MARITIM CYBERSÄKERHET – BÄSTA PRAXIS FÖR REDERIER

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

www.huoltovarmuuskeskus.fi

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

Med försörjningsberedskap avses förmågan att upprätthålla sådana ekonomiska grundfunktioner i samhället som är nödvändiga för att trygga befolkningens levnadsmöjligheter, samhällets funktion och säkerhet samt de materiella förutsättningarna för landets försvar vid allvarliga störningar och undantagsförhållanden.

Försörjningsberedskapscentralen (FBC) hör till Arbets- och näringsministeriets förvaltningsområde. Dess uppgifter består av planering och operativ verksamhet i anslutning till upprätthållandet och utvecklandet av landets försörjningsberedskap. I anslutning till Försörjningsberedskapscentralen finns Försörjningsberedskapsrådet samt sektorer och pooler som är permanenta samarbetsorgan och fungerar på samma sätt som kommittéer. Sammantagna bildar de försörjningsberedskapsorganisationen.

På uppdrag av Försörjningsberedskaporganisationen, Sjötransportpool och Rederierna I Finland

Författare: Deductive Labs Ab

Utgivare: Försörjningsberedskaporganisationen, Sjötransportpool

Bilder: Shutterstock

Layout: Up-to-Point Oy

Publikationsår: 2021

ISBN: 978-952-7470-05-3

Innehåll

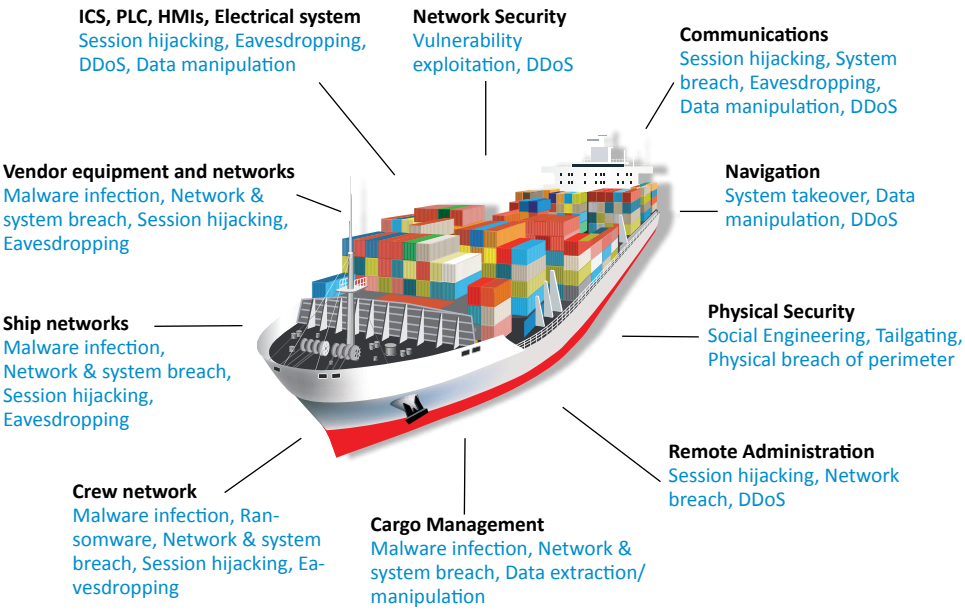
De olika stegen och bästa praxis för cybersäkerhet på rederier presenteras i detta dokument på följande sätt:

BAKGRUND OCH INTRODUKTION

Sjöfart och fartyg kan verka som ovanliga mål för cyberattacker, men med den ökande digitaliseringen av den marina miljön och den ökade användningen av uppkopplade Informationssystem (IT), Operativa system (OT-system), industriella styrsystem (ICS) och satellitkommunikation, är de marina miljöerna mottagliga för attacker från cyberbrottslingar och andra hotgrupper. Det är därför viktigt att cybersäkerhet hanteras effektivt inom sjöfarten för att skydda organisationen, fartygen, besättning och last mot potentiella cybersäkerhetshot och attacker.

Maritim cybersäkerhet är urvalet av policyer, riktlinjer, förfaranden, säkerhetskontroller och åtgärder, riskhanteringsåtgärder, best practice, utbildning, verktyg och teknik som används för att skydda rederier, deras miljöer och fartyg.

Risker med IT- och OT-system skiljer sig åt genom att IT-system främst påverkar finansiering och rykte medan OT-system kan påverka och hota liv, egendom och miljön om sådana risker förverkligas.



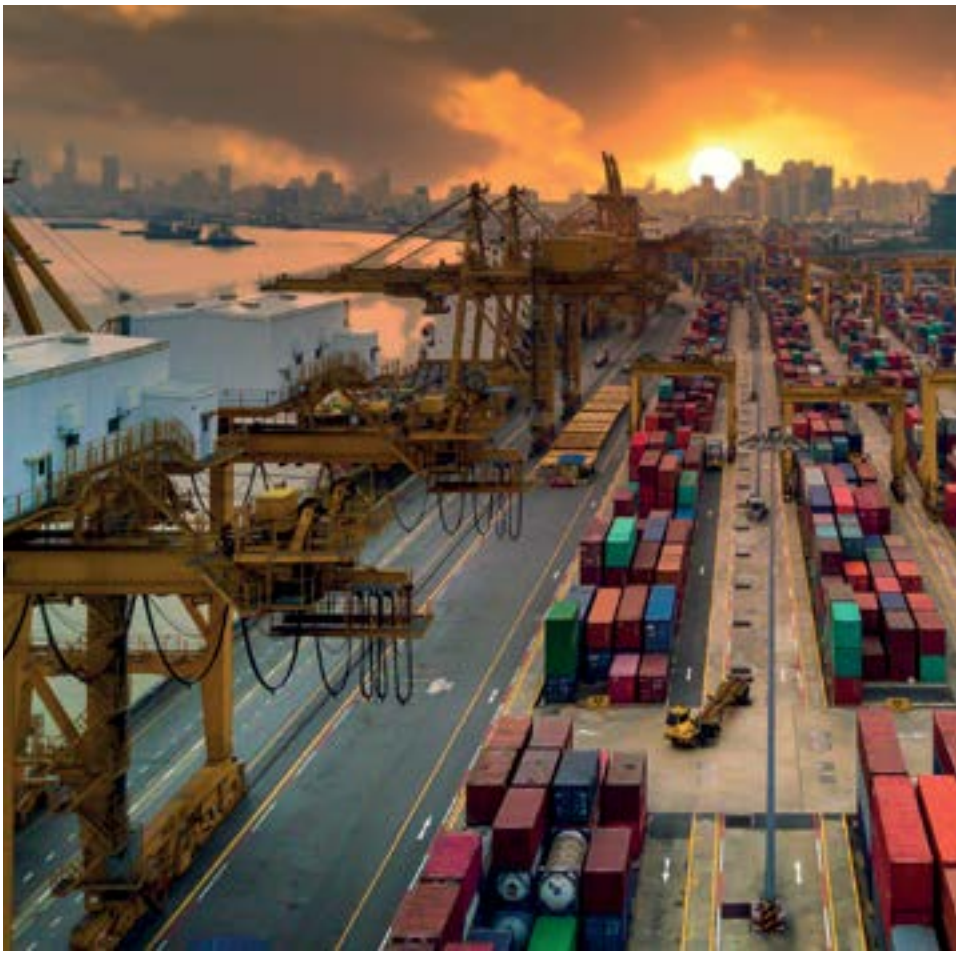
I januari 2021 inledde den Finska Redarföreningen tillsammans med Försörjningsberedskapscentralen i Finland ett project för att kartlägga cybersäkerhetssituationen inom den finska sjöfartsnäringen. Deductive Labs Ab, ett finskt bolag cybersäkerhetsspecialist inom sjöfart, engagerades för att genomföra projektet.

Projektet resulterade i tre separata dokument, alla tillgängliga via Rederierna i Finland tillsammans med Försörjningsberedskapscentralen i Finland: *https://www.huoltovarmuuskeskus.fi/julkaisut* och *https://shipowners.fi/vastuullisuus/turvallisuus/kyberturvallisuus/*

1. ***Maritime Cybersecurity Report – Finnish Maritime Fleet Maturity (ENG),***
   en omfattande rapport om den aktuella situationen i den finska sjöfartssektorn

2. ***Maritime Cybersecurity – Maritim cybersäkerhet – Bästa praxis för fartyg,***
   en sammanfattning av resultaten och presentation av bästa praxis för fartyg.

3. ***Maritime Cybersecurity – Maritim cybersäkerhet – Bästa praxis för rederier,***
   en sammanfattning av resultat och presentation av bästa praxis för för rederier



1. LEDNINGENS STÖD

Företagets ledning och engagemang är avgörande för att lyckas med cybersäkerhet i din organisation. De här rekommenderade åtgärderna hjälper med att få ledningens förståelse och stöd för cybersäkerhet.

Åtgärder:

1. Engagera cybersäkerhet med företagets ledning samt inkludera cybersäkerhet på dess agenda
2. Inkludera cybersäkerhet i beslutsprocessen
3. Använd riskhantering som ett vardagligt verktyg för beslutsfattande
4. Utbilda företagets ledning i cybersäkerhet

Mål:

- Ökad förståelse för cybersäkerhet och risker för organisationen
- Beslut fattas baserat på information från riskbedömningar
- Företagets ledning är förebild och visar att cybersäkerhet är en prioritet

Tips:

för styrelsen och ledningen som kan användas för att öka förståelsen för cybersäkerhet:

- *https://www.kyberturvallisuuskeskus.fi/sv/publikationer/cybersakerhet-och-styrelsens-ansvar*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_SWEdigi_auk280120.pdf*

2. CYBERSÄKERHETSUTBILDNING

Utbildning och cybersäkerhetsmedvetenhet är avgörande för hela organisationen, från ledning till anställda och besättning.

Åtgärder:

1. Organisera cybersäkerhetsutbildning för alla anställda
2. Genomföra cybersäkerhetsutbildning regelbundet
3. Upprätta cybersäkerhetsutbildning som en kontinuerlig del av företagets process och kultur

Mål:

- Ökad förståelse för cybersäkerhet för alla anställda
- Enhetlig med IMO: s riktlinjer för cyberriskhantering[1]
- Ökad förståelse för cybersäkerhet i organisationen

Tips:

Om din organisation har dedikerade cybersäkerhetsresurser kan de användas för att skapa utbildningsmaterial för din organisation. Säkerhetsutbildningen kan också outsourcas vid behov. Utbildning i cybersäkerhet bör ges till alla anställda, även ledningen. Olika roller behöver olika tillvägagångssätt, så överväg att tillhandahålla utbildning som är anpassad för de specifika rollerna och deras specifika cybersäkerhetsutmaningar och behov.

Externa parter kan användas för att att genomföra utbildningar

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

3. CYBERSÄKERHETSPROCEDURER OCH INSTRUKTIONER

Organisationens anställda och fartygspersonal måste ha tydliga och koncisa procedurer som definierar hur cybersäkerhet hanteras i organisationen och på fartygen.

Åtgärder:

Skapa praktiska procedurer, riktlinjer och instruktioner för besättningen:

1. Procedurer för användning av system och tjänster
2. Procedurer för hur man hanterar externa media
3. Procedurer för hur man hanterar och uppdaterar system
4. Procedurer för hur man använder personliga enheter, nätverk och Internet
5. Procedurer för fjärråtkomst för leverantörer
6. Procedurer för hantering av cybersäkerhetshändelser
7. Procedurer för cybersäkerhetsövningar

Mål:

- Organisationens medarbetare och fartygens besättning har dokumenterade rutiner för hur cybersäkerhet hanteras i organisationen och på fartygen.
- Organisationens och fartygens procedurer stöder kraven från ISM / ISPS

Tips:

Samarbeta med medarbetare, besättning, leverantörer och andra tredje parter att förstå deras dagliga verksamhet och hur deras verksamhet påverkar organisationens och fartygens cybersäkerhet. Inkludera parterna i utvecklingen av praktiska procedurer som är lätta att förstå och följa. Utveckling av rederiets cybersäkerhetskultur är på ledningens ansvar.

4. ORGANISATIONENS KRITISKA TJÄNSTER OCH FUNKTIONER

Att identifiera de kritiska tjänsterna och funktionerna som används i organisationen och på dess fartyg är avgörande för att förstå och upprätthålla cybersäkerhet. Organisationen böt identifiera alla kritiska tjänster och funktioner och relaterade IT- och OT-tillgångar för att identifiera riskerna och potentiella effekter på leveransen av tjänsterna i händelse av en cybersäkerhetsincident. Detta inkluderar alla tjänster och funktioner som används i organisationen, både på land och på fartygen.

Åtgärder:

1. Identifiera och dokumentera alla kritiska tjänster och funktioner i organisationen
2. Identifiera och dokumentera alla IT- och OT-tillgångar relaterade till leveransen av kritiska tjänster och funktioner.
3. Börja med grundläggande verktyg som kalkylark och dokument och överväg automatiserade verktyg för att göra processen effektivare

Mål:

- Organisationens kritiska tjänster och funktioner är inventerade
- Organisationens IT- och OT-tillgångar är inventerade. Detta inkluderar både organisationssystem och fartygssystem
- Inventeringen kan användas i riskhanteringsprocessen

Tips:

Tillgångshantering och skapande av tillgångsregister kan vara utmanande arbete. Vi rekommenderar att börja med DCSAs ***"Asset Management and Risk Register Templates Reading Guide"*** som innehåller användbara mallar för skapandet av tillgångsregister och riskhantering. Börja med att identifiera och dokumentera kritiska system och funktioner och deras relaterade tillgångar med potentiell stor inverkan på organisationen eller fartygets verksamhet och säkerhet.

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

5. CYBERSÄKERHETSRISKER FÖR IDENTIFIERADE TJÄNSTER OCH FUNKTIONER OCH DERAS RELATERADE TILLGÅNGAR

När organisationens kritiska tjänster och deras relaterade IT- och OT-tillgångar har identifierats och dokumenterats bör en riskbedömning göras för att identifiera hot, risker och sårbarheter relaterade till tillgångarna som kan påverka organisationens och fartygens verksamhet och säkerhet.

Åtgärder:

1. Bedöm cybersäkerhetsrisker för de identifierade tillgångarna
2. Identifiera åtgärder som behövs för att avhjälpa de identifierade riskerna
3. Skapa en handlingsplan utifrån de åtgärder som identifierats i riskbedömningen
4. Referera till hanteringen av cyberrisker i säkerhetsledningssystemet (SMS)

Mål:

- Organisationens cybersäkerhetsrisker relaterade till kritiska tjänster och funktioner identifieras och dokumenteras
- En handlingsplan för att hantera identifierade risker dokumenteras
- Organisationens cybersäkerhetsrisker hanteras i enlighet med IMO:s krav

Tips:

Det finns många olika modeller och kalkylblad allmänt tillgängliga som kan användas för att komma igång med grundläggande riskhantering. Vi rekommenderar att du börjar med DCSA: s ***"Asset Management and Risk Register Templates Reading Guide"*** [2] som innehåller användbara mallar för tillgångshantering och riskhantering. När riskhanteringsprocessen mognar kan andra verktyg användas.

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

6. RISKHANTERINGSPLAN

När samtliga kritiska tjänster, funktioner och tillhörande tillgångar och deras risker har identifierats är nästa steg att skapa en riskhanteringsplan med åtgärder för att hantera de identifierade riskerna. Detta steg är baserat på riskbedömningarna och beskriver både procedurmässiga och tekniska kontroller som behöver implementeras för att minimera och åtgärda riskerna.

Åtgärder:

1. Skapa en projektplan för åtgärderna i riskhanteringsplanen
2. Se till att projektplanen identifierar de steg och åtgärder som behövs för att åtgärda risken, vilka resurser som behövs, vem som är ansvarig, vad tidsplanen är och att det finns en godkänd budget
3. Genomför projektplanen

Mål:

- Handlingsplanen har dokumenterats och genomförts
- De identifierade riskerna har åtgärdats

Tips:

Behandla åtgärderna som projekt med dokumenterade planer och uppgifter som kan följas upp. Du behöver inte uppfinna hjulet, använda organisationens etablerade projektledningsmetoder och verktyg för att få jobbet gjort.

Externa resurser kan användas för att effektivisera riskhanteringsarbetet.

7. CYBERSÄKERHETSARKITEKTUR

En dokumenterad cybersäkerhetsarkitektur för organisationen och fartygen behövs för att beskriva hur cybersäkerhet implementeras i organisationen och på fartygen. En cybersäkerhetsarkitektur hjälper till att säkerställa att cybersäkerhetskontroller dokumenteras och implementeras på ett standardiserat sätt i organisationen och på fartygen.

Åtgärder:

1. Skapa en cybersäkerhetsarkitektur som beskriver hur cybersäkerhet implementeras i organisationen och på fartygen
2. Skapa specifika cybersäkerhetsplaner (CSP) för varje fartyg baserat på cybersäkerhetsarkitekturen och den faktiska tekniska miljön och behoven hos varje fartyg
3. Anpassa cybersäkerhetsplanen med dokumenterade cybersäkerhetsförfaranden

Mål:

- En cybersäkerhetsarkitektur har dokumenterats som beskriver hur cybersäkerhet implementeras i organisationen och fartygen
- Cybersäkerhetsarkitekturen används för att skapa cybersäkerhetsplaner för fartygen

Tips:

Fartygets cybersäkerhetsplan kan ingå i befintliga fartygssäkerhetsplaner (SSP) men vi rekommenderar att man skapar en separat cybersäkerhetsplan (CSP) för att hålla dokumenten åtskilda, eftersom SSP traditionellt fokuserar mer på fartygens fysiska säkerhet. Att lägga till cybersäkerhet i SSP kan göra det mer komplext och svårare att förstå och följa. Planen för cybersäkerhet bör anpassas till de dokumenterade cybersäkerhetsförfaranden som har utvecklats.

8. CYBERSÄKERHET I LEVERANTÖRSKEDJAN

Den marina sektorn är mycket beroende av olika externa leverantörer och tredje part och de har en viktig roll i förvaltningen och driften av fartygen. Leverantörerna har vanligtvis ett ansvar för att hantera och övervaka kritiska system ombord på fartygen, såsom ECDIS-system, motorer och krafthantering, lasthanteringssystem, GPS-system, PLC: er, sensorer etc.

Åtgärder:

1. Identifiera alla leverantörer
2. Bedöm leverantörnas cybersäkerhetrisker
3. Skapa cybersäkerhetskrav för leverantörer
4. Inkludera cybersäkerhetskrav i avtal med leverantören
5. Säkerställ att rätten till revision av cybersäkerhet ingår i leverantörsavtalen

Mål:

- Leverantörer har identifieras
- Krav på cybersäkerhet för leverantörer har dokumenteras
- Cybersäkerhet i leveranskedjan hanteras

Tips:

Börja med att identifiera och dokumentera alla leverantörer som tillhandahåller system och tjänster till fartygen. Utveckla cybersäkerhetskrav för leverantörerna baserat på de riskbedömningar som har gjorts.

God och användbar vägledning om säkerhet i försörjningskedjan finns i den brittiska NCSC Supply chain-säkerhetsguiden[3].

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

9. INCIDENTHANTERING, RESPONS OCH ÅTERHÄMTNING

Effektiv incidenthantering gör det möjligt för organisationer att identifiera cybersäkerhetsincidenter och att snabbt svara och återhämta sig från incidenten så att påverkan av incidenten inte påverkar fartygets säkerhet.

Åtgärder:

1. Skapa ett hanteringsförfarande för cybersäkerhetsincidenter. Förfarandet ska beskriva vilka åtgärder anställda och besättningen ska göra i händelse av en cybersäkerhetsincident samt hur kritiska systems loggar analyseras och övervakas.
2. Se till att miljön övervakas och händelserna loggas för att underlätta upptäckten av incidenter
3. Organisera cyberövningar för att utbilda de anställda och besättningen i hur man reagerar vid en cybersäkerhetsincident.

Mål:

- Organisationen upptäcker, reagerar på och återhämtar sig från cybersäkerhetsincidenter
- Cybersäkerhetsövningar görs regelbundet

Tips:

Börja med att skapa procedurer för incidenthantering som beskriver vad anställda och fartygens besättning ska göra i händelse av en cybersäkerhetsincident i organisationen eller på fartygen. Procedurerna bör inkludera hur cyberskerhetsincidenter upptäcks, hur respons aktiviteter organiseras och vad som behöver göras för återhämtning från incidenten.

Använd Cybersäkerhetscentrets anvisningar för att komma igång med planering av cybersäkerhetsövningar:

- *https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar*
- *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Anvisning%20om%20cyber%C3%B6vningar.pdf*

Cybersäkerhetsövningar är ett bra och effektivt sätt att utbilda och träna anställda och besättningen i hur man reagerar på cybersäkerhetsincidenter.

10. CYBERSÄKERHETSSTANDARDER OCH RAMVERK

ISO 27001 är en etablerad standard för att skapa ett informationssäkerhetshanteringssystem (ISMS), men standarden är inte helt anpassad till sjöfartens krav och miljö. Standarder som NIST Cybersecurity Frameworks (NIST CSF) och ISA / IEC 62443 Security for Industrial Automation and Control Systems är bättre anpassade och används för cybersäkerhet i en maritim miljö.

Åtgärder:

1. Välj en cybersäkerhetsstandard eller ramverk för din organisation
2. Använd riskanalyser för att identifiera nödvändiga åtgärder och kontroller
3. Dokumentera cybersäkerhetspolicyer, processer och procedurer baserat på det valda ramverket

Mål:

- Organisationen använder en etablerad standard eller ram för cybersäkerhet

Tips:

Det finns många olika standarder och ramar tillgängliga som kan användas för att vägleda din ansträngningar för cybersäkerhet, den mest använda är ISO 27001, ISA / IEC 62443 och NIST Cybersecurity framework.

Vi rekommenderar att organisationen investerar lite tid och ansträngningar, eller kontaktar externa resurser och specialister för att få insikt i de olika standarderna och ramarna och för att avgöra vilken som passar bäst för din specifika miljö och dina behov.

Genom att använda etablerade standarder blir cybersäkerhetsaktiviteter mer standardiserade och enklare att implementera, underhålla och granska.

11. SAMARBETE MED EXTERNA PARTER

En slutlig rekommendation, om det bedöms nödvändigt, är att använda extern hjälp från branschorganisationer, rederier, föreningar eller erfarna partners inom cybersäkerhet som kan hjälpa till att implementera cybersäkerhet i din miljö.

Exempel på externa organisationer är:

- Branschkolleger
- Maritima organisationer och föreningar
- Klassificeringssällskap
- Maritima försäkringsbolag
- Nationella cybersäkerhetsmyndigheter
- Cybersäkerhetskonsulter

Cybersäkerhet är en komplex strävan som kräver specialkunskaper som är svåra att hitta. Dina IT- och OT-team arbetar troligtvis redan hårt med sina vanliga uppgifter och projekt, och det kan vara lättare och billigare att få hjälp från externa resurser med tidigare kunskap om maritim cybersäkerhet istället för att anställa cybersäkerhetsexperter till din organisation.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI