CENTER FOR CYBERSIKKERHED

Cybersikkerhed i operationelle systemer på skibe

Skibe anvender i stigende grad digitale systemer til at støtte eller varetage kritiske operationer om bord, herunder navigation, kommunikation, maskinkontrol og lastsystemer, de såkaldte OT-systemer (Operationel Teknologi). Disse digitale systemer kan være sårbare over for trusler som hackerangreb, virus med videre, der kan påvirke den operationelle drift af skibe. Denne vejledning skal støtte rederier i at håndtere disse trusler.

Arbejdet med cybersikkerhed kan sammenlignes med andet arbejde med sikkerhed om bord, hvor menneskelige ressourcer, organisatoriske forhold og tekniske løsninger koordineres for at begrænse risici. For eksempel kræver SOLAS-konventionen veluddannede søfolk, klare procedurer og godkendt redningsudstyr. På samme måde kræver effektiv cybersikkerhed både kompetencer og viden hos medarbejderne såvel i land som til søs. I lighed med sikkerhed til søs kræver cybersikkerhed også en klar ansvarsfordeling, det rette tekniske udstyr og de rette processer.

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cfcs@cfcs.dk
www.cfcs.dk

Digitale sårbarheder kan udnyttes via direkte forbindelse til internettet, via en leverandør med ekstern adgang til systemerne eller ved, at besætningen overfører malware til de centrale systemer.

Cybersikkerheden kan styrkes ved at håndtere fire typer af sårbarheder: Manglende viden hos medarbejderne, uklar ansvarsfordeling, manglende processer og usikre tekniske forhold.
Center for Cybersikkerhed anbefaler følgende:

1. **Medarbejderne skal have de rette kompetencer**. Medarbejderne skal vide, hvorfor og hvordan de skal støtte cybersikkerheden i OT-systemer ombord på skibe. Til søs skal besætningsmedlemmerne eksempelvis vide, hvorfor adgangen på tværs af digitale netværk kan være begrænset på trods af, at det kan gøre arbejdet lidt mere besværligt. Organisationen i land skal støtte skibenes sikre drift.
2. **Ansvarsfordelingen skal være klar.** De enkelte besætningsmedlemmer skal vide, hvilket ansvar de har for cybersikkerhed. Besætningsmedlemmerne skal også vide, hvilket ansvar andre besætningsmedlemmer, skibsføreren og organisationen i land har for cybersikkerheden.
3. **Der skal være procedurer, der støtter arbejdet ombord.**
   Der skal være procedurer og politikker for at håndtere cybersikkerheden både til søs og i land. Leverandørkontrakter, herunder charter-kontrakter bør beskrive, hvordan eventuelle konsekvenser af cyberrisici håndteres. Når arbejdet med cybersikkerhed er transparent, kan alle bidrage.
4. **Tekniske tiltag skal begrænse tekniske sårbarheder.**
   Der er flere enkle tekniske tiltag, der kan fremme cybersikkerheden. Det første er at etablere et overblik over de netværk og komponenter, der er på hvert enkelt skib. Dette overblik danner grundlag for overvågning og beskyttelse. Der bør være særligt fokus på de forbindelser hvert skib har til internettet. Adgange til internettet bør overvåges og beskyttes. Det anbefales, at al trafik mellem skibets operationelle systemer og internettet går via rederiet i en krypteret og autentificeret forbindelse. Rederiet kan på den måde beskytte skibet mod kendte trusler og logge datatrafikken.

Beskyttelse af OT-systemer mod cybertrusler skal være specialiseret teknisk viden på tværs af organisationen, det er ikke et afgrænset it-problem. En huskeliste til, hvordan et rederi kan strukturere dette arbejde, findes på næste side.

Huskelisten er ikke en udtømmende liste over anbefalinger og råd til at håndtere de risici, som cybertruslen kan medføre for OT-systemer ombord på skibe. Center for Cybersikkerhed har tidligere udgivet vejledningerne: *Håndtering af industrikontrolsystemer, Informationssikkerhed i leverandørforhold* og *Cyberforsvar der virker.*

Overblik over egne systemer, netværk og eksterne forbindelser

- ◯ Skab og vedligehold et overblik over alle IT- og OT-systemers funktioner, komponenter og netværk på alle skibe.
- ◯ Kortlæg eksterne forbindelser fra alle skibe, herunder forbindelsernes kommunikationsteknologi, protokol samt brugt kryptering og autentifikation.

Nedskriv en informationssikkerhedspolitik

Fastlæg ansvarsfordelingen og samarbejdet mellem organisationen i land og til søs.
Lav procedurer for håndtering af nye trusler eller sårbarheder samt ved nedbrud eller angreb på de forskellige IT- og OT-systemer.
Alle ombord og i land skal bidrage til en styret præventiv og reaktiv indsats, på baggrund af nedskrevet ansvar og opgaver samt tildelte adgange og rettigheder for:

- ◯ Skibsfører
- ◯ Maskinchef
- ◯ Styrmænd
- ◯ Øvrige officerer
- ◯ Andre besætningsmedlemmer
- ◯ Medsejlende vedligeholdelsesteknikere samt eksterne leverandører.

Træn cybersikkerheden til søs og i land

De planlagte procedurer for håndtering af varsler om trusler og sårbarheder skal trænes med jævne mellemrum både til søs og i land. Træningen skal indeholde:

- ◯ Erkendelse af en hændelse,
- ◯ Skadesbegrænsning,
- ◯ Nøddrift,
- ◯ Reetablering af systemernes funktion og data, herunder brug af lokal backup.

De lokale forhold afgør, hvad der er relevant at træne. Det kan for eksempel være:

- ◯ Driftsovervågning af fremdrivningen uden digitale systemer
- ◯ Håndtering af uautoriseret adgang til navigationssystemet
- ◯ Angreb via en leverandør.

Rederiets organisation i land og samarbejdspartnere såsom it-sikkerhedsvirksomheder bør inddrages i træningen, hvis de forventes at bidrage til den operative håndtering af hændelser.

Segmenter og overvåg netværk ombord

Opdel netværket ombord i segmenter med forskellige sikkerhedsniveauer og politikker.

- ◯ Lav regler for datatrafik til og fra hvert enkelt segment
- ◯ Overvåg kritiske segmenter - aktiviteter som portscanninger, firmware-opdateringer og protokoller giver en alarm
- ◯ Log adgangsforsøg til og fra kritiske segmenter
- ◯ Lad rederiet beskytte skibet ved at al trafik går via rederiets firewall.
- ◯ Overvåg opdatering af OT-systemer som navigationssystemer eller maskinkontrolsystem
- ◯ Ikke opdaterbare OT-systemer skal ikke forbindes til internettet.

Inddrag leverandørerne i arbejdet med sikkerhed på en styret måde

- ◯ Inddrag centrale leverandører i udarbejdelsen af beredskabsplaner og øvelser
- ◯ Forpligt leverandørerne til at følge regler for fjernadgang herunder:
  - ◯ Opdatering af OT-systemer bør ske etapevis, så der altid er tilgængelige driftssystemer
  - ◯ Leverandørers fjernadgang skal logges, være tidsmæssigt begrænset og overvåget.