MARITIM CYBERSÄKERHET – BÄSTA PRAXIS FÖR FARTYG

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

www.huoltovarmuus.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: 978-952-7470-00-8

Innehåll

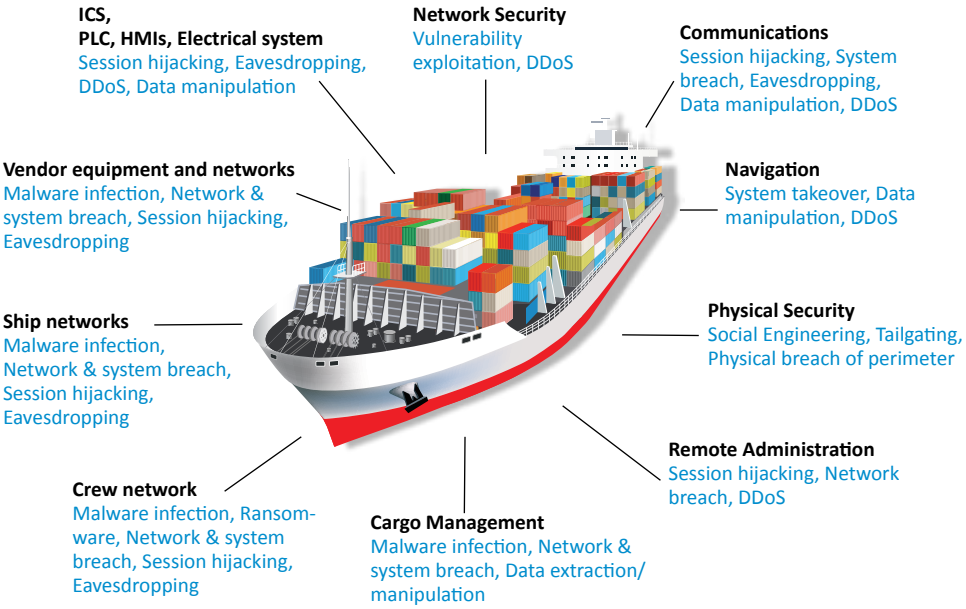
De olika stegen och bästa praxis för cybersäkerhet ombord på fartyg presenteras i detta dokument på följande sätt:

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 projekt för att kartlägga cybersäkerhetssituationen inom den finska sjöfartsnäringen. Deductive Labs Ab, en finsk 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 – Best practices for vessels – Best practice fartyg,*** en sammanfattning av resultaten och presentation av best practice för aktiviteter ombord

3. ***Bästa praxis cybersäkerhet för rederier,*** en sammanfattning av resultat och presentation av best practice för rederier

1. FARTYGENS KRITISKA TJÄNSTERS OCH FUNKTIONERS RISKER

- Identifiera alla kritiska tjänster och funktioner på fartygen (navigering, framdrivning, stabilitet, ballast, etc.)
- Identifiera alla IT- och OT-system (datorer, nätverk, styr- och automatiseringssystem, bryggsystem, navigering, framdrivning och maskiner osv.) som tillhandahåller dessa kritiska tjänster
- Identifiera risker och deras effekter för alla identifierade kritiska tjänster, funktioner och system
- Skapa en riskhanteringsplan med åtgärder för att åtgärda eller minimera identifierade risker
- Uppdatera listan över system och risker alltid då ändringar görs.

Tips:

Använd etablerade riskhanteringsrutiner från befintliga ISM / ISPS-procedurer om sådana är tillgängliga eller använda till exempel "DCSA Asset Management and Risk Assessment" Mallar:

- DCSA Asset List Risk Assessment Framework examples
- DCSA Asset Management and Risk Register Templates Reading Guide

Mål:

- Det finns en kartläggning samt riskanalys av fartygens kritiska tjänster, funktioner och tillhörande IT- och OT-system
- Fartygens hantering av cyberrisker överensstämmer med kraven i IMO MSC.428(98)
- Riskhanteringsplanen beskriver åtgärder hantera identifierade risker och säkra fartygen

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT- och cybersäkerhetsansvariga

Att tänka på:

- ❑ *fartygets nätverk och datorer*
- ❑ *bryggsystem*
- ❑ *godshantering och ledningssystem*
- ❑ *framdrivnings- och maskiner, styrsystem*
- ❑ *passersystem*
- ❑ *passagerarservice- och hanteringssystem*
- ❑ *passagerare som använder publika nätverk*
- ❑ *administrativa system och besättningens system*
- ❑ *kommunikationssystem*

2. NÄTVERKSSEGMENTERING

De kritiska systemen som används på fartygen bör segmenteras i olika nätverk för att skydda dem och begränsa eventuella intrång och attacker. Nätverkssegmentering är en standardregel som används i kritiska nätverk och en av de viktigaste kontrollerna i standarder som ISO27001 och ISA / IEC62443.

1. Identifiera alla kritiska system och bedöma den aktuella nätverksdesignen och segmenteringen
2. Skapa nätverk för olika grupper av kritiska system som kommunikation, brygga, motor, last, affärs-, besättnings- och wi-fi-nätverk.
3. Flytta systemen till de segmenterade nätverken och uppdatera brandväggspolicyerna i enlighet med detta (Steg 3)

Tips:

Använd standarder som ISO27000 eller ISA / IEC 62443 för mer information om segmentering och användning av säkerhetszoner / ledningar för att öka cybersäkerheten för kritiska tillgångar. Skapa nätverksdiagram för fartygen för att ha en lättillgänglig visualisering av samtliga nätverk och system. Börja med att segmentera de ”enklaste” nätverken som besättning, gästnätverk innan du fortsätter att segmentera kritiska operationella system. Kombinera liknande system till samma nätverk baserat på kritiskhet och funktionalitet, men se till att undvika över-segmentering som kommer att vara kontraproduktivt för uppgiften.

Mål:

- Kritiska IT- och OT-system (brygga, maskin, etc.) är segmenterade till separata nätverk

Ansvarig:

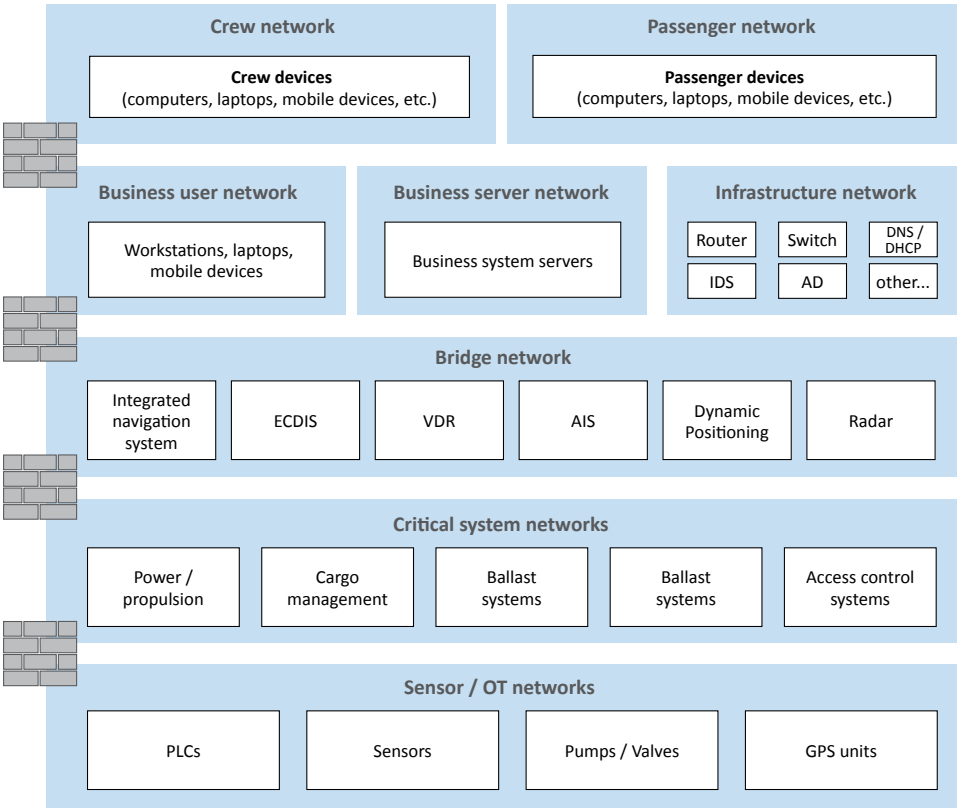
- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT-, nätverks och cybersäkerhetsansvariga

Att tänka på:

nätverkssegmentering för fartygs nätverk

- ❑ *affärsnätverken*
- ❑ *besättningens nätverk*
- ❑ *Wifi-nätverk*
- ❑ *passagerarnätverk*
- ❑ *Maskin-, och andra driftsnätverk*
- ❑ *leverantörsnätverk*
- ❑ *andra nätverk som kan behövas efter riskanalys*

Exempeldiagram på segmentering av fartygsnätverk:



3. BRANDVÄGGSKONFIGURATIONER

När system har segmenterats är det viktigt att lämpliga brandväggskonfigurationer tillämpas på nätverk och system för att endast tillåta godkänd och nödvändig trafik till och från systemen.

1. Se till att alla system och nätverk är korrekt skyddade. Tillåt endast nödvändig åtkomst och undvik att tillåta åtkomst från offentliga, ej godkända källor. Var särskilt uppmärksam på fartygskommunikationssystem (VSAT, Fleet bredband, etc.) och skydda dem ordentligt genom att filtrera kommunikation, segmentera system och tillämpa säkra konfigurationer (se steg 8 – systemhärdning)
2. Identifiera IP-adresser, nätverkskommunikationsprotokoll och dataflöden som behövs för att de systemen ska fungera korrekt.
3. Analysera brandväggspolicyer och se till att endast nödvändig kommunikation är tillåten till och från systemen
4. Konfigurera brandväggar med en standard-block konfiguration som blockerar och loggar all icke-godkänd nätverkskommunikation (default-deny policy)

Tips:

Använd identifierade system- och tillgångsgrupper och nätverks- och dataflödesdiagram skapade under nätverkssegmenteringen (steg 2) samt säkerställ att rätt brandväggspolicies skapas för systemen och nätverken baserat på systemkommunikationskraven.

Mål:

- Brandväggar är korrekt konfigurerade och tillämpade för att endast tillåta nödvändig trafik till och från kritiska segmenterade system

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT-, nätverks och cybersäkerhetsansvariga

Att tänka på:

- ❑ *fartygets brandväggar*
- ❑ *Segmenterade nätverk och tillgångar*

4. FJÄRRÅTKOMST TILL KRITISKA SYSTEM OCH NÄTVERK

De flesta fartyg är beroende av flera tredjepart och leverantörer för kritiska system och tillgångar. Det är viktigt att kontrollera fjärr- och lokal tillgång till kritiska system för både tredje part och interna användare.

1. Identifiera tredjeparts- och interna användare som har krav på att få tillgång till fartygssystem och tillgångar
2. Identifiera och dokumentera vilka IP-adresser, nätverksportar / tjänster och tillgångar som de behöver åtkomst för att
3. uppdatera brandväggspolicyer för att tillåta åtkomst för tredje part och användare de system och tillgångar och tjänster de behöver tillgång till
4. Dokumentera alla fjärråtkomstanslutningar och se till att lämpliga fjärråtkomstavtal finns på plats.
5. Kontrollera leverantörens lokala tillgång till kritiska system och nätverk. Se till att leverantörer inte ansluter osäkra enheter till fartygsnätverk och övervakar användningen vid behov.

Tips:

Använd tredjeparts- och leverantörsdokumentation för att identifiera systemåtkomstkrav som kan användas i brandväggspolicyerna. Skapa sekretessavtal samt avtal om fjärråtkomst som beskriver företagets krav på åtkomst till fartygsnätverk (personliga användare, starka lösenord / MFA, skydd mot skadlig kod på datorer etc.).

Mål:

- Fjärråtkomst till kritiska system och nätverk kommer att kontrolleras
- Avtal för fjärråtkomst har upprättats med tredje part och leverantörer

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT-, nätverks och cybersäkerhetsansvariga
- Externa leverantörer och tredje parter

Att tänka på:

- ❑ *Lista över tredjepart och leverantörer*
- ❑ *Kritiska system som hanteras av tredjepart eller leverantören*
- ❑ *anvisningar för leverantör*

5. SKYDD MOT SKADLIG KOD

Att implementera ett skydd mot skadlig kod är en grundläggande del i cybersäkerhet. Även EDR-lösningar (end-point-protection-and-response) rekommenderas eftersom de både skyddar systemen och ger avancerad övervaknings- och svarsfunktion i händelse av infektion med skadlig kod.

1. Installera och konfigurera verktyg för skydd mot skadlig programvara på alla kritiska system där det är möjligt (Windows, Linux, MacOS)
2. Se till att verktyg för skydd mot skadlig programvara uppdateras regelbundet och automatiskt
3. Identifiera system där skadlig kod inte kan installeras och skapa kontroller för dessa system (nätverkssegmentering, strikt åtkomst kontroller, etc). ECDIS-system är till exempel typgodkända och ad hoc-installationer är inte tillåtna och olika skyddsåtgärder behövs
4. Se till att alla externa USB och liknande enheter kontrolleras för skadlig programvara innan de används på kritiska system

Tips:

Se till att alla system har skydd implementerat för att skydda mot skadlig programvara. Detta inkluderar skydd för e-post, webbplatser och USB-enheter som nås och används på fartyget.

Mål:

- Skydd mot skadlig kod implementeras på alla fartygssystem och tillgångar där det är möjligt
- System som inte kan implementeras med skydd mot skadlig kod har identifierats och alternativa kontroller har identifierats och implementerats för att skydda dessa system mot skadlig programvara

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT-, nätverks och cybersäkerhetsansvariga

Att tänka på:

- ❑ *Se till att system för skydd mot skadlig programvara uppdateras regelbundet*
- ❑ *Se till att aktiviteter och händelser i malware system loggas och analyseras*

6. LOGGHANTERING OCH ÖVERVAKNING

Övervakning (monitorering) och loggning av tjänster och system är nödvändigt för att ha förmågan att övervaka och upptäcka cyberattacker. Utan övervaknings- och loggningsfunktioner är det mycket svårt att upptäcka attacker och reagera på dem.

1. Installera övervaknings- och logglösningar för fartygens IT- och OT-system
2. Konfigurera alla IT- och OT-system för att övervaka och logga till en central logglösning
3. Konfigurera loggning för brandväggar och andra nätverksenheter
4. Analysera loggarna kontinuerligt för att upptäcka attacker

Tips:

Det finns många logglösningar tillgängliga på marknaden som kan användas. Logg- och analystjänster kan även anlitas via en pålitlig partner som har kunskapen och förmågan att leverera en loggtjänst.

Mål:

- Fartygens kritiska system övervakas och loggar skickas till en central lösning för analys

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT, nätverks och cybersäkerhetsansvariga

Att tänka på:

- ❑ *Alla IT- system på fartygen*
- ❑ *OT-system som har förmågan att skapa loggar*

7. REGELBUNDEN UPPDATERING AV SYSTEM

Den vanligaste metoden för angripare är att utnyttja sårbarheter i system och applikationer är att få tillgång till dem.Därför är det viktigt att regelbundet uppdatera system och applikationer för att säkra systemen så att sårbarheterna inte kan utnyttjas av potentiella angripare.

1. Övervaka publicerade sårbarheter från leverantörer för alla system och applikationer
2. Uppdatera kritiska system och applikationer regelbundet för att åtgärda sårbarheter.
3. Var särskilt uppmärksam på system och applikationer som exponeras för opålitliga nätverk eller Internet och se till att dessa system regelbundet lappas
4. Dokumentera rutiner för patchning och ansvar samt se till att systemen uppdateras på ett kontrollerat sätt när och där det är möjligt (i docka, i hamn, till havs osv.)

Det rekommenderas att patcha åtminstone varje månad för regelbundna uppdateringar men se till att IT-team har möjlighet att installera kritiska uppdateringar snabbt vid behov

Tips:

Patching av system och applikationer kan vara svårt och tidskrävande, särskilt om arbetet måste göras manuellt. Använd automatiseringsverktyg och skript för att hjälpa till med lapp-system på ett centraliserat och automatiserat sätt. Automation minskar de mänskliga resurser som behövs och säkerställer en standardiserad metod för att distribuera korrigeringsfiler.

Mål:

- System och applikationer som används på fartygen är uppdaterade

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT, nätverks och cybersäkerhetsansvariga
- Externa leverantörer och tredje parter

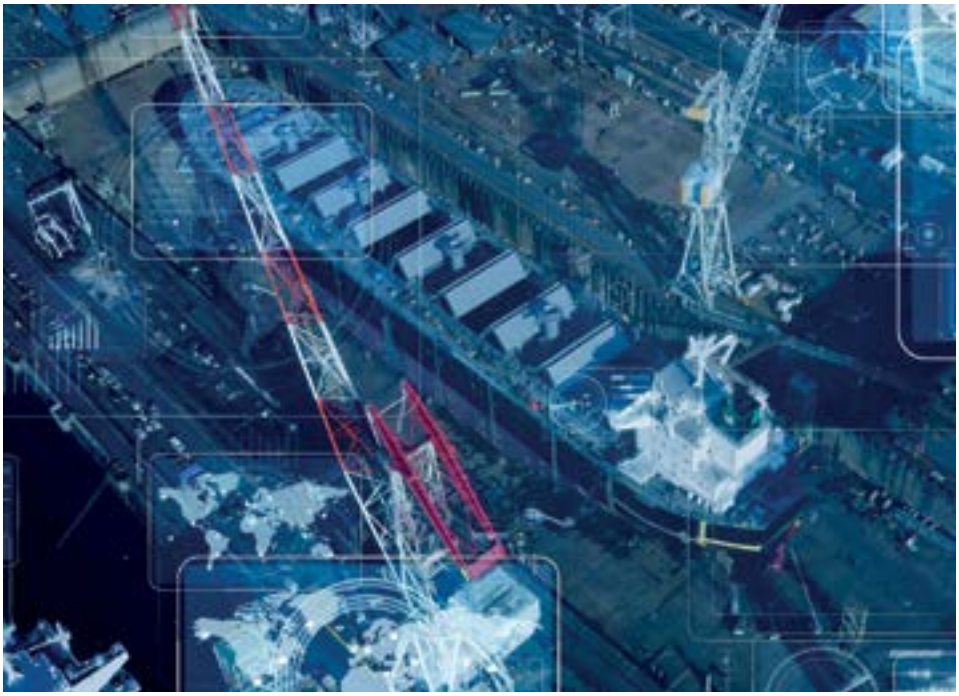
Att tänka på:

- ❑ *Patchningsrutiner beroende på system*
- ❑ *Kommunikation om patchningsrutiner med personer som är ansvariga för systemet (intern, leverantör)*

8. HÄRDNING AV SYSTEM

Härdning av system är processen att säkerställa att alla system och applikationer är korrekt och säkert konfigureras enligt best practice. Detta inkluderar att säkra administrativa användarlösenord, konfigurationer, använda nätverksprotokoll (telnet vs ssh), nätverkssegmentering, etc.

1. Ändra alla standard administrationslösenord på fartygssystem (Satcom, Navigation, Engine control systems, Serial-to-IP-omvandlare, etc.)
2. Se till att alla inbyggda Wi-Fi-nätverk är ordentligt skyddade och konfigurerade med starka lösenord och protokoll
3. Säkra USB-portar. Se till att du använder dedikerade och säkra USB-enheter om sådana enheter behövs. Kontrollera USB-enheter för skadlig programvara innan du ansluter till kritiska system
4. Anslut inte några personliga, osäkra enheter till fartygssystem eller operativa nätverk. Använd endast dedikerade besättnings nätverk.
5. Skapa standardkonfigurationer för alla system och applikationer som tar hänsyn till cybersäkerhet.
6. Distribuera standardiserade konfigurationer till system och applikationer
7. Skapa checklistor med åtgärder för nya system (ändra standardlösenord, konfigurera säkra inställningar etc.)



Tips:

Använd verktyg för att skapa centrala förvar för konfigurationer och använd automatiserings-verktyg för att hjälpa till med konfigurering av system på ett centraliserat och automatiserat sätt. Standardiserade konfigurationer säkerställer till exempel att standardlösenord ändras och att säkra konfigurationer och protokoll används.

Var särskilt uppmärksam på kritiska system som ECDIS, integrerade bryggsystem, radar, GPS, etc. som ger kritiska funktioner till fartyget och se till att det finns korrekta procedurer för att säkra dessa system från attacker, störningar och spoofing.

Mål:

- Standardiserade och säkra konfigurationer skapas som kan användas för alla system och applikationer i flottan
- Konfigurationer distribueras till system och applikationer på ett centraliserat sätt

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT, nätverks och cybersäkerhetsansvariga
- Externa leverantörer och tredje parter

Att tänka på:

- ❑ *Leverantörssystem kan vara svåra eller omöjliga att automatisera*
- ❑ *Se till att leverantörer följer företagets fastställda krav och instruktioner för sina system*

9. LEVERANTÖRERS CYBERSÄKERHET

De flesta fartyg är beroende av många tredjeparter och leverantörer för drift av kritiska system och tillgångar. Det är viktigt att veta vilka tredjeparter och leverantörer används på fartyget och för att säkerställa att de har lämpliga cybersäkerhetskontroller på plats. Avtalen bör innehålla cybersäkerhetskrav och ansvar som leverantörer måste följa vid leveransen av sin tjänst.

1. Skapa cybersäkerhetskrav för tredjepart och leverantörer som ser till att deras leverans är säker.
2. Kräva att tredje part och leverantörssystem är säkra
3. Se till att externa parter och levrantörer övervakas när de arbetar med kritiska system

Tips:

Cybersäkerhet sägs vanligtvis vara lika säker som den svagaste länken. Cybersäkerheten hos leverantörer är därför viktigt och måste hanteras för att säkerställa att cybersäkerhet hanteras ordentligt. Se till att cybersäkerhetskrav och ansvar dokumenteras och informeras till leverantörer.

Mål:

- Tredjeparts- och leverantörsavtal inkluderar cybersäkerhetskrav som behövs för att säkerställa leverans till fartygen

Ansvarig:

- Nyckelpersoner ansvariga för fartygens IT- och OT-system
- Organisationens IT, nätverks och cybersäkerhetsansvariga
- Marine operations
- Externa tredje parter och leverantörer

Att tänka på:

❑ *Alla tredje parter och leverantörer som används på fartyg*

10. CYBERSÄKERHETSUTBILDNING

Utbildning och medvetenhet om cybersäkerhet är avgörande för hela organisationen, från ledning till anställda och besättning. För att ha en grundläggande förståelse för cybersäkerhet och hur det påverkar fartyget bör besättningen få utbildning i cybersäkerhet. Detta säkerställer att de har kunskap om vad cybersäkerhet är och vad de ska göra för att skydda fartyget.

1. Organisera cybersäkerhetsutbildning för hela besättningen
2. Ge anpassad och relevant utbildning till olika roller i besättningen
3. Genomför cybersäkerhetsutbildning regelbundet
4. Inrätta cybersäkerhetsutbildning som en kontinuerlig del av företagets process och kultur

Tips:

Använd externa utbildningsleverantörer och onlineplattformar för att leverera regelbunden cybersäkerhetsutbildning till Besättnings

Mål:

- Ökad förståelse för cybersäkerhet för alla anställda
- Uppfyller IMO: s riktlinjer för hantering av cyberrisker

Ansvarig:

- Organisationens cybersäkerhetsansvariga
- Fartygens befäl

Att tänka på:

- ❑ *Ge utbildning till alla anställda, inklusive ledande befattningshavare*
- ❑ *Anpassad och relevant utbildning för olika roller*

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI