INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telefon: +44 (0)20 7735 7611 Faks: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5. juli 2017

RETNINGSLINJER FOR CYBERSIKKERHET I MARITIM NÆRING

1 På FAL-komiteens (Facilitation Committee) 44. sesjon (4. til 7. april 2017) og sjøsikkerhetskomiteens (MSC) 98. sesjon (7. til 16. juni 2017) ble *Retningslinjer for cybersikkerhet i maritim næring*, slik de fremgår i vedlegget, godkjent etter drøfting av det sterke behovet for å øke bevisstheten rundt cyberrisiko, trusler og sårbarhet på nett.

2 Retningslinjene gir faglige anbefalinger om håndtering av cyberrisiko i maritim næring for å beskytte skipsfarten mot eksisterende og nye cybertrusler og svake punkter. Retningslinjene inneholder også funksjonelle elementer for effektiv håndtering av cyberrisiko.

3 Medlemslandene inviteres til å gjøre innholdet i dette sirkulæret kjent for alle aktuelle aktører.

4 Dette sirkulæret erstatter de midlertidige retningslinjene i MSC.1/Circ.1526

***

VEDLEGG

RETNINGSLINJER FOR CYBERSIKKERHET I MARITIM NÆRING

1 INNLEDNING

1.1 Disse retningslinjene gir faglige anbefalinger om håndtering av cyberrisiko i maritim næring. I dette dokumentet refererer *maritim cyberrisiko* til en målestokk for i hvilken grad en teknologisk ressurs er truet av en mulig omstendighet eller hendelse som kan resultere i skipsfartsrelatert drifts- eller sikkerhetssvikt som en konsekvens av at informasjon eller systemer blir ødelagt, går tapt eller blir skadet på annen måte.

1.2 Alle aktører må gjøre nødvendige tiltak for å beskytte skipsfarten mot eksisterende og nye trusler og sårbarheter innen digitalisering, integrering og automatisering av prosesser og systemer.

1.3 For detaljer og veiledning knyttet til utvikling og implementering av spesifikke risikostyringsprosesser bør brukere av disse retningslinjene vise til aktuelle medlems- og flaggstaters krav og relevante standarder og mønsterpraksis internasjonalt og i bransjen.

1.4 Risikostyring er en grunnleggende forutsetning for trygg skipsfart. Tradisjonelt sett har risikostyring handlet om fysiske operasjoner, men mer digitalisering, integrasjon, automatisering og nettverksbaserte systemer har skapt et økende behov for nettrisikostyring i skipsfarten.

1.5 Basert på målet om å bygge opp under en trygg og sikker skipsfart som er operasjonelt motstandsdyktig mot cyberrisiko, gir disse retningslinjene anbefalinger som kan innlemmes i eksisterende risikostyringsprosesser. Retningslinjene utfyller derfor gjeldende sikkerhetsstyringspraksis som er etablert av IMO.

2 GENERELT

2.1 Bakgrunn

2.1.1 Cyberteknologi er blitt svært viktig for operasjon og styring av en rekke systemer som er avgjørende for sikkerheten innen skipsfart, og for å beskytte det marine miljøet. I noen tilfeller skal disse systemene være i samsvar med internasjonale standarder og flaggstatenes krav. Imidlertid kan sårbarheten som oppstår når det gis tilgang til disse systemene, og når de kobles sammen eller til nettverk, føre til ~~en~~ cyberrisiko som vi må gripe fatt i. Sårbare systemer kan omfatte, men er ikke begrenset til:

.1 brosystemer
.2 systemer for håndtering og styring av last
.3 framdriftssystemer, systemer for styring av maskineri og kraftstyringssystemer
.4 tilgangskontrollsystemer
.5 passasjerservice- og -styringssystemer
.6 offentlige nettverk for passasjerer
.7 administrative systemer og velferdssystemer for mannskap
.8 kommunikasjonssystemer

2.1.2 Skillet mellom informasjonsteknologi og operasjonelle teknologisystemer bør vurderes. Informasjonsteknologisystemer kan betraktes som systemer som bruker data som informasjon. Operasjonelle teknologisystemer er systemer som bruker data for å kontrollere eller overvåke fysiske prosesser. Videre bør beskyttelse av informasjon og datautveksling innen disse systemene også vurderes.

2.1.3 Selv om disse teknologiene og systemene gir en betydelig effektivitetsgevinst for den maritime næringen, utgjør de også en risiko for kritiske systemer og prosesser knyttet til driften av systemer som er vesentlige for skipsfarten. Slik risiko kan skyldes sårbarhet på grunn av utilstrekkelig drift, integrering, vedlikehold og design av nettbaserte systemer, og på grunn av forsettlige og utilsiktede cybertrusler.

2.1.4 Trusler skjer i form av ondsinnede handlinger (f.eks. hacking eller innføring av skadelig programvare) eller utilsiktede konsekvenser av godartede handlinger (f.eks. vedlikehold av programvare eller brukertillatelser). Disse handlingene avslører sårbarhet (f.eks. utdatert programvare og ineffektive brannmurer) eller utnytter sårbarhet innen drifts- eller informasjonsteknologi. Effektiv håndtering av cyberrisiko må ta hensyn til begge typer trusler.

2.1.5 Sårbarhet kan skyldes mangelfull design, integrering og/eller vedlikehold av systemer, samt mangel på nettdisiplin. Når sårbarhet i drifts- og/eller informasjonsteknologi avdekkes eller utnyttes, enten direkte (f.eks. svake passord som fører til uautorisert tilgang) eller indirekte (f.eks. mangel på nettverkssegregering), kan det få følger for konfidensialitet, integritet og tilgang til informasjon. Dessuten, når sårbarhet innen drifts- og/eller informasjonsteknologi avdekkes eller utnyttes, kan det få følger for sikkerheten, spesielt når kritiske systemer (f.eks. bronavigasjon eller hovedframdriftssystemer) blir skadet.

2.1.6 Effektiv håndtering av cyberrisiko må også ta hensyn til sikkerhetshendelser som følge av eksponering eller utnyttelse av sårbarhet i informasjonsteknologisystemer. Dette kan skyldes feil koblinger til operasjonelle teknologisystemer eller operativt personell eller tredje-parter som viker fra prosedyrer, noe som kan være en trussel mot disse systemene (f.eks. feil bruk av flyttbare medier, som minnepinner).

2.1.7 Mer informasjon om sårbarhet og trusler finner du i tilleggsveiledningen og standardene som det vises til i avsnitt 4.

2.1.8 Teknologien og truslene forandrer seg stadig, noe som gjør det vanskelig å håndtere risikoen kun gjennom tekniske standarder. Derfor er anbefalingen i disse retningslinjene en fleksibel risikostyring som er motstandsdyktig og utvikler seg som en naturlig utvidelse av eksisterende sikkehetsstyringspraksis.

2.1.9 Når mulige kilder til trusler og sårbarhet og tilhørende risikoreduserende strategier skal vurderes, bør også en rekke mulige alternativer for håndtering av cyberrisiko tas i betraktning, som styringskontroll, kontroll av drift og prosedyrer og teknisk kontroll.

2.2 **Anvendelse**

2.2.1 Disse retningslinjene er først og fremst ment for alle organisasjoner i skipsfartssektoren, og de er utformet for å oppmuntre til en bedre praksis innen cybersikkerhet og sikkerhetsstyring.

2.2.2 Ingen organisasjoner i skipsfartssektoren er like, så retningslinjene er generelt uttrykt for å kunne bli brukt av mange. Skip som bruker cyber-relaterte systemer i begrenset grad, erfarer kanskje at enkel bruk av disse retningslinjene er tilstrekkelig, mens skip med komplekse cyber-relaterte systemer trenger enda mer beskyttelse og bør finne ytterligere hjelpemidler gjennom anerkjente partnere i bransjen og hos myndighetene.

2.2.3 Disse retningslinjene er veiledende.

3 ELEMENTER AV CYBERRISIKOSTYRING

3.1 I dette dokumentet er *cyberrisikostyring* prosessen med å identifisere, analysere, vurdere og formidle cyberrisiko, og å akseptere, unngå, overføre eller redusere den til et akseptabelt nivå med tanke på kostnader og effekter av tiltak for de involverte.

3.2 Målet med cyberrisikostyring i maritim næring er å bygge opp om en sikker skipsfart som er driftsmessig motstandsdyktig mot cyberrisiko.

3.3 Effektiv cyberrisikostyring bør starte på toppledernivå. Toppledelsen bør sørge for en kultur der alle nivåer i organisasjonen er bevisste på cybersikkerhet, og sikre en helhetlig og fleksibel ordning for cyberrisikostyring som er i kontinuerlig drift og evalueres ved hjelp av effektive tilbakemeldingsmekanismer.

3.4 Én akseptert tilnærming for å oppnå dette er å gjennomføre en omfattende vurdering og sammenligning av organisasjonens nåværende og ønskede posisjon når det gjelder cyberrisikostyring. En slik sammenligning kan avdekke hull det kan jobbes med for å oppnå målene for risikostyring gjennom en prioritert styringsplan for cyberrisiko. En slik risikobasert tilnærming vil gjøre det mulig for organisasjonen å bruke ressursene på den mest effektive måten.

3.5 Retningslinjene presenterer funksjonelle elementer som støtter effektiv cyberrisikostyring. De funksjonelle elementene er ikke plassert i en bestemt orden – alle skal være samtidige og kontinuerlige i praksis og bør innarbeides på en hensiktsmessig måte i et rammeverk for risikostyring.

.1 Identifiser: Definer personellets roller og ansvar innen cyberrisikostyring, og identifiser systemer, maskinvare, data og evner som utgjør en risiko for skipets drift når de forstyrres.

.2 Beskytt: Innfør prosesser og tiltak for risikostyringskontroll, og beredskapsplaner for å beskytte mot cyberhendelser og sikre kontinuitet i driften.

.3 Oppdag: Sørg for å utvikle og innføre nødvendige aktiviteter for å oppdage cyberhendelser i tide.

.4 Reager: Sørg for å utvikle og innføre aktiviteter og planer som gir motstandskraft og gjenoppretter nødvendige systemer for skipsdrift eller tjenester som kan svekkes av en cyberhendelse.

.5 Bygg opp: Identifiser tiltak for å sikkerhetskopiere og gjenopprette nødvendige nettbaserte systemer for skipsdrift som påvirkes av cyberhendelser.

3.6 Disse funksjonelle elementene omfatter aktiviteter og ønskede resultater av effektiv styring av cyberrisiko på tvers av kritiske systemer som påvirker maritim drift og informasjonsutveksling, og utgjør en pågående prosess med effektive tilbakemeldingsmekanismer.

3.7 Effektiv cyberrisikostyring bør sikre et passende nivå av bevissthet om cyberrisiko på alle nivåer i en organisasjon. Bevissthets- og beredskapsnivået bør være tilpasset roller og ansvar i systemet for cyberrisikostyring.

4 BESTEPRAKSIS FOR IMPLEMENTERING AV CYBERRISIKOSTYRING

4.1 Tilnærmingen til cyberrisikostyring som er beskrevet her, gir et grunnlag for bedre forståelse og styring av cyberrisiko, og muliggjør dermed en risikostyringsmetode for å håndtere cybertrusler og sårbarhet. For detaljert veiledning om cyberrisikostyring bør brukere av disse retningslinjene også vise til medlems- og flaggstatenes krav, samt relevante internasjonale og bransjestandarder og beste praksis.

4.2 Ytterligere veiledning og standarder kan omfatte, men er ikke begrenset til:

.1 "The Guidelines on Cyber Security Onboard Ships", utarbeidet og støttet av BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF og IUMI.

.2 ISO/IEC 27001 – standard for informasjonsteknologi, sikkerhetsteknikk, styringssystemer for informasjonssikkerhet og krav. Utgitt i fellesskap av den internasjonale standardiseringsorganisasjonen (ISO) og den internasjonale elektrotekniske kommisjonen (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure *Cybers*ecurity (the NIST Framework).

4.3 Det skal vises til den nyeste versjonen av alle retningslinjer og standarder som brukes.

---

1 Ytterligere veiledning og standarder er oppført som en ikke-uttømmende referanse til mer detaljert informasjon for brukere av disse retningslinjene. De refererte veiledningene og standardene er ikke utstedt av organisasjonen, og hvordan de anvendes, er opp til den enkelte brukeren av disse retningslinjene.