuus, kuten rakennukset ja laitteet, on arvokasta, mutta nykymaailmassa tieto ja tietojärjestelmät ovat usein vielä arvokkaampia. Menetettyjen tai vaarantuneiden tietojen aiheuttamat vahingot voivat olla merkittäviä., ja niillä voi olla pitkäkestoisia vaikutuksia yrityksen toimintaan ja maineeseen.

1.1 ISO/IEC27001 -standardin mukaisen hallintajärjestelmän edut

1. **Luottamus:** asiakkaat ja yhteistyökumppanit luottavat siihen, että heidän tietonsa ovat turvassa. ISO/IEC 27001 -sertifiointi voi parantaa yrityksen mainetta ja luottamusta.

2. **Kilpailuetu:** yritykset, joilla on vahva kyberturvallisuus, voivat kilpailla tehokkaammin markkinoilla. Ne voivat tarjota asiakkailleen varmuuden siitä, että heidän tietojaan käsitellään turvallisesti.

3. **Sääntelyvaatimusten toteutuminen:** monet alat edellyttävät tiettyjen tietoturvastandardien noudattamista. ISO/IEC 27001 auttaa yrityksiä täyttämään nämä vaatimukset ja varmistaa, että tietoturvakäytännöt ovat linjassa yleisten standardien kanssa. Lisäksi NIS2-direktiivi asettaa erityisiä velvoitteita kriittisten ja tärkeiden palveluiden tarjoajille, kuten kyberturvallisuustoimenpiteiden toteuttamiselle ja raportointivelvollisuuksille. Noudattamalla näitä vaatimuksia yritykset voivat välttää merkittäviä sanktioita ja muita seuraamuksia, joita sääntöjen rikkomisesta voisi seurata.

4. **Vahinkojen minimoiminen:** hyvin toteutettu kyberturvallisuus auttaa estämään tietomurtoja ja muita kyberhyökkäyksiä sekä minimoimaan niiden vaikutukset. Tämä voidaan nähdä analogiana vakuutukseen: aivan kuten fyysisen omaisuuden vakuuttaminen suojaa yritystä odottamattomilta vahingoilta, kyberturvallisuus suojaa yrityksen tietoja ja tietojärjestelmiä menetyksiltä ja rikollisuudelta.

2

Järjestelmien kyberturvallisuus-vaatimukset

Meriklusterin tieto- ja kyberturvallisuuden toteuttaminen ja hallinta on haastavaa, sillä se edellyttää monipuolisten Information Technology (IT) ja Operational Technology (OT) -järjestelmien suojaamista erilaisilta kyberuhkilta ja -hyökkäyksiltä sekä toimijoiden kattavaa ja monipuolista osaamista.

Meriklusteritoimijoiden tieto- ja kyberturvallisuutta ohjataan erilaisilla kansallisilla ja kansainvälisillä säädöksillä, standardeilla, määräyksillä ja ohjeilla. Esimerkiksi:

- **NIS2- direktiivi (EU:n kyberturvallisuusdirektiivi)**
  - Voimaantulo 16.1.2023
  - Direktiivin vaatimukset osaksi kansallista lainsäädäntöä 17.10.2024 mennessä

- **GDPR (EU:n yleinen tietosuoja-asetus)**
  - Voimaantulo 25.5.2018

- **EU:n meriliikenteen kyberturvallisuuden strategia**
  - Voimaantulo vuonna 2018, päivitetty 2020

- **IMO:n (International Maritime Organization) kyberturvallisuuden suuntaviivat**
  - Julkaisuvuosi 2017
  - Pakollisen soveltamisen voimaantulo 1.1.2021

- **ISACS:n (International Ship and Port Facility Security Code) meriliikenteen ja satamien turvallisuustoimenpidemääräykset**

- **IEC:n (International Electrotechnical Commission) OT-kyberturvallisuuden standardit**
  - EC 62443-2-1: julkaistu vuonna 2010. Käsittelee teollisuusautomaation ja -ohjauksen kyberturvallisuuden hallintajärjestelmiä.
  - IEC 62443-3-3: julkaistu vuonna 2013. Määrittelee teknisiä kyberturvallisuusvaatimuksia OT-järjestelmille.

- **IACS:n (International Association of Classification Societies) UR (Unified Requirements)**
  - 26 Alusten kyberresilienssi
  - 27 Aluksella olevien järjestelmien kyberresilienssi
  - Julkaistu 2022
  - Voimaantulo 1.1.2024

Nämä ovat hyödyllisiä lähteitä. Lisäksi tarvitaan informaatiota meriklusteritoimijoiden OT-järjestelmien ominaisuuksista, haavoittuvuuksista, uhkista ja riskeistä sekä niiden hallintakeinoista.

Erityisesti NIS2-direktiivi vaikuttaa meriklusteritoimijoihin, sillä se sisältää uusia velvoitteita ja vaatimuksia meriliikenteen ja merenkulun turvallisuudelle. Direktiivin mukaan meriliikenteen ja merenkulun toimijat kuuluvat olennaisiin yhteiskunnan toimintoihin (OYT), jotka ovat velvollisia noudattamaan kattavia kyberturvallisuusstandardeja ja raportoimaan kyberturvallisuuspoikkeamista kansallisille viranomaisille. NIS2 asettaa myös erityisiä vaatimuksia yrityksen johdon vastuusta kyberturvallisuuden tasoon sekä riskien seurantaan liittyen.

NIS2-direktiivi, joka kansallisesti toimeenpannaan kyberturvallisuuslain kautta, myös laajentaa soveltamisalaa kattamaan uusia toimijoita, kuten satamat, satamapalvelut, meriliikenteen hallinta ja meripelastus. Direktiivissä on huomioitavaa, että siinä määräävää on myös organisaation koko. Vaikka se ei suoraan koskisikaan organisaatiota, voi se velvoittaa toimitusketjun toimijaa isomman organisaation kautta. Suurempien organisaatioiden vaatimukset siirtyvät toimitusketjujen kautta pienemmille organisaatioille.

3 Meriklusteri-toimijoiden OT-ympäristöt

Meriklusteritoimijat käyttävät erilaisia OT-järjestelmiä operatiivisen tehokkuuden, turvallisuuden ja kestävyyden parantamiseen. OT-ympäristö on joukko laitteita, ohjelmistoja ja verkkoja, jotka ohjaavat, valvovat ja optimoivat teollisia tai toiminnallisia prosesseja.

Meriklusteritoimijoiden OT-järjestelmät tuottavat ja käsittelevät erilaista dataa, joka liittyy esimerkiksi alusten sijaintiin, nopeuteen, kurssiin, lastiin, polttoaineeseen, miehistöön, matkustajiin, ympäristöön, navigointiin, viestintään ja turvallisuuteen. Tämä data voi olla arkaluonteista tai luottamuksellista ja sen menetys, vääristyminen tai väärinkäyttö voi aiheuttaa vakavia seurauksia. Siksi dataa tulisi suojata asianmukaisesti fyysisesti ja digitaalisesti sekä varmistaa sen eheys, saatavuus ja luottamuksellisuus.

Alla on yleisluonteinen kuvaus OT-järjestelmistä:

3.1 Merilogistiikan OT-järjestelmät

- Automaattiset terminaalin käyttöjärjestelmät (TOS-järjestelmät):
    - Käytetään satamien konttiterminaalien operaatioiden hallintaan. Järjestelmät tarjoavat reaaliaikaista näkyvyyttä terminaalitoimintoihin, optimoivat resurssien käyttöä ja parantavat toimintojen tehokkuutta.

- Laivaliikenteen hallintajärjestelmät (VTS):
  - Auttaa valvomaan ja hallitsemaan laivaliikennettä satamissa ja merialueilla. Parantaa navigointiturvallisuutta ja liikenteen sujuvuutta yhdistämällä tutkatietoja, AIS-tietoja (Automatic Identification System), joita ovat alusten sijainnin, nopeuden ja reittien seuraamiseen liittyvät tiedot ja muuta anturidataa tarjotakseen kattavan näkymän liikennetilanteeseen.

- Satamien infrastruktuurin hallintajärjestelmät (PCS):
  - Seuraavat ja hallitsevat satamien infrastruktuurin, kuten nostureiden, porttien ja valvontakameroiden, tilaa ja toimintaa. Tämä parantaa sataman operatiivista tehokkuutta ja turvallisuutta.

- Satamien logistiikka- ja lastausjärjestelmät (PCS):
  - Optimoivat satamien logistiikkaa ja lastaustoimintoja. Järjestelmät mahdollistavat tehokkaan lastin käsittelyn, varastoinnin ja kuljetuksen, mikä parantaa toimitusketjun hallintaa.

- Viestintä- ja tietoliikennejärjestelmät:
  - Mahdollistavat alusten ja satamien välisen viestinnän ja tietoliikenteen. Nämä järjestelmät tukevat reaaliaikaista tiedonvaihtoa ja koordinaatiota, mikä on tärkeää turvallisuuden ja tehokkuuden kannalta.

3.2 Meriteollisuuden OT-järjestelmät

- Integroidut automaatiojärjestelmät:
  - Yhdistää laivan kaikkien järjestelmien ohjauksen ja valvonnan yhteen käyttöliittymään. Tämä parantaa operatiivista tehokkuutta ja vähentää energiankulutusta hallitsemalla voimantuotantoa, potkurijärjestelmiä ja ympäristöjärjestelmiä.

- Kunnonvalvontajärjestelmät:
  - Käytetään alusten ja meriteollisuuden laitteiden tila- ja toimintatietojen seurantaan. Järjestelmät seuraavat koneiden tärinää, lämpötilaa ja muita parametreja, mikä mahdollistaa ennakoivan huollon ja vähentää odottamattomia laitteistovikoja. Myös alusten rungon kuntoa seurataan ultraääni- ja visuaalisin tarkastuksin rakenteellisten vaurioiden ehkäisemiseksi.

- Energianhallintajärjestelmät:
  - Käytetään laivojen energianhallintaan. Järjestelmät optimoivat energian käytön ja parantavat tehokkuutta seuraamalla ja ohjaamalla sähköjärjestelmiä, valaistusta, ilmanvaihtoa ja muita energiankuluttajia. Tämä auttaa optimoimaan polttoaineenkulutuksen ja vähentämään päästöjä keräämällä tietoja kaikista energian kulutuspisteistä ja käyttämällä analytiikkaa tehokkuuden parantamiseen.

- Telakoiden tuotanto-, suunnittelu- ja testausjärjestelmät:
    - Käytetään telakoilla alusten tuotanto-, suunnittelu- ja testausprosessien hallintaan. Nämä järjestelmät parantavat tuotannon laatua ja tehokkuutta integroimalla eri vaiheet saumattomasti.

- Innovaatio-, kehitys- ja markkinointijärjestelmät:
    - Meriteknologia-alan yritykset käyttävät näitä järjestelmiä innovaatioiden, tuotekehityksen ja markkinoinnin hallintaan. Järjestelmät tukevat uusien teknologioiden kehittämistä ja markkinoille tuomista, mikä parantaa kilpailukykyä ja liiketoiminnan kasvua.

3.3 Alusten ja varustamojen OT-järjestelmät

- Alusten kunnon- ja toimintatilan valvontajärjestelmät:
    - Seuraavat alusten koneiden, järjestelmien ja laitteiden tilaa ja toimintaa. Nämä järjestelmät mahdollistavat ennakoivan huollon ja optimoinnin, mikä vähentää laitteistovikoja ja parantaa operatiivista tehokkuutta.

- Alusten sijainti-, nopeus- ja reittitietojärjestelmät:
    - Käytetään seuraamaan ja hallitsemaan alusten sijaintia, nopeutta ja reittejä. Nämä järjestelmät parantavat navigointiturvallisuutta ja operatiivista tehokkuutta.

- Alusten ja varustamojen väliset viestintä- ja tietoliikennejärjestelmät:
    - Mahdollistavat reaaliaikaisen tiedonvaihdon alusten ja varustamojen välillä. Tämä parantaa operatiivista tehokkuutta ja turvallisuutta tarjoamalla jatkuvan yhteydenpidon ja koordinaation.

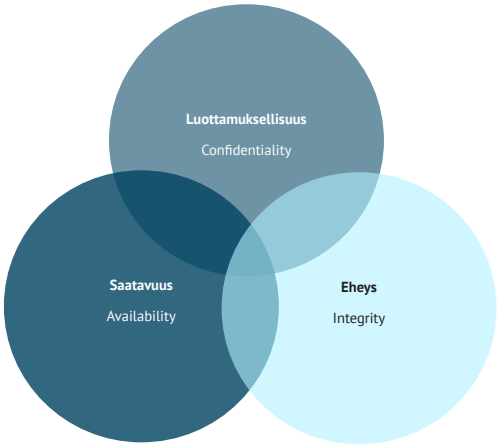
Nämä OT-järjestelmät ovat esimerkkejä keskeisistä merilogistiikan ja meriteollisuuden operatiivisen tehokkuuden, turvallisuuden ja kestävyyden parantamisessa.

4

Tieto- ja kyber-turvallisuuden hallintamalli

Tietoturvallisuus tarkoittaa, että niin sanottu CIA-malli (confidentiality eli luottamuksellisuus, integrity eli eheys, availability eli saatavuus) toteutuu eli tieto on suojattu luvattomalta pääsyltä, muutokselta, häviämiseltä tai tuhoutumiselta. Olennainen kontrolli CIA-mallin toteutumiselle onkin pääsynhallinnan varmistaminen.

Tietoturvallisuus kattaa sekä digitaalisessa että fyysisessä muodossa olevan tiedon. Kyberturvallisuus tarkoittaa sitä, että tietoverkot, verkkoon liitetyt laitteet ja niiden kautta kulkeva tieto on suojattu kyberuhkilta ja -hyökkäyksiltä. Kyberturvallisuus kattaa erityisesti digitaalisen tiedon ja järjestelmät sekä verkkoon liitetyt OT-laitteet.

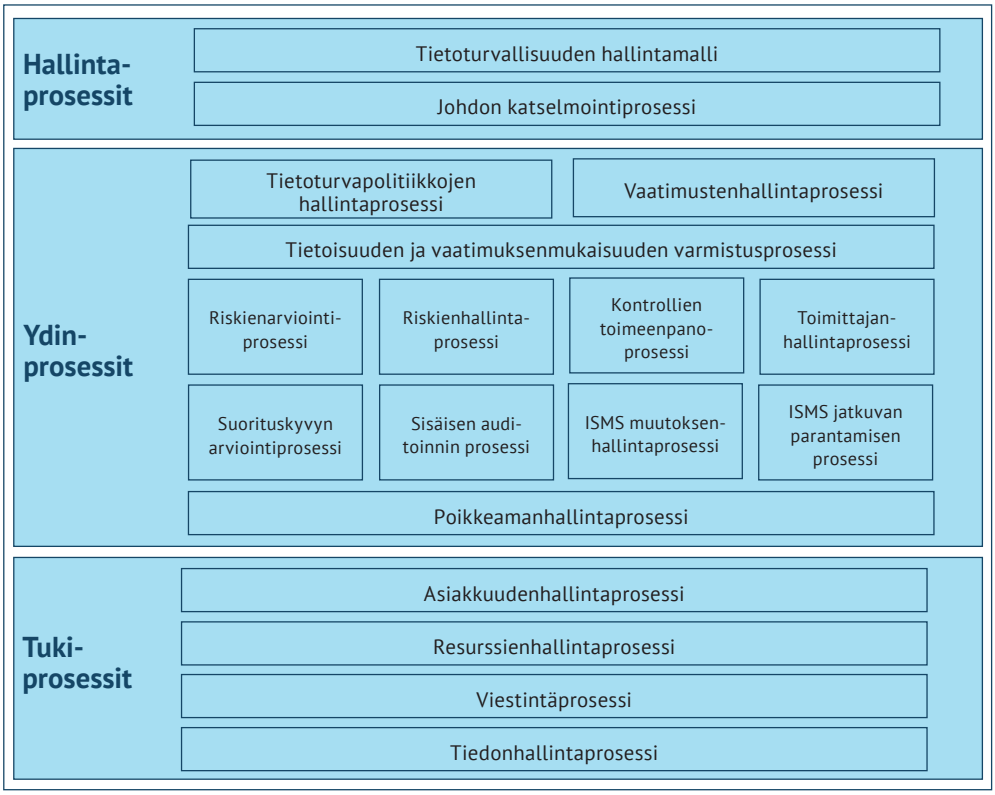


Kuvio 1.
Tietoturvallisuuden CIA -malli.

Governance-malli eli **hallintamalli** tarkoittaa mallia, toimintatapoja ja ohjeistuksia, miten organisaatio hallitsee ja ohjaa toimintaansa, erityisesti tietotekniikkaa, tietoa ja dataa. Hallintamalli määrittelee organisaation tietoturvallisuuteen liittyvät strategiset tavoitteet, vastuut, roolit, prosessit, mittarit ja standardit liittyen näihin alueisiin. Hallintamallin avulla organisaatio voi varmistaa, että se käyttää resurssejaan tehokkaasti, noudattaa lakeja ja säännöksiä, parantaa laatua, turvallisuutta sekä toimintavarmuutta. Yksinkertaistettuna hallintamallilla tarkoitetaan päätöksenteko- sekä raportointiprosessia, vastuita ja resursseja.

Tietoturvallisuuden hallintajärjestelmällä (ISMS, Information Security Management System) tarkoitetaan käytännön järjestelmää tai kehystä, jolla hallitaan tietoturvariskejä ja jolla varmistetaan suojaustoimenpiteiden toimivuus ja jatkuva parantaminen.

Tieto- ja kyberturvallisuuden hallintamalleja on erilaisia riippuen organisaation koosta, toimialasta, kulttuurista ja strategiasta. Hallintamallin valintaan ja toteutukseen vaikuttavat myös organisaation ulkoiset tekijät, kuten kilpailu, markkinat, asiakkaat, kumppanit ja sidosryhmät. Hallintamalli voi olla kokonaisturvallisuuteen, riskienhallintaan tai yhteistyöhön perustuva.



Kuva 2.
Tieto- ja kyberturvallisuuden hallintamalli.

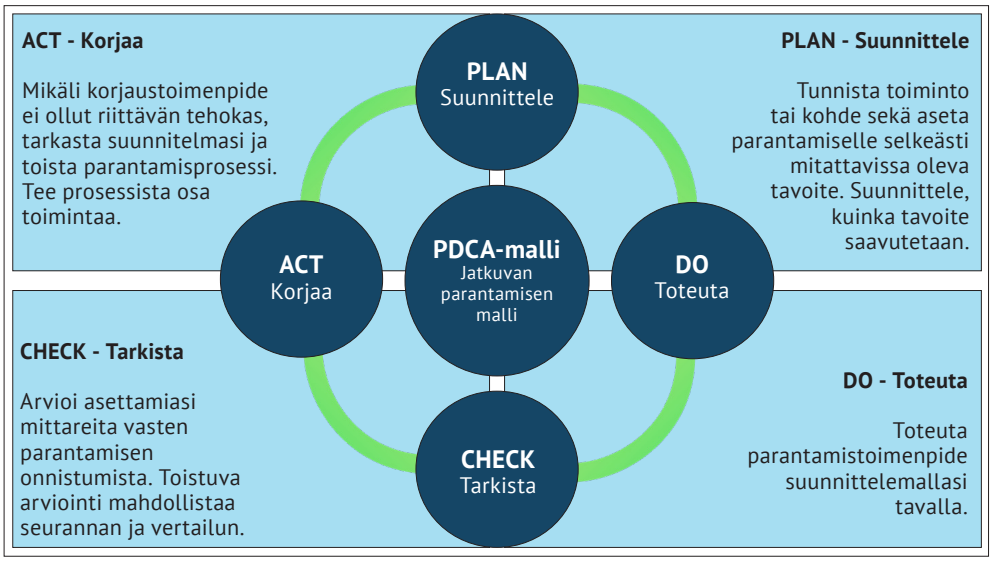
5

Meriklusteri-toimijoiden tieto- ja kyberturvallisuuden hallintamalli

Tieto- ja kyberturvallisuuden hallintamallin tulee tukea organisaation liiketoimintastrategiaa ja tavoitteita. Sen luomiseen ja ylläpitämiseen tarvitaan johdon sitoutumista, henkilöstön osaamista, selkeitä ohjeita ja työkaluja sekä jatkuvaa seurantaa ja arviointia. Se on dynaaminen ja muuttuva kokonaisuus, joka vaatii jatkuvaa kehittämistä ja parantamista. Hallintamalli keskittyy tietoturvallisuuden strategiseen ohjaamiseen ja valvontaan ja se asettaa periaatteet, vastuut ja valtuudet tietoturvaan liittyen.

Mikäli hallintamallia ei ole olemassa tai se on puutteellinen tai vanhentunut, organisaation voi olla vaikeaa hallita riskejä, joiden seurauksena voi olla tieto- ja kyberturvallisuuteen liittyvät loukkaukset, oikeudelliset seuraamukset tai toimintakyvyn ja maineen menetys. Tieto- ja kyberturvallisuus ovat siis olennainen osa nykyaikaista ja luotettavaa liiketoimintaa.

Hallintamalli sisältää hallintajärjestelmän (ISMS), joka on jäsennelty lähestymistapa, jolla hallitaan ja suojataan organisaation tietoja. Hallintajärjestelmiksi on olemassa valmiita malleja (esim. ISO27001-standardi), joita noudattamalla kattaa menettelytavat tietojen suojaamiseksi. Ne käsittävät esimerkiksi riskienhallinnan, käytännöt ja prosessit. Käytännössä hallintamallit noudattavat jatkuvan parantamisen mallia, joka toteuttaa kansainvälisesti tunnettua PDCA-mallia (Plan, Do, Check, Act):



Kuvio 2.

Tietoturvallisuuden jatkuvan parantamisen malli (PDCA).

6 Riskiperusteinen toimintamalli

Tieto- ja kyberturvallisuuden hallintamallin sisältämän hallintajärjestelmän tarkoituksena on riskienhallintaperusteinen toiminta, jolla tunnistetaan ja arvioidaan toimintaympäristöön, henkilöstöön sekä operatiiviseen teknologiaan liittyvät riskit, kuten kyberuhkat, laitteistoviat ja toimintaprosessien häiriöt. Riskienhallintaperusteisella hallintamallilla suojataan aluksia, satamia ja muita merenkulun infrastruktuureja kyberuhkilta ja muilta riskeiltä. Riskienhallinnan tavoitteena onkin kehittää ja ottaa käyttöön riskienhallintastrategioita ja -toimenpiteitä jatkuvan parantamisen (PDCA-malli) prosessilla.

Meriklusteritoimijoiden hallintamallilla varmistetaan, että operatiiviset järjestelmät toimivat luotettavasti ja turvallisesti, estäen epäkäytettävyystilanteita, onnettomuuksia ja vaaratilanteita. Tieto- ja kyberturvallisuustoimenpiteillä suojataan operatiivisia järjestelmiä kyberuhkilta ja tietomurroilta. Tällä pyritään varmistamaan, että kaikki järjestelmät ja laitteet ovat ajan tasalla ja suojattuja haittaohjelmilta ja muilta kyberhyökkäyksiltä. Tällä taas minimoidaan toiminnan keskeytyksiä ja varmistetaan laitteiden ja järjestelmien jatkuva toiminta.

Hallintamallilla voidaan varmistua, että organisaatio noudattaa toiminnalle asetettuja kansallisia ja kansainvälisiä lakeja, määräyksiä ja standardeja, kuten IMO (International Maritime Organization) ohjeistuksia. Tällä varmistetaan, että kaikki operatiiviset prosessit ja teknologiat täyttävät asetetut strategiassa asetetut tavoitteet ja vaatimukset.

Tietojen hallinnalla ja integroinnilla varmistetaan tiedon tarkkuus, eheys ja saatavuus sekä hallitaan operatiivisten järjestelmien tuottama data tehokkaasti. OT-hallintamalli on kriittinen osa modernia merenkulkua, jossa digitaalisten ja fyysisten järjestelmien integrointi ja hallinta ovat yhä tärkeämpiä turvallisuuden ja tehokkuuden varmistamiseksi.

6.1 Riskiperusteinen arviointi

Riskiperusteinen arviointi auttaa ymmärtämään, mikä tieto on merkittävää ja miten sitä tulisi suojata. Tärkeintä on tunnistaa tiedot, arvioida mahdolliset riskit, määritellä tiedon arvo ja toteuttaa tarvittavat suojaustoimet. Näin varmistetaan, että tärkeimmät tiedot pysyvät turvassa.

Mitä tarkoittaa riskiperusteinen arviointi?

Riskiperusteinen arviointi tarkoittaa sitä, että mietit, mitkä asiat voisivat uhata tietojasi ja kuinka vakavia seurauksia näillä uhilla voisi olla. Tämä auttaa päättämään, mikä tieto on erityisen tärkeää suojata ja miten se kannattaa suojata.

Kuinka määritellä, mikä tieto on merkittävää?

- Tunnista tieto: Ensin tulee selvittää, mitä tietoja organisaatiolla on. Onko organisaatiolla henkilötietoja, kuten nimiä ja osoitteita tai organisaation liiketoiminnan kannalta muita tärkeitä tietoja.
- Arvioi riskejä: Mieti, mitä voisi tapahtua, jos nämä tiedot joutuvat vääriin käsiin tai katoavat:
    - Kuka voisi olla kiinnostunut tästä tiedosta ja miksi?
    - Miten sen voisi yrittää saada haltuun?
    - Mitä tapahtuisi, jos tieto joutuu vääriin käsiin tai menetettäisiin?

Määritä tiedon arvo:

Määritä, kuinka tärkeää tieto on organisaatiollesi. Onko se jotain, joka voisi aiheuttaa suurta vahinkoa, jos se paljastuisi? Esimerkiksi:

- Henkilötiedot (kuten nimet ja osoitteet) ovat erittäin arkaluontoisia.
- Liikesalaisuudet voivat olla erittäin tärkeitä yrityksellesi.

Priorisoi suojaustoimet

Kun tiedetään, mikä tieto on tärkeintä, voidaan päättää, miten sitä suojataan parhaiten. Tämä voi tarkoittaa esimerkiksi:

- salasanojen käyttöä ja säännöllistä vaihtamista
- tietojen salaamista (kryptausta), jolloin niitä ei voida lukea ilman oikeaa avainta
- pääsyn rajoittamista niin, että vain tietyt henkilöt voivat päästä tietoihin käsiksi.

6.1.1 Esimerkki riskiperusteisesta arvioinnista

Kuvitellaan tilanne, jossa yrityksen asiakasrekisterissä on asiakkaiden yhteystiedot ja tilaushistoria.

- Tunnista tieto: Asiakasrekisteri sisältää henkilötietoja ja tilaushistoriaa.
- Arvioi riskejä: Jos tämä tieto varastetaan:
    - o Rikolliset voivat käyttää tietoja huijauksiin.
    - o Kilpailijat voivat saada tietoa asiakkaista.
    - o Yrityksen maine voi kärsiä.

Määritä tiedon arvo: asiakastiedot ovat erittäin tärkeitä, koska ne vaikuttavat suoraan yrityksen toimintaan ja maineeseen.

Priorisoi suojaustoimet: voidaan toimia esimerkiksi näin:

- Käytetään vahvoja salasanoja asiakasrekisterin suojana.
- Rajoitetaan pääsy rekisteriin vain niille työntekijöille, jotka tarvitsevat tietoa työnsä tekemiseen.
- Salataan tiedot, jotta niitä ei voida lukea ilman oikeaa avainta.

Yhteenveto

Riskiperusteinen arviointi auttaa ymmärtämään, mikä tieto on merkittävää ja miten sitä tulisi suojata. Tärkeintä on tunnistaa tiedot, arvioida mahdolliset riskit, määritellä tiedon arvo ja toteuttaa tarvittavat suojaustoimet. Näin voit varmistaa, että tärkeimmät tietosi pysyvät turvassa!

7

OT-ympäristön tunnistetut haavoittuvuudet

Meriklusteritoimijoiden OT-kyberturvallisuudessa voi olla erilaisia haavoittuvuuksia, jotka voivat liittyä esimerkiksi vanhentuneisiin tai suojaamattomiin OT-järjestelmiin, riittämättömään tietoisuuteen ja koulutukseen, heikkoon yhteistyöhön ja tiedonvaihtoon, puutteellisiin kyberturvallisuusstrategioihin ja -politiikkoihin sekä epäselviin rooleihin ja vastuisiin. Nämä puutteet voivat lisätä meriklusteritoimijoiden haavoittuvuutta kyberhyökkäyksille ja vähentää toimijoiden kykyä reagoida niihin tehokkaasti.

Mahdollisia haavoittuvuuksia OT-ympäristöissä:

- Vanhentunut ja päivittämätön ohjelmisto – Yksi yleisimmistä haavoittuvuuksista OT-ympäristöissä on vanhentuneen ja päivittämättömän ohjelmiston läsnäolo. Tämä voi johtaa siihen, että OT-järjestelmät ovat alttiita tunnetuille hyökkäyksille, jotka hyödyntävät ohjelmiston heikkouksia. Huomioi, että aina OT-ympäristön päivittäminen ei ole mahdollista ja tällöin tulee ratkaista suojaaminen muilla keinoin.
- Heikko tunnistautuminen ja pääsynhallinta – Riittämättömät tunnistautumismenetelmät ja löyhät pääsynhallintakäytännöt ovat merkittäviä haavoittuvuuksia OT-verkoissa. Ne voivat mahdollistaa luvattoman pääsyn OT-järjestelmiin ja niiden manipuloinnin.
- Suojaamattomat portit ja palvelut – Monet nykyiset OT-järjestelmät on suunniteltu ilman sisäänrakennettua tietoturvaa, mikä tarkoittaa, että tietoturvatoimenpiteet eivät ole olleet keskiössä järjestelmien kehitysvaiheessa. Suojaamattomat portit ja palvelut voivat olla potentiaalinen hyökkääjien kohde. Esimerkiksi teollisuuden ohjausjärjestelmissä (ICS) käytetään usein vanhoja tai räätälöityjä protokollia, jotka eivät sisällä salaus- tai todennusmekanismeja.

- Puutteellinen tietoisuus ja koulutus – OT-ympäristöjen henkilöstö ei välttämättä ole tietoinen kyberturvallisuusuhista ja -käytännöistä, jotka koskevat heidän työtään. Tämä voi johtaa virheisiin tai huolimattomuuteen, jotka voivat vaarantaa OT-järjestelmien turvallisuuden. Esimerkiksi henkilöstö voi käyttää oletussalasanoja, liittää epäluotettavia laitteita OT-verkkoon tai klikata haitallisia linkkejä sähköposteissa.
- Heikko yhteistyö ja tiedonvaihto – OT-ympäristöt ovat usein erillään IT-ympäristöistä, mikä voi vaikeuttaa yhteistyötä ja tiedonvaihtoa kyberturvallisuudesta vastaavien tahojen välillä. Tämä voi johtaa siihen, että OT-järjestelmien kyberturvallisuustilanne ei ole selvillä tai että kyberhyökkäyksiin ei reagoida nopeasti ja tehokkaasti.

OT-ympäristön haavoittuvuuksia tulee arvioida riskiperusteisesti ja mahdollisen hyväksikäytön vaikutusten mukaan. Mikäli vaikutus organisaation toiminnalle tai tiedoille on vähäinen, voi suojaustoimina riittää vähäisempi ja kevyempi ratkaisu. Mikäli vaikutus on suuri, tulee suojaustoimiin panostaa riittävästi.

8

OT-ympäristön valvonta

Koska monet OT-järjestelmät on toistaiseksi vielä suunniteltu ilman sisäänrakennettua tietoturvaa, luo se haavoittuvuuksia, jotka vaativat erityisiä valvontakäytäntöjä. Suurin ero IT ja OT SOCien (Security Operation Center) toiminnoissa on, että OT-ympäristöjen tiedot eivät ole samalla tavalla standardisoituja. OT SOCien osalta joudutaan usein tekemään hälytysten ja raja-arvojen mallintamista, jotta valvonta olisi mahdollista tehokkaasti ja toivotulla tavalla.

Operational technology (OT) -toiminnoissa tulisikin ottaa huomioon valvonnan/valvomon SOCin rooli ja tehtävät kyberturvallisuuden varmistamisessa. SOC on tiimi, jonka pääasiallinen tehtävä on hallita ja lieventää kyberturvallisuusuhkia. Tämä tiimi siis seuraa verkko- ja laitetoimintaa tunnistaakseen ja torjuakseen ongelmia.

OT-ympäristöissä SOCin tulisi pystyä ymmärtämään ja suojaamaan järjestelmiä, kuten teollisuuden ohjausjärjestelmiä (ICS), jotka ovat usein kriittisiä infrastruktuureja. OT SOCin tulisi myös integroitua IT SOCin kanssa, jotta voidaan saavuttaa yhtenäinen näkymä kyberturvallisuustilanteesta ja parantaa yhteistyötä ja tiedonjakoa.

Kriittisimmissä järjestelmissä organisaatiolla tulee olla valvonnan lisäksi joko sisäisesti tai ulkoistettuna myös reagointikykyä tilanteissa, jotka vaativat välitöntä tai nopeaa reagointia. Organisaation tulee arvioida, onko kyvykkyys tarpeen hankkia itselle vai voidaanko se hankkia ulkoistettuna palveluna. Joissakin tilanteissa tiedon tuottaminen kolmannelle osapuolelle voi itsessään tuottaa riskin.

Meriklusteritoimijoiden OT SOCissa kulkee dataa, joka liittyy merenkulun ja meriteollisuuden kyberturvallisuuteen. Meriklusteritoimijat ovat esimerkiksi varustamoita, telakoita, satamia, logistiikkayrityksiä ja meriteknologia-alan yrityksiä, jotka tuottavat tai käyttävät merellisiä palveluja tai tuotteita. Meriklusteritoimijoiden OT SOCissa dataa analysoidaan ja hyödynnetään tunnistamaan ja torjumaan mahdollisia kyberuhkia tai -hyökkäyksiä, jotka voisivat aiheuttaa vakavia häiriöitä tai vahinkoja näille kriittisille toiminnoille.

Kuten IT SOCissakin, meriklusteritoimijoiden OT SOCissa kulkeva data voi sisältää esimerkiksi seuraavia tietoja:

- verkkoliikenne
- loki- ja tapahtumatiedot
- haavoittuvuustiedot
- pääsynhallintatiedot
- uhkakuvatiedot
- tietoturvatapahtumisen hälytykset.

Meriklusteritoimijoiden OT SOCin rakentaminen ja ylläpitäminen vaatii erityistä osaamista ja työkaluja, jotka huomioivat merenkulun ja meriteollisuuden erityispiirteet ja haasteet. OT SOCin tulee olla yhteensopiva IT SOCin kanssa, joka vastaa tietotekniikan kyberturvallisuudesta. Niiden välillä tulee olla hyvä yhteistyö ja tiedonvaihto, jotta voidaan varmistaa koko meriklusterin kyberturvallisuus. Koska OT -järjestelmien SOC-monitorointiin kohdennettuja tuotteita ja palveluita ei ole kovin laajasti saatavilla, kaipaavat ne yhä jatkokehittämistä.

9

OT-ympäristön tieto-ja kyber-turvallisuuden hallintajärjestelmä

Hallintajärjestelmän käyttöönotto on strateginen päätös, joka riippuu organisaation toimintaympäristöstä, tarpeista, tavoitteista, turvallisuusvaatimuksista, prosesseista sekä koosta ja rakenteesta. **Järjestelmä on minimissään vastaus regulaatiovaatimuksiin ja parhaimmillaan organisaation läpileikkaava jatkuvaan parantamiseen kannustava järjestelmä.**

Jatkuvalla parantamisella ei tarkoiteta täydellisyyden tavoittelua, vaan riittävää, organisaation riskiarvioon perustuvaa tapaa hallita liiketoimintakriittistä tai muuten suojattavaksi määriteltyä tietoa, tietojärjestelmiä jne.

Tietoturvallisuuden hallintajärjestelmän tarkoituksena on siis suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta tehokkaan riskienhallinnan kautta. Se lisää myös sidosryhmien luottamusta organisaatioon ja sen asettamiin tietoturvavaatimuksiin.

Hallintajärjestelmän tulisi olla osa organisaation yleisiä prosesseja ja johtamisrakenteita, ja tietoturvallisuus tulee huomioida kaikissa suunnitteluvaiheissa. Tietoturvajärjestelmä räätälöidään organisaation toimintaympäristön ja erityistarpeiden mukaan.

Jotta tieto- ja kyberturvallisuutta voisi hallita, on hyvä hyödyntää olemassa olevia standardeja kokonaisnäkemyksen saamiseksi ja vaatimuksenmukaisuuden saavuttamiseksi. ISO/IEC 27001 -standardi pitää sisällään useita ohjeita, joita voi käsitellä meriklusteritoimijoiden näkökulmasta esimerkiksi seuraavasti:

9.1 Johdon sitoutuminen

Jotta tieto- ja kyberturvallisuuden hallinta ja hallintajärjestelmän rakentaminen olisi mahdollista, on johdon sitouduttava sen kehittämiseen ja ylläpitoon. NIS2 soveltamisalan piirissä olevien toimijoiden osalta direktiivi velvoittaa johdon vastuun yksiselitteisesti. Hallintajärjestelmän onnistuneen käyttöönoton olennaisin elementti onkin johdon sitoutuminen. Johto määrittää strategiset tavoitteet ja kohdentaa resurssit tieto- ja kyberturvallisuuden hallintajärjestelmään.

Organisaation johto:

- asettaa tieto- ja kyberturvallisuuden tavoitteet
- allekirjoittaa tietoturvapolitiikan ja osoittaa sillä sitoutumisensa politiikan kirjauksiin
- varmistaa, että tavoitteet ovat linjassa organisaation strategisten tavoitteiden kanssa
- varmistaa, että tieto- ja kyberturvallisuuden vaatimukset yhdistyvät organisaation prosesseihin ja että jatkuvan parantamisen prosessi toteutuu
- antaa ja kohdentaa resurssit, sisältäen osaamisen kehittämisen, tieto- ja kyberturvallisuuden hallintajärjestelmälle, sen rakentamiselle ja ylläpidolle
- määrittää ja varmistaa, että vastuut, roolit ja valtuudet vastaavat vaatimuksia ja tavoitteita
- viestii hallintajärjestelmästä, sen tavoitteista ja vaatimuksista organisaatiolle sekä sidosryhmille.

Tavoite

Johdon sitoutumisen päätavoitteena on varmistaa, että meriklusteritoimijat voivat toimia turvallisesti ja luotettavasti digitaalisen infrastruktuurin ja tietojen suojauksen osalta. Tavoitteena on suojata organisaatiota ja sen sidosryhmiä kyberuhkilta, vähentää liiketoiminnan keskeytyksiä, suojata mainetta sekä täyttää lakisääteiset ja sopimukselliset vaatimukset.

Tietoturvallisuus integroituu johdon sitoutumisen kautta osaksi organisaation arvoja ja päivittäistä toimintaa, mikä vahvistaa organisaation kokonaisvaltaista toimintavarmuutta ja luottamusta sidosryhmien keskuudessa.

9.2 Tietoturvapolitiikka

Tietoturvapolitiikka on hallintajärjestelmän ydin, dokumentoitu ohjeisto, joka määrittelee, miten organisaatio suojaa tietojaan ja varmistaa tietoturvallisuuden kaikilla tasoilla. Tietoturvapolitiikka auttaa suojaamaan organisaation kriittisiä tietoja luvattomalta pääsyltä, muutoksilta ja häviämiseltä. Se varmistaa, että organisaation tiedot ovat luottamuksellisia, eheitä ja saatavilla silloin, kun niitä tarvitaan. Politiikka on keskeinen osa ISO 27001 -standardin mukaista tietoturvallisuuden hallintajärjestelmää (ISMS).

Tietoturvapolitiikan tärkeimmät ominaisuudet:

- **Selkeä ja dokumentoitu ohjeistus:**
  - o Tietoturvapolitiikka tarjoaa selkeän suunnitelman ja ohjeet siitä, miten tietoturvallisuuteen liittyviä asioita käsitellään organisaatiossa.
  - o Se sisältää yksityiskohtaiset menettelytavat ja käytännöt, joita kaikkien työntekijöiden on noudatettava.

- **Johdon sitoutuminen:**
  - o Politiikka osoittaa johdon sitoutumisen tietoturvallisuuteen, mikä on tärkeää, jotta tietoturvatoimet saavat tarvittavan tuen ja resurssit.
  - o Johto allekirjoittaa ja hyväksyy tietoturvapolitiikan, mikä osoittaa sen tärkeyden koko organisaatiolle.

- **Tietoturvatavoitteet:**
  - o Tietoturvapolitiikka määrittelee organisaation tietoturvatavoitteet ja -periaatteet.
  - o Näiden tavoitteiden avulla organisaatio voi rajata ja kohdentaa tietoturvatoimenpiteensä ja arvioida niiden tehokkuutta.

- **Vastuut ja roolit:**
  - o Politiikassa määritellään selkeästi, kuka on vastuussa tietoturvasta ja mitkä ovat eri henkilöiden roolit ja tehtävät tietoturvallisuuden varmistamisessa.
  - o Tämä auttaa varmistamaan, että kaikki tietävät omat vastuunsa ja että tietoturva on integroitu organisaation päivittäiseen toimintaan.

- **Riskienhallinta:**
  - o Politiikka sisältää ohjeet tietoturvariskien tunnistamiseen, arviointiin ja hallintaan.
  - o Tämä auttaa organisaatiota ennakoimaan ja reagoimaan tehokkaasti mahdollisiin tietoturvauhkauksiin.
- **Tietoturvakoulutus ja tietoisuuden lisääminen:**
  - o Tietoturvapolitiikka korostaa koulutuksen ja tietoisuuden lisäämisen merkitystä.
  - o Organisaation työntekijöitä koulutetaan tietoturvakäytännöistä ja -menettelyistä, mikä auttaa ehkäisemään inhimillisiä virheitä ja parantaa tietoturvakulttuuria.

Tavoitteet

Vähennetään riskiä ja taloudellisia menetyksiä: Hyvin laadittu tietoturvapolitiikka auttaa vähentämään tietoturvariskien aiheuttamia taloudellisia menetyksiä, kuten tietomurtoja, kyberhyökkäyksiä ja palvelunestohyökkäyksiä. Se auttaa myös varmistamaan liiketoiminnan jatkuvuuden ja minimoimaan toiminnan keskeytyksiä.

Noudatetaan lakeja ja säädöksiä: Tietoturvapolitiikka auttaa organisaatiota noudattamaan tietoturvalainsäädäntöä ja -säädöksiä, kuten GDPR:ää. Tämä on tärkeää, jotta organisaatio välttää mahdolliset oikeudelliset seuraamukset ja mainehaitat.

Parannetaan asiakkaiden ja sidosryhmien luottamusta: Näyttämällä, että organisaatio ottaa tietoturvallisuuden vakavasti ja noudattaa parhaita käytäntöjä, se voi parantaa asiakkaiden ja sidosryhmien luottamusta. Tämä voi johtaa parempiin liiketoimintamahdollisuuksiin ja vahvempaan maineeseen.

Tuetaan jatkuvaa parantamista: Tietoturvapolitiikka luo perustan jatkuvalle parantamiselle, jossa organisaatio säännöllisesti arvioi ja päivittää tietoturvakäytäntöjään ja -toimenpiteitään. Tämä auttaa varmistamaan, että tietoturva pysyy ajan tasalla ja vastaa jatkuvasti muuttuvia uhkia ja haasteita.

Yhteenveto

Tietoturvapolitiikka on keskeinen työkalu, joka auttaa organisaatiota suojaamaan tietojaan, hallitsemaan riskejä ja varmistamaan, että tietoturvallisuus on integroitu osaksi organisaation päivittäistä toimintaa. Tietoturvapolitiikan tavoitteena on luoda vahva ja kestävä tietoturvainfrastruktuuri, joka suojaa organisaation kriittisiä resursseja ja mahdollistaa turvallisen ja keskeytymättömän toiminnan. Tämä saavutetaan yhdistämällä tekniset ratkaisut, organisatoriset toimenpiteet, koulutus ja sidosryhmäyhteistyö.

Tietoturvapolitiikan tulee sisältää selkeästi kirjatut tavoitteet tieto- ja kyberturvallisuuden toteutumiseksi. Se on oltava kaikkien saatavilla oleva dokumentti, josta on tunnistettavissa myös OT-ympäristön suojaamisen vastuut organisaation kaikilla tasoilla. Lisäksi tietoturvapolitiikan tulee kattaa sidosryhmille osoitetut vaatimukset ja velvoitteet sekä sisältää ilmoituskanavat poikkeamahavainnoille. Tietoturvapolitiikkaa ja sen sisältämiä mittareita arvioidaan ja päivitetään säännöllisesti, jotta varmistetaan sen jatkuva ajantasaisuus ja tehokkuus.

9.3 Toimintaympäristö

Toimintaympäristön eri elementtien tunnistaminen auttaa organisaatiota varmistamaan, että kaikki tekijät, jotka voivat vaikuttaa sen tieto- ja kyberturvallisuuteen, otetaan huomioon. Tämä prosessi mahdollistaa kattavan tietoturvallisuuden hallintajärjestelmän (ISMS) rakentamisen, joka suojaa organisaation tietoja ja resursseja tehokkaasti sekä auttaa täyttämään ISO 27001 -standardin vaatimukset.

Toimintaympäristön tunnistaminen edellyttää organisaation kartoittavan ja ymmärtävän sekä ulkoiset että sisäiset tekijät, sidosryhmien tarpeet ja odotukset sekä tietoturvallisuuteen liittyvät riskit. Näin varmistetaan, että tietoturvatoimenpiteet ovat linjassa liiketoimintatavoitteiden ja -strategian kanssa, ja organisaatio pystyy vastaamaan nopeasti ja tehokkaasti tietoturvauhkien muuttuviin olosuhteisiin. Lisäksi tämä voi parantaa organisaation mainetta ja luottamusta sidosryhmien keskuudessa.

Toimintaympäristön tunnistaminen

Ulkoisten tekijöiden analyysi:

- Lainsäädäntö ja sääntely: mitä lakeja ja määräyksiä organisaation on noudatettava? Esimerkiksi tietosuojalainsäädäntö (GDPR) ja alakohtaiset säädökset.
- Markkinat ja kilpailu: mitkä ovat kilpailutilanteet ja markkinatrendit, jotka voivat vaikuttaa tietoturvallisuuteen?
- Teknologiset kehitykset: mitkä uudet teknologiat tai teknologiset muutokset voivat vaikuttaa organisaation toimintaan ja tietoturvallisuuteen?
- Taloudelliset olosuhteet: mitkä taloudelliset tekijät voivat vaikuttaa organisaation kykyyn ylläpitää tietoturvallisuutta?

Sisäisten tekijöiden analyysi:

- Organisaatiorakenne: miten organisaatio on järjestetty? Ketkä ovat vastuussa tietoturvallisuudesta eri osastoilla?
- Prosessit ja toiminnot: mitkä ovat organisaation keskeiset prosessit ja toiminnot, jotka liittyvät tietoturvallisuuteen?
- Resurssit ja osaaminen: millaisia resursseja ja osaamista organisaatiolla on käytettävissään tietoturvallisuuden varmistamiseksi?
- Tietojärjestelmät ja teknologiat: mitkä tietojärjestelmät ja teknologiat ovat käytössä, ja miten ne tukevat organisaation toimintaa?

Sidosryhmien tunnistaminen:

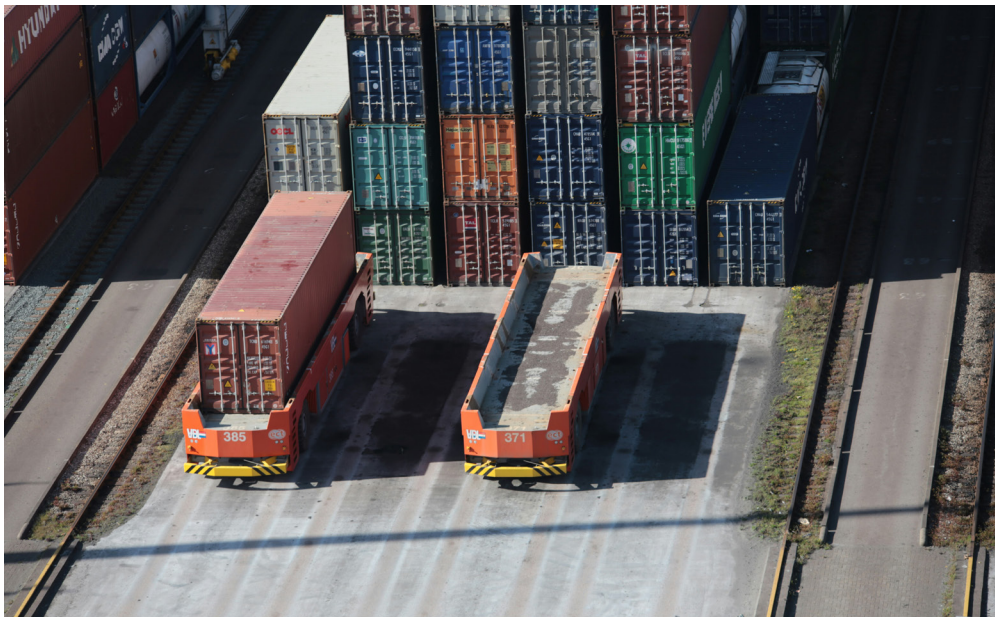
- Sisäiset sidosryhmät: ketkä organisaation sisällä ovat keskeisiä tietoturvallisuuden kannalta? Tämä voi sisältää johdon, IT-osaston, tietoturvatiimin ja muut keskeiset henkilöt.
- Ulkoiset sidosryhmät: ketkä organisaation ulkopuolella vaikuttavat tai ovat riippuvaisia tietoturvallisuudesta? Tämä voi sisältää asiakkaat, toimittajat, yhteistyökumppanit ja viranomaiset.

Riskien ja mahdollisuuksien arviointi:

- Riskien tunnistaminen: mitkä ovat tietoturvallisuuteen liittyvät riskit? Tämä voi sisältää kyberhyökkäyksiä, tietovuotoja ja teknologisia vikoja.
- Mahdollisuuksien tunnistaminen: mitkä ovat mahdollisuudet parantaa tietoturvallisuutta? Tämä voi sisältää uusien teknologioiden käyttöönottoa tai parannuksia prosesseihin ja toimintatapoihin.

Tavoite:

Kattava toimintaympäristötuntemus mahdollistaa proaktiivisen ja ennakoivan sekä vaatimuksenmukaisen toiminnan kyberturvallisuusuhkien hallinnassa varmistaen operatiivisen jatkuvuuden.



9.4 Riskien arviointi

Riskien arviointi on prosessi, jonka avulla organisaatio tunnistaa, analysoi ja arvioi tietoturvariskit. Tämä on keskeinen osa myös riskienhallintaperusteista ISO 27001 -standardia. Riskien arviointi on järjestelmällinen lähestymistapa, jonka avulla organisaatio tunnistaa mahdolliset uhat, arvioi niiden todennäköisyyden ja vaikutuksen, ja määrittää, miten näihin riskeihin tulisi reagoida. Tavoitteena on varmistaa, että tietoturvatoimenpiteet ovat suhteutettuja liiketoiminnalle kohdistuviin riskeihin.

Riskien arviointi auttaa organisaatiota tunnistamaan, mitkä uhat voivat vaikuttaa sen toimintaan. Tämä voi sisältää kyberhyökkäykset, tietovuodot, luonnonkatastrofit ja sisäiset uhat, kuten inhimilliset virheet. Prosessin aikana arvioidaan kunkin riskin todennäköisyys ja mahdollinen vaikutus liiketoimintaan. Tämä auttaa priorisoimaan toimenpiteet ja kohdentamaan resurssit tehokkaasti.

Riskien arvioinnin avulla organisaatio voi siis kohdistaa resurssinsa ja tietoturvatoimenpiteensä niihin alueisiin, joilla on suurin riski. Tämä varmistaa, että resursseja ei käytetä turhaan vähämerkityksisiin uhkiin.

Tunnistamalla ja hallitsemalla riskejä, organisaatio voi parantaa liiketoiminnan jatkuvuutta ja varmistaa, että se pystyy toipumaan nopeasti mahdollisista häiriöistä.

9.4.1 Riskienhallinnan prosessi

Riskien tunnistaminen

Ensimmäinen askel on tunnistaa kaikki mahdolliset riskit, jotka voivat vaikuttaa organisaation tietoturvallisuuteen. Tämä voi tapahtua esimerkiksi SWOT-analyysin haastattelujen ja tarkastusten avulla. SWOT-analyysi on strategisen suunnittelun työkalu, jota käytetään arvioimaan organisaation sisäisiä ja ulkoisia tekijöitä.

- Vahvuudet (Strengths): Organisaation sisäiset tekijät, jotka antavat kilpailuetua.
- Heikkoudet (Weaknesses): Organisaation sisäiset tekijät, jotka heikentävät suorituskykyä.
- Mahdollisuudet (Opportunities): Ulkoiset tekijät, jotka voivat tarjota kasvun tai parantamisen mahdollisuuksia.
- Uhat (Threats): Ulkoiset tekijät, jotka voivat aiheuttaa haittaa tai riskejä organisaatiolle.

SWOT-analyysin avulla organisaatiot voivat tunnistaa strategisia prioriteetteja ja kehittää toimintasuunnitelmia vahvistamalla vahvuuksia, korjaamalla heikkouksia, hyödyntämällä mahdollisuuksia ja minimoimalla uhkia.

Riskien arviointi: Arvioidaan kunkin riskin todennäköisyys ja vaikutus. Tämä auttaa ymmärtämään, mitkä riskit ovat merkittävimpiä ja vaativat eniten huomiota.

Riskien hallinta: Kehitetään strategiat ja toimenpiteet riskien hallitsemiseksi. Tämä voi sisältää riskin välttämistä, vähentämistä, siirtämistä (esimerkiksi vakuutusten avulla) tai hyväksymistä.

Toimenpiteiden suhteuttaminen: Toimenpiteet suunnitellaan ja toteutetaan suhteessa arvioituihin riskeihin. Suurimmille riskeille varataan enemmän resursseja ja tiukempia toimenpiteitä, kun taas vähäisemmille riskeille riittävät kevyemmät toimenpiteet.

Esimerkki

Organisaatio tunnistaa riskin, jossa työntekijän inhimillinen virhe voi johtaa tietovuotoon. Riskiperustainen arviointi voisi näyttää tältä:

- Tunnistaminen:
  - Inhimillinen virhe tiedon käsittelyssä.

- Arviointi:
  - Todennäköisyys: keskitaso
  - Vaikutus: korkea (liiketoiminnan maine ja luottamus kärsivät)

- Hallinta:
  - Välttäminen: Koulutetaan henkilöstöä paremmin
  - Vähentäminen: Otetaan käyttöön automaattiset tarkistusjärjestelmät
  - Siirtäminen: Otetaan käyttöön vakuutuksia tietovuotojen varalta
  - Hyväksyminen: Hyväksytään pieni jäännösriski, jota ei voida poistaa kokonaan.

Yhteenveto

Riskien arviointi on keskeinen osa ISO 27001 -standardia ja tärkeä prosessi organisaation tietoturvallisuuden varmistamiseksi. Se auttaa tunnistamaan ja hallitsemaan tietoturvariskejä tehokkaasti, kohdentamaan resurssit oikein ja parantamaan liiketoiminnan jatkuvuutta. Riskiperustainen lähestymistapa varmistaa, että tietoturvatoimenpiteet ovat suhteutettuja liiketoiminnalle kohdistuvaan riskiin, mikä tekee niistä taloudellisesti järkeviä ja tehokkaita.

Organisaation tulee tunnistaa toimintaympäristöönsä kohdistuvat tieto- ja kyberturvallisuusriskit, jotta niitä voidaan hallita tehokkaasti.

- Määritä riskeille toimintaympäristöön soveltuva arviointiprosessi.
- Laadi ja ylläpidä toimintaan soveltuvat riski- ja priorisointikriteerit.
- Määritä riskien hallintakeinot.
- Määritä riskien hyväksyntäkriteerit ja -prosessi.
- Tunnista ja arvioi toimintaan kohdistuvat realistiset riskit.
- Analysoi riskien vaikuttavuus todennäköisyyden, seurausten sekä toistettavuuden näkökulmista.
- Määritä riskeille omistaja – myös jäännösriskeille sekä käsittelysuunnitelma.
- Käytä riskienhallintaan selkeää ja vertailtavuuden mahdollistavaa dokumentointitapaa.

Tavoite

Meriklusteritoimijoiden OT-tietoturva- ja kyberriskien arvioinnin päämääränä on varmistaa operatiivisten teknologioiden turvallisuus ja jatkuvuus. Tämä saavutetaan suojaamalla kriittiset järjestelmät ja tiedot, kuten navigointi- ja viestintäjärjestelmät, kyberuhkilta ja tietomurroilta.

Tavoitteena on minimoida toimintakatkoksista ja tietovuodoista aiheutuvat riskit, taata merenkulun turvallisuus ja tehokkuus sekä ylläpitää sidosryhmien luottamus. Tämä edellyttää jatkuvaa valvontaa, riskien arviointia ja nopeaa reagointia mahdollisiin uhkiin.

9.4.2 Skenaariopohjainen riskienarviointi

Meriklusteritoimijoiden riskienarvioinnissa erilaisten skenaarioiden pohtiminen on hyödyllistä, koska se auttaa tunnistamaan ja ymmärtämään monimutkaisia ja usein ennakoimattomia riskejä, jotka voivat vaikuttaa toiminnan jatkuvuuteen ja turvallisuuteen. Skenaariotyöskentely tarjoaa syvällisemmän näkemyksen mahdollisista uhkista, heikkouksista ja häiriötilanteista, jotka voivat kohdata meriliikenteen, satamien ja logistiikkaketjujen toimijoita.

Kun tarkastellaan erilaisia skenaarioita, voidaan valmistautua paremmin kyberhyökkäyksiin, luonnonkatastrofeihin, toimitusketjujen katkoksiin ja muihin kriittisiin tapahtumiin. Tämä menetelmä auttaa tunnistamaan myös piileviä riskejä ja mahdollistaa ennakoivien toimenpiteiden suunnittelun ja käyttöönoton. Skenaarioesimerkkien avulla pyritään valottamaan konkreettisesti, millaisia tilanteita voi syntyä ja miten niihin voidaan varautua tehokkaasti.

9.4.2.1 Skenaario 1: Kyberhyökkäys sataman kontinkäsittelyjärjestelmään

Tausta

Satamaoperaattori käyttää OT-järjestelmää (Operational Technology) konttien käsittelyyn ja varastointiin. Järjestelmä on keskeinen sataman toiminnan sujuvuuden kannalta. Se hallinnoi automaattisia nostureita ja kuljetusvälineitä, jotka siirtävät kontteja laivojen ja varastoalueiden välillä.

Tunnistaminen

Organisaatio tunnistaa, että kyberhyökkäys voi kohdistua kontinkäsittelyjärjestelmään, mikä voisi aiheuttaa vakavia toimintahäiriöitä ja turvallisuusriskejä.

Arviointi

Todennäköisyys: keskitaso. Kyberhyökkäykset sataman infrastruktuuriin ovat mahdollisia, mutta satamalla on jo olemassa perustason tietoturvatoimenpiteitä.

Vaikutus: korkea. Järjestelmän kaatuminen tai manipulointi voisi johtaa suurten konttimäärien virheelliseen käsittelyyn, mikä aiheuttaisi merkittäviä logistisia viiveitä ja taloudellisia menetyksiä sekä mahdollisia turvallisuusriskejä työntekijöille.

Hallinta ja toimenpiteet

- **Välttäminen:**
  - Toimenpiteet: parannetaan sataman kyberturvallisuuskoulutusta henkilöstölle, erityisesti niille, jotka ovat vastuussa OT-järjestelmien käytöstä ja valvonnasta.
  - Perustelu: koulutettu henkilöstö pystyy tunnistamaan ja reagoimaan nopeasti epäilyttäviin toimintoihin.

- **Vähentäminen:**
  - Toimenpiteet: otetaan käyttöön edistyksellisiä palomuureja ja tunkeutumisen havaitsemisjärjestelmiä (IDS) erityisesti kontinkäsittelyjärjestelmissä.
    - Perustelu: nämä teknologiat voivat havaita ja estää epäilyttävän liikenteen ja hyökkäykset ennen kuin ne aiheuttavat vahinkoa.

- **Siirtäminen:**
  - Toimenpiteet: hankitaan kybervakuutus, joka kattaa mahdolliset taloudelliset menetykset kyberhyökkäyksen sattuessa.
  - Perustelu: vakuutus voi tarjota taloudellista suojaa ja tukea palautumisprosessissa.

- **Hyväksyminen:**
  - Toimenpiteet: määritetään jäännösriski, jota ei voida täysin eliminoida, ja valmistellaan kriisinhallintasuunnitelma, joka sisältää selkeät ohjeet hyökkäystilanteen varalle.
  - Perustelu: vaikka kaikki riskit eivät ole täysin hallittavissa, kriisinhallintasuunnitelma varmistaa nopean ja tehokkaan reagoinnin.

9.4.2.2 Skenaario 2: Laitevika aluksen navigointijärjestelmässä

Tausta

Merikuljetusyritys käyttää kehittynyttä OT-järjestelmää alusten navigointiin ja reittisuunnitteluun. Järjestelmä varmistaa alusten turvallisen ja tehokkaan liikkumisen merellä.

Tunnistaminen

Organisaatio tunnistaa, että navigointijärjestelmän laitevika voi aiheuttaa aluksen ohjauksen menettämisen, mikä voisi johtaa törmäyksiin tai eksymiseen.

Arviointi

Todennäköisyys: matala. Laiteviat navigointijärjestelmissä ovat harvinaisia hyvin ylläpidetyissä järjestelmissä, mutta ne voivat silti tapahtua.

Vaikutus: erittäin korkea. Laitevika navigointijärjestelmässä voi johtaa vakaviin onnettomuuksiin, ympäristövahinkoihin ja ihmishenkien menetyksiin.

Hallinta ja toimenpiteet

- **Välttäminen:**
  - Toimenpiteet: säännölliset huolto- ja tarkastustoimenpiteet navigointijärjestelmille.
  - Perustelu: ennakoiva huolto vähentää laitevikojen todennäköisyyttä ja varmistaa, että järjestelmät toimivat optimaalisesti.

- **Vähentäminen:**
  - Toimenpiteet: otetaan käyttöön redundanttiset järjestelmät, jotka voivat ottaa navigointijärjestelmän tehtävät haltuunsa laitevian sattuessa.
  - Perustelu: redundanssi varmistaa, että navigointijärjestelmä voi jatkaa toimintaansa, vaikka yksi osa siitä pettäisi.

- **Siirtäminen:**
  - Toimenpiteet: laajennetaan laitevakuutusta kattamaan navigointijärjestelmien viat.
  - Perustelu: vakuutus voi auttaa kattamaan korjauskustannuksia ja taloudellisia menetyksiä, jos laitevika tapahtuu.

- **Hyväksyminen:**
    - o Toimenpiteet: kehitetään yksityiskohtainen jatkuvuussuunnitelma, joka sisältää toimenpiteet ja vastuut laitevian sattuessa.
    - o Perustelu: vaikka laitevikojen todennäköisyys on matala, jatkuvuussuunnitelma varmistaa nopean ja organisoidun reagoinnin.

Näissä skenaarioissa riskiperustainen arviointi auttaa organisaatiota suunnittelemaan ja toteuttamaan toimenpiteitä, jotka ovat suhteutettuja liiketoiminnan riskeihin, varmistaen turvallisuuden ja tehokkuuden kriittisissä OT-järjestelmissä merilogistiikassa.

9.5 Organisointi ja osaaminen

Tieto- ja kyberturvallisuuden hallintajärjestelmässä yksi keskeisistä osa-alueista on organisaation ja osaamisen hallinta. Tämä tarkoittaa sitä, että organisaation tulee varmistaa, että sillä on riittävät resurssit ja osaaminen tietoturvallisuuden hallintajärjestelmän (ISMS) suunnitteluun, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen.

Jotta organisointi ja osaamisen hallinta olisivat mahdollisia, tulee organisaation varmistaa, että:

- sillä on tarpeeksi henkilöstöä hoitamaan tietoturvatehtäviä
- henkilöstö on osaavaa tietoturvallisuuden eri osa-alueilla
- jokaisella henkilöllä on selkeä ja dokumentoitu rooli ja vastuut tietoturvan hallinnassa
- henkilöstön osaamista kehitetään ja päivitetään jatkuvasti.

Resurssoinnin merkitys korostuu erityisesti tietoturvan hallintajärjestelmän onnistuneessa perustamisessa ja käytössä. Ilman riittäviä resursseja ja osaamista organisaatio ei pysty tehokkaasti hallitsemaan tietoturvariskejä. Puutteet resurssoinnissa ja osaamisessa voivat johtaa merkittäviin riskeihin, kuten tietovuotoihin, kyberhyökkäyksiin ja toimintakatkoksiin.

Riittävä henkilöresursointi:

Riittävä henkilöstömäärä varmistaa, että kaikki tietoturvan hallintajärjestelmän osa-alueet voidaan hoitaa tehokkaasti. Puutteellinen henkilöstömäärä voi johtaa siihen, että tietoturvatehtäviä ei ehditä hoitaa kunnolla, mikä lisää riskiä tietoturvaloukkauksille.

Osaaminen ja koulutus:

Henkilöstön tulee olla koulutettu ymmärtämään ja tunnistamaan tietoturvariskejä sekä toteuttamaan tarvittavia toimenpiteitä. Osaamisen puute voi johtaa virheisiin ja heikkoon tietoturvauhkien reagointiin. Tämä voi vaarantaa koko organisaation tietoturvan.

Selkeät roolit ja vastuut:

Selkeät roolit ja vastuut varmistavat, että jokainen tietää, mitä heiltä odotetaan tietoturvan hallinnassa. Epäselvät roolit ja vastuut voivat johtaa siihen, että tärkeitä tehtäviä jää tekemättä tai tehdään puutteellisesti.

Jatkuva kehittäminen:

Tietoturvauhkat sekä toimintaympäristö kehittyvät jatkuvasti, joten myös henkilöstön osaamista täytyy jatkuvasti päivittää. Ilman jatkuvaa koulutusta henkilöstön taidot voivat vanhentua, mikä tekee organisaation haavoittuvaisemmaksi uusille uhille.

9.5.1 Esimerkki: Merilogistiikan OT-järjestelmät

Resurssien ja osaamisen merkitys merilogistiikan yrityksessä, joka käyttää operatiivisia teknologioita (OT) alusten navigointiin ja sataman toimintojen hallintaan.

Henkilöstö:

- Organisaation tulee varmistaa, että sillä on tarpeeksi henkilöstöä valvomaan ja ylläpitämään OT-järjestelmiä.

Koulutus:

- Henkilöstön tulee ymmärtää, miten OT-järjestelmät toimivat, mitkä ovat niiden haavoittuvuudet ja miten niitä suojataan.

Roolit ja vastuut:

- Selkeät roolit ja vastuut takaavat, että jokainen tietää tehtävänsä esimerkiksi laitevian tai kyberhyökkäyksen sattuessa.

Jatkuva kehitys:

- Henkilöstön on osallistuttava säännöllisesti koulutuksiin ja harjoituksiin, jotta heidän tietonsa ja taitonsa pysyvät ajan tasalla.

Yhteenveto

ISO 27001 -standardin organisaation ja osaamisen hallinnan osuus korostaa riittävien resurssien ja osaamisen merkitystä. Puutteet näissä alueissa muodostavat merkittävän riskin tietoturvan hallintajärjestelmän onnistuneelle perustamiselle ja käytölle. Varmistamalla riittävän henkilöstömäärän, asianmukaisen koulutuksen ja jatkuvan kehittämisen organisaatio voi tehokkaasti hallita tietoturvariskejä ja suojata kriittisiä tietojaan.

Organisaatio

- määrittää, minkälaista tieto- ja kyberturvallisuusosaamista OT-ympäristön suojaaminen vaatii
- varmistaa, että vastuuhenkilöillä on riittävä osaaminen tai oikeanlaista koulutusta saatavilla
- huolehtii kattavan tietoisuuden rakentamisesta organisaation eri tasoille esimerkiksi tietoisuusohjelman kautta, jotta henkilöstöllä on riittävä käsitys organisaatioon ja toimintoihin kohdistuvista uhkista.
- varmistaa, että jokainen organisaation jäsen tunnistaa roolinsa ja keinonsa tietoturvallisuuden parantamiseksi organisaatiossa
- varmistaa, että henkilöstö ymmärtää tietoturvapolitiikan vastaisen toiminnan seuraukset organisaation toiminnalle ja jatkuvuudelle
- teettää taustatutkimukset avaintehtävissä oleville henkilöille.

Tavoite

Organisoinnin ja osaamisen varmistamisen tavoitteena on varmistaa, että organisaation jäsenillä on selkeä ymmärrys omasta roolistaan ja vastuistaan tietoturvan ylläpitämisessä ja parantamisessa. Päällekkäisten vastuiden karsiminen ja vastuuaukkojen sekä osaamisvajeiden tunnistaminen on mahdollista näillä toimenpiteillä.

9.6 Omaisuuden hallinta

Omaisuuden hallinta tarkoittaa kaikkien organisaation tietovarojen, kuten laitteiden, ohjelmistojen, tietojen ja palveluiden, tunnistamista, luokittelua ja suojaamista. Tämä sisältää myös resurssien hallinnan, niiden käytön valvonnan ja suojatoimien toteuttamisen, jotta tietojen luottamuksellisuus, eheys ja saatavuus varmistetaan. Omaisuuden hallinta sisältää siis sekä fyysisen että virtuaalisen omaisuuden, kuten immateriaalioikeudet (IPR), operatiivisen tiedon ja liiketoimintatiedon.

Lyhyesti

- Luetteloi omaisuus ja määritä omistajuus niiden kriittisyyden mukaan.
- Luokittele tieto organisaation tietoturvaperiaatteiden mukaisesti.
- Päivitä luetteloa säännöllisesti.
- Määritä tiedon ja järjestelmien käyttösäännöt ohjeistamalla selkeästi käyttöperiaatteet.
- Huolehdi, että tieto- ja muu omaisuus ja niiden luokitus on merkitty selkeästi.
- Varmista, että tiedon siirtämisellä ja käsittelyllä on selkeä prosessi.
- Varmista, että tieto- tai muuta omaisuutta ei jää sellaisen haltuun, jolla ei siihen ole oikeutta tai oikeus päättyy.

Fyysinen omaisuus sisältää laitteet, kuten tietokoneet, palvelimet, tietoverkot ja muut fyysiset laitteet, joita käytetään tietojen käsittelyyn ja tallentamiseen. Fyysisen omaisuuden hallinta varmistaa, että nämä laitteet ovat asianmukaisesti suojattuina varkauksilta, fyysisiltä vahingoilta ja luonnonkatastrofeilta.

Virtuaalinen omaisuus kattaa digitaalisen tiedon, kuten liiketoimintatiedot, asiakastiedot, immateriaalioikeudet (IPR), ja operatiiviset tiedot. Virtuaalisen omaisuuden hallinta varmistaa, että tiedot ovat suojattuja luvattomalta pääsyltä, muutoksilta ja häviämiseltä.

Fyysisen omaisuuden, kuten tietokoneiden ja palvelimien, menettäminen voi johtaa merkittäviin tietovuotoihin ja toimintahäiriöihin. Virtuaalisen omaisuuden, kuten liiketoimintatiedon, menettäminen tai väärinkäyttö voi aiheuttaa taloudellisia menetyksiä ja vahingoittaa organisaation mainetta.

Hyvin hallittu omaisuus auttaa varmistamaan, että organisaatio pystyy jatkamaan toimintaansa myös poikkeustilanteissa, kuten kyberhyökkäyksen tai luonnonkatastrofin sattuessa. Erityisen tärkeää on operatiivisten tietojen suojelu, jotta kriittiset toiminnot voivat jatkua keskeytyksettä.

9.6.1 Esimerkki 1: Sataman valvontajärjestelmät

- **Fyysinen omaisuus:** sataman valvontakamerat ja turvajärjestelmät.
- **Virtuaalinen omaisuus:** valvontakameran tallenteet ja turvallisuuteen liittyvä data.
- **Merkitys:** sataman valvontajärjestelmät ovat kriittisiä turvallisuuden kannalta. Fyysisen valvontakameran vaurioituminen tai virtuaalisten tallenteiden menettäminen voisi johtaa turvallisuusaukkoihin, mahdollisiin varkauksiin ja kyvyttömyyteen seurata tapahtumia tarkasti.

9.6.2 Esimerkki 2: Aluksen navigointijärjestelmä

- **Fyysinen omaisuus:** aluksen navigointilaitteet, kuten tutkat ja GPS-järjestelmät.
- **Virtuaalinen omaisuus:** navigointidata ja reittisuunnitelmat.
- **Merkitys:** navigointijärjestelmän fyysinen vahingoittuminen voi estää alusta navigoimasta turvallisesti, mikä voi johtaa törmäyksiin tai eksymiseen. Virtuaalisen navigointidatan menettäminen tai manipulointi voisi johtaa vääriin reittisuunnitelmiin, mikä vaarantaa aluksen ja miehistön turvallisuuden sekä aiheuttaa logistisia viiveitä.

Tavoite ja yhteenveto

Meriklusteritoimijoiden omaisuuden hallinta keskittyy erityisesti merenkulun ja logistiikan kriittisiin infrastruktuureihin, kuten laivoihin, satamiin ja navigointijärjestelmiin. Tavoitteena on suojata näitä resursseja kyberuhkilta ja toimintahäiriöiltä, taaten turvallinen ja tehokas operointi merellä.

Omaisuuden hallinta ISO 27001 -standardissa kattaa sekä fyysisen että virtuaalisen omaisuuden, jotka ovat elintärkeitä organisaation toiminnan jatkuvuuden ja turvallisuuden kannalta. Ilman asianmukaista omaisuuden hallintaa organisaatiot voivat kohdata merkittäviä riskejä, kuten tietovuotoja, taloudellisia menetyksiä ja mainehaittoja. Merilogistiikan esimerkit korostavat, kuinka tärkeää on suojata sekä fyysisiä laitteita että digitaalista tietoa turvallisuuden ja toiminnan sujuvuuden varmistamiseksi.

9.7 Pääsynhallinta

Pääsynhallinta on keskeinen osa tietoturvallisuuden hallintaa, erityisesti ISO 27001 -standardin mukaisessa tietoturvallisuuden hallintajärjestelmässä (ISMS). Se varmistaa, että vain valtuutetut henkilöt pääsevät käsiksi organisaation järjestelmiin ja tietoihin, mikä suojaa arkaluontoista tietoa luvattomalta pääsyltä ja väärinkäytöltä.

Pääsynhallinnan keskeiset periaatteet

Pääsy vain tarpeeseen perustuen: tämä tarkoittaa, että vain henkilöt, joiden työtehtävät sitä edellyttävät, pääsevät käsiksi järjestelmiin ja tietoihin. Tämä on tärkeää, koska rajoittamalla pääsyä minimoidaan riski tietojen väärinkäytöstä tai luvattomasta pääsystä.

Käyttöoikeuksien myöntäminen ja tunnistautuminen: käyttöoikeuksien myöntämiselle, tunnistautumiselle ja vastuisiin on oltava selkeä prosessi. Tämä varmistaa, että käyttöoikeudet myönnetään asianmukaisesti ja että pääsy voidaan jäljittää tarvittaessa.

Rajoitetut käyttö- ja ylläpito-oikeudet: laajoja käyttö- ja ylläpito-oikeuksia rajoitetaan ja valvotaan. Tämä vähentää riskiä, että yksittäinen käyttäjä voi vahingoittaa järjestelmää tai käyttää tietoja väärin.

Roolipohjainen ja kerroksellinen pääsynhallinta: roolipohjainen ja kerroksellinen pääsynhallinta varmistaa, että pääsy on rajoitettu vain niihin tietoihin, joita tarvitaan työtehtävien suorittamiseen.

Pääsyoikeuksien katselmointiprosessi: pääsyoikeuksia tarkastellaan säännöllisesti vanhentuneiden oikeuksien poistamiseksi. Tämä varmistaa, että vain ajantasaiset ja tarpeelliset käyttöoikeudet säilyvät voimassa.

Pääsyoikeuksien poistaminen työsuhteen päättyessä: on tärkeää varmistaa, että organisaatiosta poistuvalle henkilölle ei jää pääsyoikeuksia. Tämä estää entisiä työntekijöitä käyttämästä tietoja väärin tai pääsemästä käsiksi arkaluontoisiin tietoihin työsuhteen päätyttyä.

Pääsyn valvonta ja lokitus: pääsyä järjestelmiin valvotaan ja lokitetaan. Tämä mahdollistaa epäilyttävän toiminnan havaitsemisen ja tutkimisen.

Toiminta rajoittavissa järjestelmissä: jos järjestelmässä ei voida teknisesti toteuttaa nykyaikaisia ja laadukkaita pääsynhallintamekanismeja, voidaan soveltaa seuraavia strategioita:

- **Manuaaliset kontrollit:** käytetään manuaalisia prosesseja ja tarkistuslistoja varmistamaan, että vain valtuutetut henkilöt pääsevät järjestelmiin ja tietoihin.
  - Nimetään vastuuhenkilöt, jotka tarkistavat ja valvovat pääsyä säännöllisesti.

- **Fyysinen turvallisuus:**
  - Varmistetaan fyysinen pääsynvalvonta tiloihin, joissa järjestelmät sijaitsevat.
  - Käytetään lukkoja, kulunvalvontajärjestelmiä ja valvontakameroita.

- **Koulutus ja tietoisuus:**
  - Koulutetaan henkilöstöä tietoturvakäytännöistä ja korostetaan heidän rooliaan tietoturvan varmistamisessa.
  - Säännölliset koulutukset ja tietoisuuskampanjat tietoturva-aiheista.

- **Säännölliset auditoinnit:**
  - Suoritetaan säännöllisiä auditointeja käyttöoikeuksien ja pääsyvalvonnan tarkistamiseksi.
  - Ulkopuoliset tai sisäiset auditoinnit, joissa tarkastetaan järjestelmien käyttöoikeudet ja niiden valvonta.

9.7.1 Esimerkki 1: Aluksen vanhentunut navigointijärjestelmä

Tilanne: aluksen navigointijärjestelmä on vanha eikä tue nykyaikaisia pääsynhallintamekanismeja.

Ratkaisu: käytetään fyysistä pääsynvalvontaa aluksen komentosillalle, missä navigointijärjestelmä sijaitsee. Vain valtuutetuilla henkilöstön jäsenillä on pääsy komentosillalle. Lisäksi manuaaliset tarkistuslistat varmistavat, että vain valtuutetut henkilöt voivat käyttää järjestelmää.

9.7.2 Esimerkki 2: Sataman lastinkäsittelyjärjestelmä

Tilanne: sataman lastinkäsittelyjärjestelmä on integroitu useisiin vanhoihin järjestelmiin, joihin ei voida helposti lisätä nykyaikaisia pääsynhallintamekanismeja.

Ratkaisu: otetaan käyttöön manuaaliset kontrollit ja tarkistuslistat, jotka tarkastetaan säännöllisesti. Fyysinen pääsynvalvonta varmistetaan käyttämällä kulunvalvontajärjestelmiä satama-alueella. Henkilöstö koulutetaan tietoturvakäytännöistä ja säännölliset auditoinnit varmistavat käyttöoikeuksien ajantasaisuuden.

Tavoite

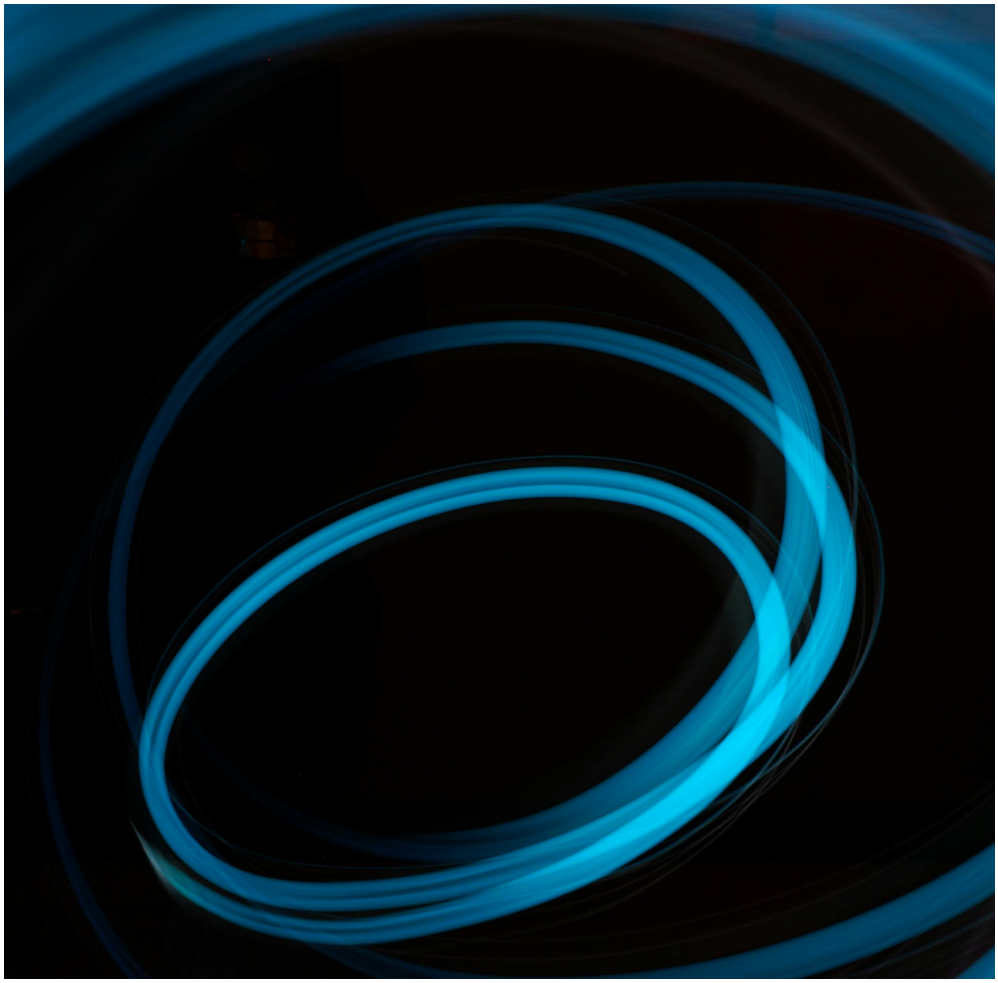
Pääsynhallinnan tavoitteena on varmistaa, että vain valtuutetut henkilöt ja järjestelmät pääsevät käsiksi kriittisiin tietoihin ja järjestelmiin. Tämä suojaa järjestelmiä kyberuhkilta, estää luvattoman käytön ja mahdollistaa nopean reagoinnin mahdollisiin tietoturvaloukkauksiin. Tavoitteena on ylläpitää operatiivinen turvallisuus ja luotettavuus merenkulun toimintaympäristössä.

Yhteenveto

Pääsynhallinta tarkoittaa kriittisten järjestelmien ja laitteiden käyttöoikeuksien hallintaa ja valvontaa. Tämä käsittää mm. laivojen navigointi- ja viestintäjärjestelmät, satamalaitteet sekä merenkulun logistiikkajärjestelmät.

Jos nykyaikaisia pääsynhallintamekanismeja ei voida toteuttaa, manuaaliset kontrollit, fyysinen turvallisuus, koulutus ja säännölliset auditoinnit voivat auttaa varmistamaan tietojen ja järjestelmien turvallisuuden. Näin voidaan tehokkaasti hallita pääsyä myös rajoittavissa järjestelmissä ja vähentää tietoturvariskejä.

- Varmista, että pääsy järjestelmiin ja tietoihin on vain niillä, joille pääsy kuuluu työtehtäviin perustuen.
- Varmista, että prosessi käyttöoikeuksien ja pääsyn myöntämiseen, tunnistautumiseen ja vastuisiin on olemassa ja toimiva.
- Varmista, että laajoja käyttö- ja ylläpito-oikeuksia rajoitetaan ja valvotaan.
- Käytä roolipohjaista ja kerroksellista pääsynhallintaa, jolla varmistetaan, että yhdellä käyttöoikeudella ei ole pääsyä laajoihin tietomassoihin.
- Määritä pääsyoikeuksien katselmointiprosessi, joka toteutuu määräajoin vanhentuneiden oikeuksien havaitsemiseksi ja poistamiseksi.
- Varmista, että organisaatiosta poistuvalle henkilölle ei jää pääsyoikeuksia.
- Valvo ja lokita pääsyä järjestelmiin.



9.8 Fyysinen turvallisuus

Fyysinen turvallisuus meriklusterin toimintaympäristössä kattaa toimenpiteet, kuten valvontakamerat, turvaovet ja kulunvalvontajärjestelmät, jotka suojaavat kriittisiä operatiivisia järjestelmiä, tallennusvälineitä ja infrastruktuuria fyysisiltä uhilta ja vahingoilta. Näillä toimenpiteillä ehkäistään riskejä, kuten luonnonkatastrofeja, ilkivaltaa, varkauksia ja muita fyysisiä uhkia, ja varmistetaan, että organisaation tiedot ja tietojärjestelmät säilyvät suojattuina ja toimintakykyisinä.

Fyysinen turvallisuus varmistaa, että vain valtuutetut henkilöt pääsevät organisaation tiloihin ja laitteisiin. Samalla estetään luvaton pääsy, joka voisi johtaa tietojen varastamiseen, vahingoittamiseen tai väärinkäyttöön. Kun suojataan kriittiset fyysiset resurssit ja tilat, voidaan varmistaa, että organisaation toiminta jatkuu keskeytyksettä. Tämä on erityisen tärkeää poikkeustilanteissa, kuten tulipalojen tai muiden onnettomuuksien sattuessa.

Fyysiset toimenpiteet täydentävät muita tietoturvatoimenpiteitä ja varmistavat tietojen luottamuksellisuuden, eheyden ja saatavuuden.

Keskeiset toimenpiteet:

Varmista, että kriittiset tilat, kuten palvelinhuoneet, ovat lukittuja ja niihin pääsee vain valtuutetut henkilöt. Käytä sähköisiä kulunvalvontajärjestelmiä, jotka tallentavat kaikkien tiloihin päässeiden henkilöiden tiedot. Asenna valvontakameroita kriittisiin paikkoihin, kuten pääsisäänkäynteihin ja palvelinhuoneisiin, ja varmista, että ne ovat jatkuvasti toiminnassa. Käytä tarvittaessa turvapartioita, jotka tarkastavat tilat säännöllisesti.

Ympäristön suojaaminen:

Asenna palohälyttimiä ja sammutusjärjestelmiä kriittisiin tiloihin. Varmista, että palvelinhuoneet ja muut laitteet pysyvät optimaalisissa lämpötiloissa ja kosteustasoissa.

Laitteiden hallinta:

- Merkitse kaikki kriittiset laitteet ja pidä yllä ajantasaista laiteluetteloa. Käytä turvallisia menetelmiä laitteiden hävittämiseen, jotta tiedot eivät päädy vääriin käsiin.
- Sijoita laitteet niin, että niitä on mahdollista suojata.
- Käytä valvontakameroita, pääsynvalvontaa ja muita mahdollisia kontrolleja tilojen ja laitteiden suojaamiseksi.
- Varmista, että kriittisiin tiloihin pääsee vain oikeutetut tahot.
- Huolehdi, että laitteet ja tilat ovat suojattuja kosteudelta, pölyltä ja muilta ympäristötekijöiltä.
- Varmista, että fyysisiä tallennusvälineitä käytetään hallitusti, luokitteluperiaatteiden mukaisesti ja käyttöä sekä luovutusta valvotaan.
- Varmista, että käytöstä poistuvat laitteet tuhotaan tai kierrätetään organisaation politiikan mukaisesti ja että ne eivät sisällä organisaation tietoja.
- Suojaa tietoa siirtävä kaapelointi vahingoittumiselta ja epäasialliselta pääsyltä.
- Varmista, että huoltotoimenpiteet tapahtuvat tietoturvallisesti ja että kolmas osapuoli toteuttaa organisaation tietoturvapolitiikassa asetettuja vaatimuksia.

9.8.1 Esimerkki 1: Sataman valvontajärjestelmät

- **Tilanne:**
  - Satamassa käytetään valvontakameroita ja kulunvalvontajärjestelmiä, jotta vain valtuutetut henkilöt pääsevät kriittisille alueille, kuten lastinkäsittelyalueille ja varastoihin.
- **Varmista:**
  - että sataman toiminta pysyy turvallisena ja estää luvattoman pääsyn, joka voisi johtaa varkauksiin tai sabotaasiin.

9.8.2 Esimerkki 2: Aluksen komentosilta

- **Tilanne:**
  - Aluksen komentosilta, jossa sijaitsevat navigointi- ja viestintäjärjestelmät, on lukittu ja siihen pääsee vain valtuutettu miehistön jäsen.
- **Suojaa:**
  - aluksen kriittisiä järjestelmiä ja varmistaa, että vain koulutettu ja valtuutettu henkilöstö voi käyttää navigointi- ja viestintälaitteita, mikä on tärkeää aluksen turvallisuuden kannalta.

Tavoite

Tavoitteena on varmistaa, että laitteistot ja infrastruktuurit, kuten laivojen navigointi- ja viestintäjärjestelmät sekä satamalaitteet, pysyvät ehjinä ja toimintakykyisinä. Fyysisen turvallisuuden avulla estetään luvaton pääsy ja vahingonteko, mikä tukee operatiivista jatkuvuutta ja turvallisuutta merenkulussa.

Yhteenveto

Fyysinen turvallisuus ISO 27001 -standardissa on ratkaisevan tärkeä organisaation tietoturvallisuuden varmistamiseksi. Se suojaa fyysiset laitteet ja tilat luvattomalta pääsyltä ja vahingoilta, mikä auttaa ylläpitämään tietojen luottamuksellisuutta, eheyttä ja saatavuutta. Fyysisen turvallisuuden toimenpiteet, kuten lukitut tilat, kulunvalvontajärjestelmät, valvontakamerat ja ympäristönsuojelu, ovat kaikki tärkeitä osia kattavassa tietoturvallisuuden hallintajärjestelmässä.

9.9 Operointi ja järjestelmäkehitys

Operointiturvallisuus ja järjestelmäkehitys meriklusteriympäristössä tarkoittavat toimenpiteitä ja käytäntöjä, joilla varmistetaan kriittisten operatiivisten teknologioiden ja järjestelmien turvallinen ja luotettava toiminta. Toimenpiteet kattavat käytännöt ja prosessit, joilla organisaatio varmistaa, että sen IT-järjestelmät ja -palvelut toimivat turvallisesti ja tehokkaasti sekä kehittyvät tietoturvallisuuden kannalta kestävällä tavalla.

Organisaation tulee määritellä ja ottaa käyttöön tietoturvakäytännöt ja menettelytavat, jotka kattavat IT-järjestelmien päivittäisen käytön. Säännölliset varmuuskopiot ja testatut palautusprosessit ovat välttämättömiä tietojen ja järjestelmien jatkuvuuden varmistamiseksi.

Näin varmistetaan, että tiedot voidaan palauttaa nopeasti ja luotettavasti tietoturvaloukkauksen tai teknisen vian sattuessa. Tietoturvakäytäntöihin kuuluu muun muassa käyttöoikeuksien hallinta, varmuuskopioiden tekeminen, järjestelmien päivittäminen ja tietoturvauhkien seuranta.

Operointiturvallisuus kattaa laivojen, satamien ja muiden merenkulun infrastruktuurien päivittäiset toiminnot.

- Varmista, että päivittäinen operointi tapahtuu organisaation määrittämien vaatimusten mukaisesti.
- Varmista, että ohjelmistopäivitykset tapahtuvat automatisoidusti tai muuten säännöllisesti järjestelmissä, joissa se on mahdollista.
- Varmista, että haavoittuvuuksienhallinnalle on olemassa prosessi.
- Varmista, että prosesseihin kohdistuu valvontaa ja säännöllisiä auditointeja.
- Varmista, että tietoturva on huomioitu jokaisessa kehitysvaiheessa ja prosessissa.
- Huolehdi, että varmuuskopiot otetaan säännöllisesti ja niitä säilytetään eri palotilassa.
- Suorita säännöllisiä testauksia ja harjoittele toipumista ja palautumista häiriötilanteesta.

Tavoite

Operointiturvallisuudella varmistetaan operaatioiden jatkuvuus ja merenkulun tehokkuus, suojaten samalla ihmishenkiä ja ympäristöä.

9.9.1 Keskeiset järjestelmäkehityksen ja operoinnin toimenpiteet

1. **Turvallinen ja luotettava toiminta:** Operoinnin käytännöt varmistavat, että IT-järjestelmät toimivat luotettavasti ja turvallisesti päivittäisessä käytössä. Tämä minimoi toimintakatkosten ja tietoturvaloukkausten riskiä.

2. **Tietoturvariskien hallinta kehityksessä:** Järjestelmäkehityksen prosessit varmistavat, että tietoturvariskit otetaan huomioon jo järjestelmien suunnittelu- ja kehitysvaiheessa. Tämä auttaa rakentamaan turvallisia ja kestäviä IT-ratkaisuja.

3. **Jatkuva parantaminen:** Sekä operointi että järjestelmäkehitys tukevat jatkuvan parantamisen periaatetta, joka on keskeinen osa ISO 27001 -standardia. Ne mahdollistavat järjestelmien ja prosessien jatkuvan arvioinnin ja parantamisen tietoturvan näkökulmasta.

4. **Järjestelmien käytön seuranta ja lokitus:** Seurannalla havaitaan epäilyttävä toiminta ja mahdollistetaan nopea reagointi. Se kattaa järjestelmäpäivitykset, virheiden ja poikkeamien lokituksen sekä käyttöoikeuksien valvonnan.

5. **Tietoturvan sisällyttäminen kehitykseen:** Tietoturva huomioidaan kaikissa kehitysvaiheissa, suunnittelusta testaukseen ja käyttöönottoon. Se sisältää riskianalyysit ja tietoturvavaatimusten määrittämisen kehitysprojektien alussa.

6. **Turvallinen koodaus ja testaus:** Kehittäjien tulee noudattaa turvallisen koodauksen käytäntöjä haavoittuvuuksien vähentämiseksi. Lisäksi järjestelmät ja sovellukset tulee testata perusteellisesti tietoturvanäkökulmasta ennen käyttöönottoa.

7. **Muutosten hallinta:** Muutosten hallintaprosessit varmistavat, että kaikki järjestelmämuutokset ovat hallittuja ja dokumentoituja. Hallintaprosessi estää odottamattomat ongelmat ja tietoturvariskit, jotka voivat johtua hallitsemattomista muutoksista.

9.9.2 Esimerkki 1: Sataman lastinkäsittelyjärjestelmä

Operointi: Sataman lastinkäsittelyjärjestelmän operointi sisältää säännölliset varmuuskopiot, käyttöoikeuksien hallinnan ja jatkuvan seurannan epäilyttävän toiminnan havaitsemiseksi.

Järjestelmäkehitys: Uusia ominaisuuksia kehitetään tietoturvaa silmällä pitäen. Tämä sisältää riskianalyysit ennen uusien ominaisuuksien käyttöönottoa ja kattavat turvallisuustestaukset.

9.9.3 Esimerkki 2: Aluksen navigointijärjestelmä

Operointi: Aluksen navigointijärjestelmän operointi varmistaa, että järjestelmät toimivat luotettavasti ja turvallisesti kaikissa olosuhteissa. Tämä sisältää säännölliset päivitykset ja järjestelmätestaukset.

Järjestelmäkehitys: Navigointijärjestelmää kehitetään jatkuvasti tietoturvan parantamiseksi. Tämä sisältää turvallisen koodauksen käytännöt ja muutosten hallintaprosessit, jotka varmistavat, että kaikki muutokset on testattu ja hyväksytty ennen käyttöönottoa.

9.10 Toimittajien ja toimitusketjujen hallinta

Toimittajien ja toimitusketjujen hallinta meriklusteritoimijoiden toimintaympäristöissä tarkoittaa prosessia, jossa valvotaan ja hallitaan kaikkia ulkoisia toimittajia ja palveluntarjoajia, jotka vaikuttavat kriittisiin operatiivisiin järjestelmiin ja infrastruktuureihin. Toimitusketjujen hallinta on kriittinen osa ISO 27001 -standardin mukaista tietoturvallisuuden hallintajärjestelmää (ISMS). Se kattaa prosessit ja toimenpiteet, joilla organisaatio varmistaa, että sen toimittajat ja alihankkijat noudattavat asianmukaisia tietoturvavaatimuksia. Tämä on erityisen tärkeää nykypäivän monimutkaisissa ja globaaleissa

toimitusketjuissa, joissa kolmansien osapuolten tietoturvasta huolehtiminen on olennainen osa organisaation kokonaisvaltaista tietoturvaa.

- Varmista, että toimittajat noudattavat vaadittavia tietoturvakäytäntöjä ja että vaatimus on mainittu tietoturvapolitiikassa.
- Auditoi toimittajien tietoturvallisuutta säännöllisesti.
- Sisällystä sopimuksiin selkeät vaatimukset ja vastuut tietoturvallisuuteen liittyen.
- Määritä toimittajille säännöt tiedon käsittelyyn, säilytykseen ja suojaamiseen.
- Kouluta myös toimittajia organisaation tietoturvakäytäntöihin.
- Varmista, että toimittajan edustajat ymmärtävät tietoturvavelvoitteet.
- Luo tehokkaat viestintäkanavat tietoturvapoikkeamien ja -uhkien ilmoittamiseksi toimitusketjun toimijoiden välillä.
- Arvioi toimitusketjuun liittyviä riskejä yhdessä toimitusketjun toimijoiden kanssa.
- Laadi varautumissuunnitelma toimitusketjuun kohdistuvien häiriötilanteiden varalle.

Tavoite

Toimittajahallinnan tavoitteena meriklusteritoimijoiden tietoturvassa on varmistaa, että kaikki toimitusketjun osapuolet noudattavat korkeita tietoturvastandardeja ja käytäntöjä. Tämä vähentää riskejä, parantaa koko toimitusketjun tietoturvallisuutta ja varmistaa, että organisaation tiedot ja järjestelmät ovat suojattuja toimittajien kautta tulevilta uhkilta. Toimittajanhallinta myös auttaa organisaatiota täyttämään sääntelyvaatimukset ja parantaa sen kykyä reagoida ja palautua tietoturvaloukkauksista.

Tietoturvariskien vähentäminen:

Toimitusketjujen hallinnan avulla organisaatio voi tunnistaa ja hallita tietoturvariskejä, jotka liittyvät kolmansien osapuolten toimintaan. Tämä auttaa estämään tietovuodot ja muut tietoturvaloukkaukset, jotka voivat johtua toimittajien tai alihankkijoiden heikosta tietoturvasta.

Liiketoiminnan jatkuvuuden varmistaminen:

Varmistamalla, että kaikki toimitusketjun osapuolet noudattavat tietoturvavaatimuksia, organisaatio voi varmistaa liiketoiminnan jatkuvuuden ja vähentää häiriöitä, jotka voivat johtua toimittajien tietoturvaongelmista.

Lakisääteisten ja sääntelyvaatimusten täyttäminen:

Toimitusketjujen hallinta auttaa organisaatiota täyttämään tietoturvalainsäädännön ja -säädösten vaatimukset, kuten NIS2-direktiivin. Tämä on tärkeää oikeudellisten seuraamusten ja mainehaittojen välttämiseksi.

Keskeiset toimenpiteet toimitusketjujen hallinnassa

- Toimittajien arviointi ja valinta:
  - Ennen sopimuksen tekemistä arvioidaan toimittajien tietoturvakäytännöt ja -valmiudet.
  - Käytetään kyselylomakkeita, auditointeja ja riskianalyyseja arvioimaan toimittajien tietoturvakäytännöt.

- Sopimukset ja tietoturvavaatimukset:
  - Sisällytetään tietoturvavaatimukset ja -käytännöt osaksi toimittajasopimuksia.
  - Sopimuksissa määritellään selkeästi toimittajien velvollisuudet tietoturvan suhteen, mukaan lukien tiedon suojaaminen, tietoturvapoikkeamien raportointi ja auditointioikeudet.

- **Jatkuva valvonta ja auditointi:**
  - Seurataan ja auditoidaan toimittajien tietoturvakäytäntöjä säännöllisesti.
  - Suoritetaan säännöllisiä tarkastuksia ja vaaditaan toimittajia raportoimaan tietoturvapoikkeamista ja -päivityksistä.

Koulutus ja tietoisuuden lisääminen:

  - Koulutetaan toimittajia ja alihankkijoita tietoturvavaatimuksista ja -käytännöistä.
  - Järjestetään säännöllisiä koulutustilaisuuksia ja tietoisuuskampanjoita toimittajille.

9.10.1 NIS2-direktiivin vaikutus toimittajanhallintaan ja toimitusketjuihin

NIS2-direktiivi laajentaa ja tiukentaa vaatimuksia erityisesti kriittisten toimialojen osalta. Se velvoittaa organisaatioita varmistamaan, että myös heidän toimittajansa ja alihankkijansa noudattavat tiukkoja tietoturvavaatimuksia.

- NIS2-direktiivi edellyttää, että organisaatiot:
  - arvioivat ja hallitsevat toimitusketjun tietoturvariskejä
  - sisällyttävät tietoturvavaatimukset kaikkiin sopimuksiin
  - valvovat ja auditoivat säännöllisesti toimittajien tietoturvakäytäntöjä.

9.10.2 Esimerkki 1: Sataman tietojärjestelmätoimittaja

Tilanne: satama käyttää ulkopuolista toimittajaa tietojärjestelmänsä ylläpitoon.

Toimenpiteet: satama arvioi toimittajan tietoturvakäytännöt ennen sopimuksen tekemistä, sisällyttää tietoturvavaatimukset sopimukseen ja suorittaa säännöllisiä auditointeja varmistamaan vaatimusten noudattamisen. Näin varmistetaan, että tietojärjestelmä on suojattu ja toimintakykyinen, mikä estää tietoturvaloukkaukset ja toiminnan keskeytykset.

9.10.3 Esimerkki 2: Aluksen navigointijärjestelmän päivitykset

Tilanne: alus käyttää navigointijärjestelmänsä päivityksiin ulkopuolista ohjelmistotoimittajaa.

Toimenpiteet: alusoperaattori varmistaa, että toimittaja noudattaa tiukkoja tietoturvavaatimuksia, kuten tietojen salausta ja turvallista koodauskäytäntöä, ja valvoo päivitysprosessia säännöllisesti. Tämä vähentää riskiä, että navigointijärjestelmässä on haavoittuvuuksia, jotka voivat johtaa aluksen turvallisuusongelmiin tai tietomurtoihin.

Yhteenveto

Toimitusketjujen hallinta on ratkaisevan tärkeää ISO 27001 -standardin mukaisessa tietoturvallisuuden hallintajärjestelmässä. Se varmistaa, että toimittajat ja alihankkijat noudattavat asianmukaisia tietoturvavaatimuksia, mikä suojaa organisaation tietoja ja varmistaa liiketoiminnan jatkuvuuden. NIS2-direktiivi lisää näiden vaatimusten merkitystä ja velvoittaa organisaatiot varmistamaan tietoturvan koko toimitusketjussa.

9.11 Jatkuvuudenhallinta ja toipumissuunnittelu

Jatkuvuudenhallinnan tarkoituksena on minimoida häiriötilanteesta johtuvat toiminnan keskeytykset ja aiheutuvat haitat. Jatkuvuussuunnitelmilla varmistetaan siis toiminnan jatkuvuus ja sopeutumiskyky kriisitilanteessa. Ne varmistavat, että organisaatio pystyy jatkamaan toimintaansa ja palautumaan nopeasti tietoturvaloukkauksen tai muun vakavan häiriön jälkeen.

- Laadi kattavat varautumis-, jatkuvuus- ja palautussuunnitelmat toiminnoille, prosesseille ja järjestelmille, kuten laivojen ja satamien operatiivisille järjestelmille.
- Huomioi jatkuvuussuunnitelmassa järjestelmien ja toimintojen väliset riippuvuudet.
- Testaa ja harjoittele suunnitelmien toimivuutta säännöllisesti.
- Päivitä ja korjaa suunnitelmia jatkuvan parantamisen mallin mukaisesti.
- Laadi ja määritä varamenettelyt, joilla toiminta voi jatkua myös häiriötilanteessa.

Tavoite

Jatkuvuudenhallinnan tavoite meriklusteritoimijoiden OT-ympäristössä on varmistaa kriittisten operatiivisten toimintojen jatkuvuus ja turvallisuus, hallita riskejä ja parantaa organisaation resilienssiä. Tämä saavutetaan kehittämällä ja ylläpitämällä kattavia palautumissuunnitelmia, suojaamalla kriittisiä tietoja ja infrastruktuuria, sekä kouluttamalla henkilöstöä ja edistämällä yhteistyötä sidosryhmien kanssa. Tavoitteena on luoda

organisaatio, joka pystyy kestämään ja toipumaan nopeasti häiriöistä, mikä parantaa kokonaisvaltaista turvallisuutta ja liiketoiminnan jatkuvuutta

Liiketoiminnan jatkuvuuden varmistaminen:

Jatkuvuudenhallinta ja toipumissuunnittelu auttavat organisaatiota valmistautumaan ja reagoimaan tehokkaasti erilaisiin häiriöihin, kuten tietomurtoihin, luonnonkatastrofeihin tai teknisiin vikoihin. Tämä varmistaa, että organisaation toiminta voi jatkua mahdollisimman keskeytyksettä ja nopeasti palata normaaliksi.

Riskienhallinta:

Nämä prosessit auttavat tunnistamaan ja arvioimaan riskejä, jotka voivat uhata organisaation toimintaa. Tämä mahdollistaa paremman varautumisen ja vähentää riskiä, että vakavat häiriöt aiheuttavat merkittävää haittaa liiketoiminnalle.

Luotettavuuden ja asiakastyytyväisyyden parantaminen:

Hyvin suunniteltu jatkuvuudenhallinta ja toipumissuunnittelu parantavat organisaation luotettavuutta ja asiakastyytyväisyyttä. Asiakkaat ja sidosryhmät voivat luottaa siihen, että organisaatio pystyy toimimaan ja suojaamaan tietojaan tehokkaasti myös kriisitilanteissa.

Lakisääteisten ja sääntelyvaatimusten täyttäminen:

Monet sääntelyelimet ja lainsäädäntö edellyttävät, että organisaatioilla on toimivat jatkuvuudenhallinta- ja toipumissuunnitelmat. Näiden vaatimusten noudattaminen on välttämätöntä oikeudellisten seuraamusten ja mainehaittojen välttämiseksi.

Keskeiset elementit

- Riskienarviointi ja analyysi
  - o Tunnistetaan ja arvioidaan mahdolliset riskit, jotka voivat häiritä organisaation toimintaa.
  - o Käytetään riskianalyysimenetelmiä ja skenaarioanalyyseja tunnistamaan kriittiset toiminnot ja haavoittuvuudet.
- Jatkuvuussuunnitelma
  - o Dokumentoitu suunnitelma, joka kuvaa, miten organisaatio ylläpitää ja palauttaa kriittiset toiminnot häiriön aikana ja sen jälkeen.
  - o Suunnitelma sisältää toimintatavat, vastuuhenkilöt, resurssit ja aikataulut kriittisten toimintojen palauttamiseksi.

- Toipumis- ja palautussuunnitelma
  - Dokumentoitu suunnitelma, joka kuvaa, miten organisaatio toipuu häiriötilanteesta sekä palauttaa tietojärjestelmät ja tiedot normaalitilaan häiriön jälkeen.
  - Sisältää tiedon palauttamisen varmuuskopioista, järjestelmien uudelleenjärjestämisen ja haittaohjelmien poistamisen.

- Testaus ja harjoittelu
  - Säännöllinen testaus ja harjoittelu varmistavat, että jatkuvuus- ja toipumissuunnitelmat toimivat käytännössä.
  - Simuloidaan häiriötilanteita ja harjoitellaan suunnitelmien toteuttamista käytännössä.

- Jatkuva parantaminen:
  - Jatkuva arviointi ja parantaminen varmistavat, että suunnitelmat pysyvät ajan tasalla ja tehokkaina.
  - Kerätään palautetta testeistä ja harjoituksista, ja päivitetään suunnitelmia tarpeen mukaan.

9.11.1 Esimerkki 1: Sataman toiminnan keskeytyminen

Tilanne: satama joutuu tulvan kohteeksi, mikä keskeyttää lastinkäsittelyn ja tietojärjestelmien toiminnan.

- **Jatkuvuussuunnitelma:** sisältää varajärjestelyt lastinkäsittelylle, kuten väliaikaiset varastointipaikat ja yhteistyökumppaneiden käyttö.
- **Toipumissuunnitelma:** tietojärjestelmien palauttaminen varmuuskopioista ja kriittisten palveluiden uudelleenkäynnistys.

9.11.2 Esimerkki 2: Aluksen navigointijärjestelmän vikatilanne

Tilanne: aluksen navigointijärjestelmä pettää teknisen vian vuoksi keskellä merimatkaa.

- **Jatkuvuussuunnitelma:** sisältää varanavigointimenetelmät, kuten paperikartat ja manuaalisen navigoinnin.
- **Toipumissuunnitelma:** järjestelmän uudelleenkäynnistys, teknisen tuen hälyttäminen ja ohjelmiston uudelleenasennus.

Yhteenveto

Jatkuvuudenhallinta ja toipumissuunnittelu ovat keskeisiä ISO 27001 -standardissa, sillä ne varmistavat, että organisaatio pystyy jatkamaan toimintaansa ja palautumaan nopeasti häiriöiden jälkeen. Ne parantavat riskienhallintaa, luotettavuutta ja asiakastyytyväisyyttä sekä varmistavat lakisääteisten vaatimusten noudattamisen. Hyvin suunnitellut ja testatut jatkuvuus- ja toipumissuunnitelmat ovat olennaisia organisaation tietoturvan ja liiketoiminnan jatkuvuuden varmistamiseksi.

Lopuksi

10

Meriklusteritoimijoiden hallintamallit, mitkä sisältävät tietoturvan hallintajärjestelmän, ovat keskeisiä elementtejä, joilla varmistetaan, että organisaatioiden tietoturva on sekä strategisesti hallittua että käytännössä tehokkaasti toteutettua.

Hallintamalli meriklusteritoimijoiden osalta tarkoittaa sitä, miten organisaation johto asettaa strategiset suuntaviivat ja varmistaa, että kaikki toiminta, mukaan lukien tieto- ja kyberturvallisuus, tukevat organisaation liiketoimintatavoitteita. Hallintamalli määrittelee roolit, vastuut ja valtuudet tietoturvan hallinnassa sekä valvoo, että tietoturvakäytännöt ja -prosessit ovat linjassa organisaation yleisen strategian kanssa.

Tietoturvallisuuden hallintajärjestelmän avulla organisaatiot käytännössä hallitsevat tietoturvariskejä ja suojaavat tietoja systemaattisesti. Hallintajärjestelmällä varmistetaan, että organisaation tietoturvakäytännöt eivät ole pelkästään johdon asettamia periaatteita, vaan ne toteutuvat myös käytännössä. Tämä sisältää riskien arvioinnin, tietoturvakontrollien implementoinnin ja jatkuvan seurannan.

Yhdessä nämä kaksi komponenttia varmistavat, että tietoturva on integroitu osaksi organisaation strategiaa ja operatiivista toimintaa, mikä on erityisen tärkeää meriklusterin kaltaisilla toimialoilla, joissa liiketoiminnan jatkuvuus ja luotettavuus ovat kriittisiä. Hallintamalli (governance) tarjoaa siis strategisen ohjauksen ja hallintajärjestelmä vastaa päivittäisestä tietoturvan hallinnasta ja riskien vähentämisestä.

Näin ollen, meriklusteritoimijoiden tehokas tietoturvan hallinta vaatii molempien osa-alueiden yhteistyötä, jotta tietoturva pysyy hallinnassa sekä strategisella että operatiivisella tasolla.

Hallintajärjestelmän rakentaminen

ISO 27001 on kansainvälinen tietoturvastandardi, joka määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmän (ISMS) rakentamiseksi ja ylläpitämiseksi. Tämä standardi on erityisen tärkeä meriklusterissa, joka käsittää satamat, alukset, logistiikkayritykset ja muut meriliikenteeseen liittyvät toimijat.

Tietoturvallisuuden hallintajärjestelmä, esimerkiksi ISO 27001, auttaa suojaamaan kriittisiä tietoja, kuten navigointitietoja, lastinkäsittelytietoja ja kaupallisia sopimuksia. Varmistamalla, että vain valtuutetut henkilöt pääsevät käsiksi näihin tietoihin, standardi estää haitalliset kyberhyökkäykset, jotka voivat vaarantaa aluksen turvallisuuden. Standardin noudattaminen parantaa toiminnan luotettavuutta ja asiakastyytyväisyyttä sekä täyttää kansainväliset ja paikalliset tietoturvasäädökset, kuten NIS2-direktiivin vaatimukset. Tämä kokonaisvaltainen lähestymistapa tietoturvaan varmistaa, että koko toimitusketju on suojattu ja toimintakykyinen.

Jatkuvuudenhallinta ja toipumissuunnittelu varmistavat, että organisaatio pystyy jatkamaan toimintaansa häiriötilanteissa, kuten tietomurroissa tai luonnonkatastrofeissa. Esimerkiksi sataman lastinkäsittelyjärjestelmän varmuuskopiointi ja palautussuunnitelmat auttavat toiminnan jatkumisessa luonnonkatastrofin jälkeen.

ISO 27001 mahdollistaa tehokkaan tietoturvariskien tunnistamisen, arvioinnin ja hallinnan. Satama voi esimerkiksi arvioida toimittajien tietoturvakäytännöt ja sisällyttää tietoturvavaatimukset sopimuksiin varmistaakseen, että koko toimitusketju on turvallinen. Standardi auttaa täyttämään kansainväliset ja paikalliset tietoturvasäädökset, kuten NIS2-direktiivin vaatimukset. Tämä varmistaa, että meriklusterin toimijat, kuten logistiikkayritykset ja alihankkijat, noudattavat tiukkoja tietoturvavaatimuksia, mikä suojaa organisaation tietoja ja varmistaa liiketoiminnan jatkuvuuden.

Lähteet

Euroopan komissio. (2023). An enhanced EU Maritime Security Strategy for evolving maritime threats. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0008

Euroopan parlamentti. (2023). The NIS2 directive: A high common level of cybersecurity in the EU. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Huoltovarmuuskeskus. (2021). Merenkulun kyberturvallisuus – alusten parhaat käytännöt. https://www.huoltovarmuuskeskus.fi/files/a3512a9ae47541a92f002c60c6fa3030dc5327d3/kyberturvallisuus-parhaat-kaytannot-aluksille.pdf

Huoltovarmuuskeskus. (2021). Merenkulun kyberturvallisuus – varustamojen parhaat käytännöt. https://www.huoltovarmuuskeskus.fi/files/dd6e8c7f90cd8163a1e18df1aa109a6394ee608b/kyberturvallisuus-varustamojen-parhaat-kaytannot.pdf

Kansainvälinen merenkulkujärjestö (IMO). (2017). Kyberturvallisuuden hallinta merenkulun turvallisuuden hallintajärjestelmissä (Maritime cyber risk management in safety management systems). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Kansainvälinen merenkulkujärjestö (IMO). (2017). Kyberturvallisuuden suuntaviivat merenkulun turvallisuuden hallintajärjestelmille (Guidelines on maritime cyber risk management). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

Simola, J., Satopää, P., Paavola, J. & Vanharanta, J. (2024). The Impact of Operational Technology Requirements in Maritime Industries. 23rd European Conference on Cyber Warfare and Security. https://doi.org/10.34190/eccws.23.1.2357

Suomen Standardisoimisliitto. (2022). ISO/IEC 27001:2022:fi. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS ry. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27001-tietoturvallisuuden-hallintajarjestelmat

Suomen Standardisoimisliitto. (2022). ISO/IEC 27002:2022:fi. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS ry. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27002-tietoturvallisuuden-hallintakeinot