Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

Rapport

Overordnet strategi for maritim digital sikkerhet

Prosjektleder: Nils Haktor Bua

Prosjektgruppe: Andreas Breivik, Johan Stensen, Jarle Kiil, Tore Walden, Håkon Styri, Bjørnar Jon Kleppe, Bente Kristin Hjelle

Framsidefoto: Christopher Bryan M. Sebastian 2019

Versjon	Dato	Kommentar
1	13.11.2020	Klar gjennomlesing SG
2	04.12.2020	Justert etter kommentarer SG og referansegruppe
3	17.12.2020	Klar for leveranse NFD og SD

Innhold

Forord

I tildelingsbrev fra Nærings- og Fiskeridepartementet til Sjøfartsdirektoratet i 2020 har direktoratet fått i oppgave å lede arbeidet med å utarbeide et utkast til en overordnet strategi for maritim digital sikkerhet. Kystverket har i sitt tildelingsbrev fra Samferdselsdepartementet fått i oppgave å delta i utarbeidelsen av strategien.

Prosjektleder for strategiarbeidet har vært Nils Haktor Bua fra Sjøfartsdirektoratet. Prosjektgruppen har i tillegg bestått av Johan Stensen og Tore Walden fra Sjøfartsdirektoratet, Andreas Breivik, Bente Kristin Hjelle og Bjørnar Jon Kleppe fra Kystverket, Jarle Kiil fra Nasjonal Kommunikasjonsmyndighet og Håkon Styri fra Nasjonal Sikkerhetsmyndighet (NSM). Grunnet situasjonen rundt Covid 19, har arbeidet i all hovedsak foregått gjennom digitale møter, foruten ved to anledninger hvor gruppen fikk mulighet til å møtes.

Styringsgruppen for strategien har bestått av kystdirektør Einar Vik Arset, sjøsikkerhets-direktør Arve Dimmen og stabsdirektør Lidvard Måseide fra Kystverket, og fra Sjøfarts-direktoratet fungerende sjøfartsdirektør Lars Alvestad, sjøfartsdirektør Olav Akselsen, administrasjonsdirektør John Malvin Økland, avdelingsdirektør for operativt tilsyn, Alf Tore Sørheim, og fungerende avdelingsdirektør for fartøy og sjøfolk, Håvard Gåseidnes.

For å sikre forankring av strategien fra maritim sektor, har det vært viktig for prosjektgruppen å sørge for involvering fra en bredere gruppe aktører i næringen. Dette ble løst gjennom opprettelse av en referansegruppe i tillegg til møter med enkeltaktører. Referansegruppen har blitt informert om arbeidet som foregår og har fått mulighet til å gi innspill til strategien. På denne måten har prosjektgruppen fått svært mange gode innspill til arbeidet, noe som har dannet grunnlag for flere hovedmål, delmål og tiltak. Referansegruppen har bestått av personer fra følgende aktører:

Norges Rederiforbund	Den Norske Krigs-forsikring for Skib (DNK)	Gard	Fiskebåt	Telenor Maritime
Det Norske Maskinistforbund	Sjømannsforbundet	Sintef	Forsvarets Forskningsinstitutt (FFI)	Bastø Fosen
Norwegian Hull Club	Norske havner	DNV GL	Sperre	Ulstein
Kongsberg	NHO Sjøfart	Hurtigbåtforbundet	Westfal-Larsen Management AS	Bergens forum for cyber security
Vard Elektro	Norsk Romsenter	Kartverket	Forsvaret	

Prosjektgruppen har hatt møter med representanter fra flere havner gjennom fellesorganisasjonen Norske havner, og med utdanningsinstitusjoner gjennom Markom2020. Gruppen har også fått god informasjon om kraftCert og EkomCert gjennom møter med disse. Prosjektgruppen har i tillegg hatt møte med Norges Rederiforbund og DNK, med informasjon om deres arbeid med digitale hendelser.

I tillegg har Norges Rederiforbund, Fiskebåt, NHO Sjøfart, Hurtigbåtforbundet og Kystrederiene bidratt, blant annet i utsendelse av en spørreundersøkelse til sine medlemmer.

For å understøtte arbeidet har Sintef og DNV GL utført analysearbeid om tidligere hendelser og sårbarheter knyttet til digitale trusler i sektoren.

En stor del av utviklingen som foregår nå, skjer gjennom ulike former for digitalisering og automatisering. Dette gjelder også for maritim sektor. Digital sikkerhet har i denne utviklingen lett for å bli glemt, og ikke minst, mangle fokus. Gjennom en felles overordnet strategi håper prosjektgruppen at aktuelle myndigheter setter en tydelig retning for arbeid knyttet til digital sikkerhet.

Rapporten oppsummerer arbeidet utført av prosjektgruppen, og er bygd opp med en strategidel og en handlingsplan med tilhørende risikobilde og tiltaksplan. I tillegg er rapporter fra analyser utført av DNV GL og Sintef vedlagt. Delingen av strategi og handlingsplan med tilhørende risikobilde og tiltaksplan er gjort for å sørge for at strategien står seg over lengre tid, i et dynamisk digitalt risikobilde. Prosjektgruppen anbefaler at risikobilde og tiltaksplan revideres jevnlig for å unngå innføring av utdaterte tiltak som følge av at risikobildet endres.

Med håp og ønske om at strategien skal gi et bidrag til økt digital sikkerhet i maritim sektor!

Nils Haktor Bua

prosjektleder

Johan Stensen

Bente Kristin Hjelle

Andreas Breivik

Jarle Kiil

Håkon Styri

Bjørnar Kleppe

Tore Walden

Sammendrag

Utkastet til overordnet strategi for maritim digital sikkerhet er utarbeidet av en prosjektgruppe sammensatt fra Sjøfartdirektoratet, Kystverket, Nasjonal kommunikasjonsmyndighet og Nasjonal sikkerhetsmyndighet. Oppdraget er gitt fra Nærings- og Fiskeridepartementet til Sjøfartsdirektoratet, og fra Samferdselsdepartementet til Kystverket.

For å sørge for maritim digital sikkerhet angir strategien fem hovedmål innen kategoriene digitalisering, infrastruktur, samarbeid, egenbeskyttelse, og utdanning og kompetanse. De fem hovedmålene er som følger:

- Digitalisering i maritim næring er gjennomgående sikker og tillitvekkende
- Den maritime næringen understøttes av pålitelig og sikker digital infrastruktur
- Styrket samarbeid og erfaringsutveksling gir den maritime næringen forbedret evne til å avdekke, håndtere og motvirke digitale angrep
- Den enkelte aktør i maritim næring har evne til egenbeskyttelse mot digitale angrep
- Mannskap og personell har nødvendig digital sikkerhetskompetanse

Hovedmålene i strategien støttes av tilhørende delmål, og egne tiltak for oppnåelse av mål i en separat handlingsplan. Handlingsplanen er bygget ut fra dagens risikobilde. Tiltakene er lagt frem fra prosjektgruppen, basert på innspill fra referansegruppe, Nasjonal strategi for digital sikkerhet, Rammeverk for håndtering av IKT-hendelser, Samfunnssikkerhetsinstruksen, Sårbarhetsanalyse fra DNV GL, Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet fra Sintef, møter med aktører i næringen samt annet materiale.

Det mest omfattende tiltaket prosjektgruppen legger frem er opprettelse av et responsmiljø for maritim sektor. Tiltaket har bakgrunn i et uttalt behov fra næringen gjennom referansegruppen, nasjonal strategi for digital sikkerhet, rammeverk for håndtering av IKT-hendelser og innføring av NIS-direktivet i nasjonal lovgiving. Tiltaket vil ha påvirkning på flere av strategiens mål og delmål, og er plassert som tiltak under hovedmålet: «Styrket samarbeid og erfaringsutveksling gir den maritime næringen forbedret evne til å avdekke, håndtere og motvirke digitale angrep».

Av tiltakene fremlagt, anbefaler prosjektgruppen følgende tidsramme for implementering:

Tiltak	Anbefalt tidsramme for implementering
Tiltak 1	Mellomlang sikt - 1-2 år
Tiltak 2	Lang sikt - 2-5 år
Tiltak 3	Lang sikt - 2-5 år
Tiltak 4	Mellomlang sikt - 1-2 år
Tiltak 5	Lang sikt - 2-5 år
Tiltak 6	Mellomlang sikt - 1-2 år
Tiltak 7	Kort til mellomlang sikt - 0-2 år
Tiltak 8	Kort til mellomlang sikt - 0-2 år
Tiltak 9	Kort sikt - 0-1 år

Tiltak	Anbefalt tidsramme for implementering
Tiltak 10	Kort til mellomlang sikt - 0-2 år
Tiltak 11	Kort til mellomlang sikt - 0-2 år
Tiltak 12	Kort sikt - 0-1 år
Tiltak 13	Kort til mellomlang sikt - 0-2 år
Tiltak 14	Kort til mellomlang sikt - 0-2 år
Tiltak 15	Kort til mellomlang sikt - 1-3 år
Tiltak 16	Mellomlang sikt - 1-2 år
Tiltak 17	Kort til mellomlang sikt - 0-2 år

Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

Overordnet strategi for maritim digital sikkerhet

Prosjektleder: Nils Haktor Bua

Prosjektgruppe: Andreas Breivik, Johan Stensen, Jarle Kiil, Tore Walden,
Håkon Styri, Bjørnar Jon Kleppe, Bente Kristin Hjelle

Framsidefoto: Steinar Haugberg

Versjon	Dato	Kommentar
1	13.11.2020	Klar gjennomlesing SG
2	04.12.2020	Justert etter kommentarer SG og referansegruppe
3	17.12.2020	Klar for leveranse NFD og SD

Innhold

1. Innledning

I en tid der globalisering har vist oss at verden er mindre enn det vi gjerne liker å tro, er det mer enn noen gang behov for å skaffe oversikt over sårbare næringer, og sikre disse. Norge er blant landene i verden som er raskest til å ta i bruk ny teknologi. Norske myndigheter jobber for at både private og offentlige virksomheter skal ta i bruk og utvikle digitale løsninger, fordi det gir store muligheter for effektivisering, konkurransekraft og nye arbeidsplasser. Dette gjelder også i maritim sektor.

At fokuset på digital sikkerhet i den maritime sektoren bør styrkes, kan relateres til økt digitalisering og at de digitale løsningene har blitt mer komplekse, både for fartøyene og for sektoren generelt. Sektoren har en kritisk samfunnsfunksjon som transportør av passasjerer og gods, både nasjonalt og internasjonalt, og som viktig tjenesteyter til blant annet olje- og gassnæringen. I tillegg har sektoren, med fartøy og havner, en viktig rolle opp mot Forsvaret knyttet til transport og mottak av allierte forsterkninger.

Sektorens digitalisering skjer både i tradisjonelle systemer for informasjonsteknologi (IT-systemer) og i operasjonell teknologi (OT) i systemer for automatisering, fremdrift, styring og andre kontrollsystemer. Ved digitale hendelser i OT-systemer kan konsekvensen for skipets drift være alvorlig[1]. I tillegg forventes det en utvikling med mer fjerntilkobling, integrering og digitalisering av OT-systemer. Økt interesse og utvikling i retning av selvgående, ubemannede og autonome fartøyer er også faktorer som tilsier behov for økt fokus på digital sikkerhet i sektoren.

Sektorens avhengighet til IT-systemer gjør den sårbar for digitale hendelser. IT-systemer i maritim sektor skiller seg i liten grad fra IT-systemer i andre sektorer, og dermed er tilgjengeligheten for sikkerhetsløsninger for disse større enn på OT-systemer. Digitale IT-hendelser kan likevel gi konsekvenser for skipsoperasjoner gjennom å sette ut administrative systemer for lastepapirer, passasjerlister, digitale sertifikater og seilingstillatelser og lignende, og på denne måten forsinke eller forhindre driften av fartøyet. Slike hendelser vil også kunne gi store økonomiske konsekvenser i tillegg til konsekvenser for omdømmet for utsatte aktører.

Maritim sektor består av få enheter, sammenlignet med veitransport. Det finnes omtrent 95 000 skip i UNCTADs[2] database. Av dette er ca. 50 000 skip over 1000 tonn. Dette betyr at det er begrensede ressurser til mer systematiske analyser og forbedringsprosesser innen bransjen, også angående digital sikkerhet. I tillegg er sektoren del av et meget kostnadssensitivt marked på grunn av sterk internasjonal konkurranse om fraktoppdrag. Dette gir en stor andel operatører og skip som ikke prioriterer digital sikkerhet høyt nok.[3]

Et skip vil vanligvis seile mellom 25 og 35 år og oppgraderinger gjøres trinnvis slik at utstyr om bord ikke skiftes ut samtidig. Det betyr også at det er stor variasjon i datautstyr om bord i skipene, både for administrative funksjoner og for styringssystemene. Med hensyn til digital sikkerhet, kan dette være en fordel fordi det kan være vanskeligere å finne en enkelt sårbarhet som kan utnyttes i mange av systemene samtidig. Det kan også være en ulempe fordi det er vanskelig å drifte systemene og å sørge for oppdaterte operativsystemer og sikkerhetsmekanismer.

1 DNV GL - 2020-09-15 ROS analyse for maritim digital sikkerhet
2 United Nations Conference on Trade and Development
3 SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet

Maritim sektor har sterke internasjonale tilknytninger, der norske skip seiler i internasjonalt farvann, mens norsk maritim infrastruktur og farled benyttes av skip med utenlandsk flagg. Den internasjonale tilknytningen går også igjen i sterk regulering gjennom internasjonale instrumenter, og deltakelse i internasjonale organisasjoner. Internasjonal regulering gir ulemper ved at det ofte blir minimumskrav som gjelder, men også fordeler ved at sikkerhetsaspektet er prioritert og tilstedeværende.

Det fraktes varer for store verdier i norsk farvann. I 2019 var total eksport på sjø fra Norge i overkant av 120 millioner tonn, mens den totale importen på sjø var i overkant 30 millioner tonn[4]. I tillegg fraktes rundt 55 millioner passasjerer innenriks, og mer enn 6 millioner passasjerer reiste i 2019 mellom norsk og utenlandsk havn[5]. Mer enn halvparten av skipstransporten som går til, fra og mellom norske havner, skjer med skip med utenlandsk flagg. I 2019 registrerte Kystverket i overkant av 121.000[6] meldepliktige ankomster til 810 ulike norske lokasjoner. Disse tallene inkluderer ikke innenriks rutegående bil- og persontransport. Rundt 70% av disse ankomstene hadde annen norsk havn som sitt forrige anløpssted. Omtrent 55 % av anløpene var lasteskip, 20% offshore/spesial, 10% tankskip, 10% passasjerfartøy og rundt 5% fiskefartøy.

Også i havner skjer en økt digitalisering og stadig flere av havneoperasjonene automatiseres. En gjennomgang av tidligere hendelser i sektoren, viser at også havner er utsatt for digitale hendelser[7]. Flere hendelser viser angrep på IT og administrative systemer, som har ført til driftsstans, informasjonstyveri og manipulasjon knyttet til smugling av gods.

Norsk internasjonalt skipsregister (NIS) inneholdt ved utgangen av 2019 totalt 668 skip, mens Norsk ordinært skipsregister (NOR) inneholdt hele 20820 fartøyer. Totalt gir disse fartøyene en panteverdi på omtrent 3000 milliarder norske kroner[8].

I tillegg utgjør skip med betydelige norske eierinteresser og utenlandsk flagg en stor del av norsk maritim sektor, sammen med tjeneste- og utstyrsleverandører og verft. Alt i alt utgjør maritim sektor i Norge en total verdiskaping på 147 milliarder norske kroner og sysselsetter rundt 90.000 arbeidere[9]. I overkant av 21.000 nordmenn har i dag ett eller flere gyldige maritime sertifikater[10].

Parallelt med utviklingen og digitaliseringen av skip og havner, pågår det også en økende automatisering av farleden. Tall fra september 2020 viser at totalt 3039 fyrstasjoner og lanterner langs norskekysten er fjernovervåket[11].

4 SSB - Tonnmengder som eksporteres gjennom norsker havner https://www.ssb.no/statbank/table/10916/
5 SSB - https://www.ssb.no/statbank/table/04225/
6 Kystverket
7 SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet
8 Sjøfartsdirektoratet – statistikk fra Skipsregistrene
9 Maritimt Forum - Maritim-Verdiskapingrapport 2020
http://s3-eu-west-1.amazonaws.com/maritimt-forum.no/documents/Maritim-Verdiskapingrapport2020.pdf
10 Sjøfartsdirektoratet
11 Kystverket

På bakgrunn av denne egenarten er maritim sektor utsatt for digitale trusler, og verdien av sektoren gir potensielt store konsekvenser ved et angrep. Analyser av tidligere hendelser viser at sektoren er utsatt for trusler fra ulike aktører, gjennom mange angrepsvektorer og angrep av ulik type. Trusselaktører i maritim sektor kan være alt fra kriminelle, uforsiktige eller misfornøyde ansatte og leverandører, konkurrenter og aktivister, til statsaktører. Motivasjonen for et angrep kan blant annet være ønske om å vandalisere eller å lage systemforstyrrelser, ønske om publisitet (for et budskap eller lignende), spionasje, vinningskriminalitet, eller i ytterste konsekvens krig og terror.

Strategien skal gi en oversikt over aktører som har viktige roller med hensyn på digital sikkerhet i maritim sektor. Strategien inneholder en beskrivelse av risikobildet i sektoren, en tiltaksplan for de ulike myndighetsrollene for å øke den digitale sikkerheten samt gode råd til den enkelte maritime virksomhet for å øke egen bevissthet og kompetanse.

Strategien for maritim digital sikkerhet skal gi et godt utgangspunkt for en felles retning og samarbeid i kampen mot uønskede angrep mot sektorens digitale systemer.

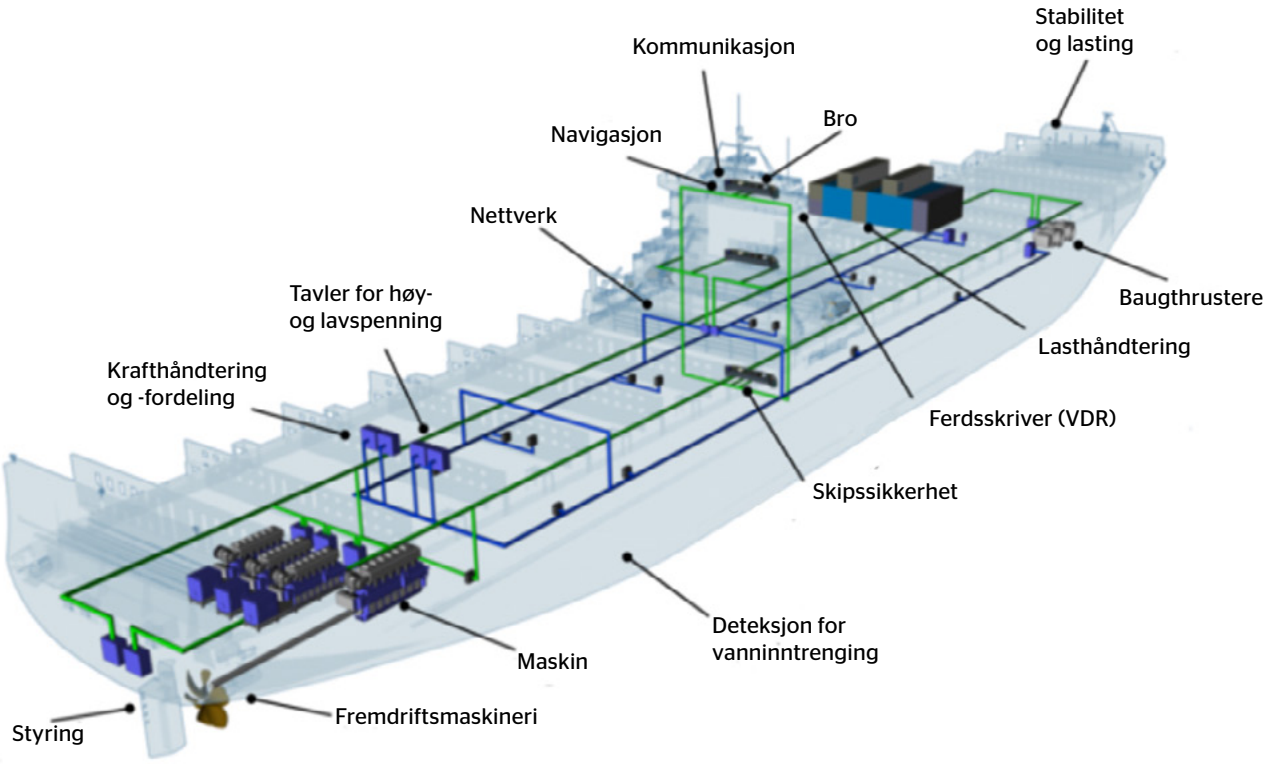
2. Omfang

Denne strategien bygger videre på Nasjonal strategi for digital sikkerhet[12] og peker på betydningen dette har for den maritime sektoren. Målsetting, aktørbilde, trusselbilde og tiltak fra Nasjonal strategi kan på et overordnet plan videreføres til den maritime sektoren, men er i denne strategien spisset mot sektoren. Dette er gjort for å gi et best mulig bidrag i arbeidet for en sikker digital hverdag i maritim sektor.

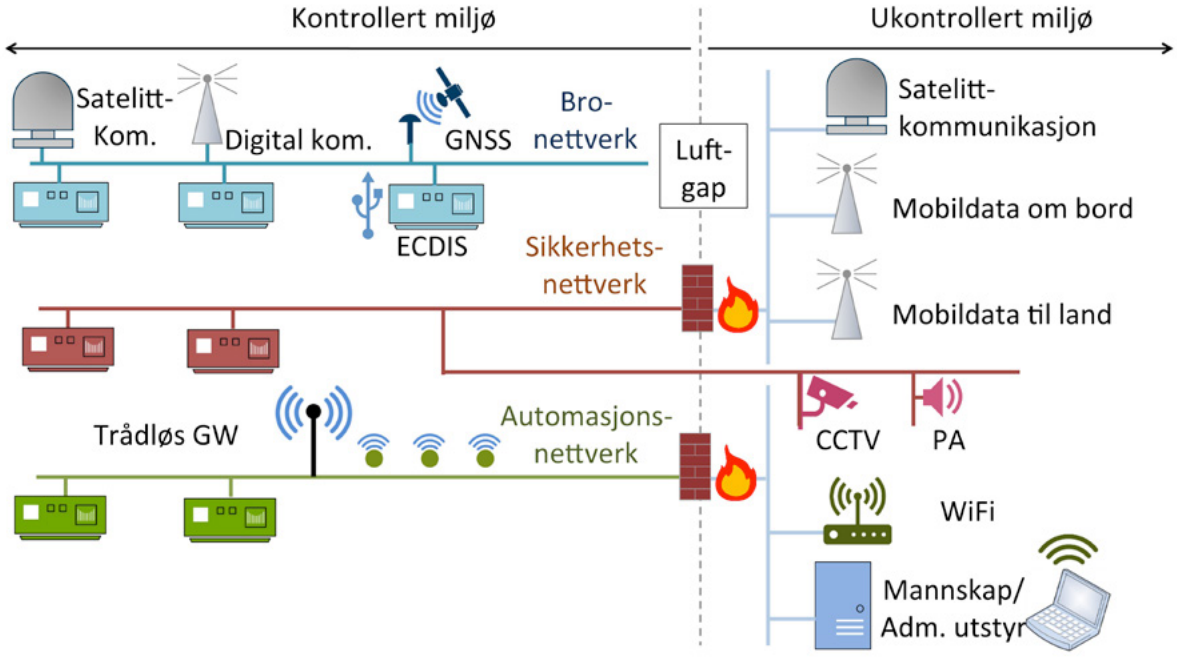
Strategien og tilhørende handlingsplan skal gi et bidrag til økt digital sikkerhet for norske skip, skip med norske interesser og verdier, utenlandske skip i norsk farvann, havner og farledsaktører.

Figurene 1 og 2 viser konseptuelle skisser over typiske digitale systemer om bord i fartøy, og figur 3 og 4 viser kommunikasjonskanaler og navigasjonssystemer som normalt brukes til og fra skip og i havn. Alle de tre figurene peker på systemer som er utsatte for digitale trusler.

12 Regjeringen - https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

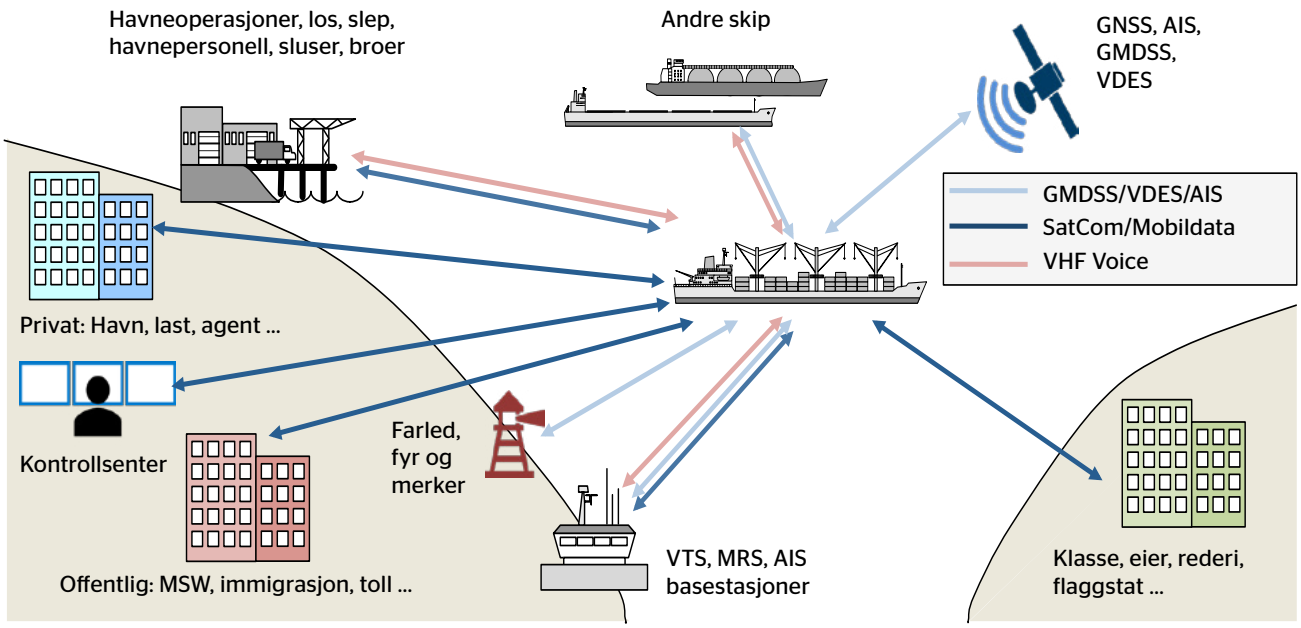


Figur 1 - Eksempelfigur digitale systemer om bord i fartøy[13]

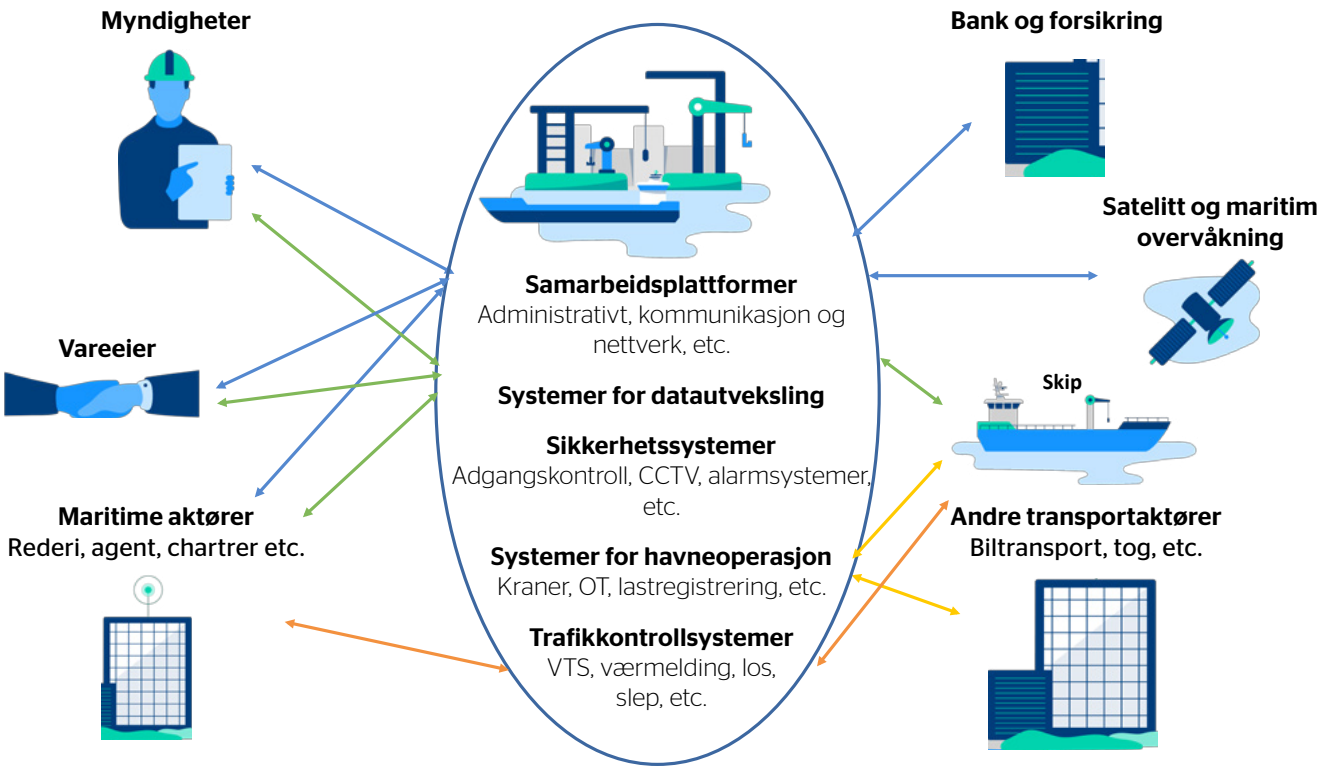


Figur 2 - Generelt datasystem om bord i skip[14]

13 DNV GL - 2020-09-15 ROS analyse for maritim digital sikkerhet - DNV GL copy right
14 SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet



Figur 3 - Generelle kommunikasjonskanaler til og fra et skip[15]



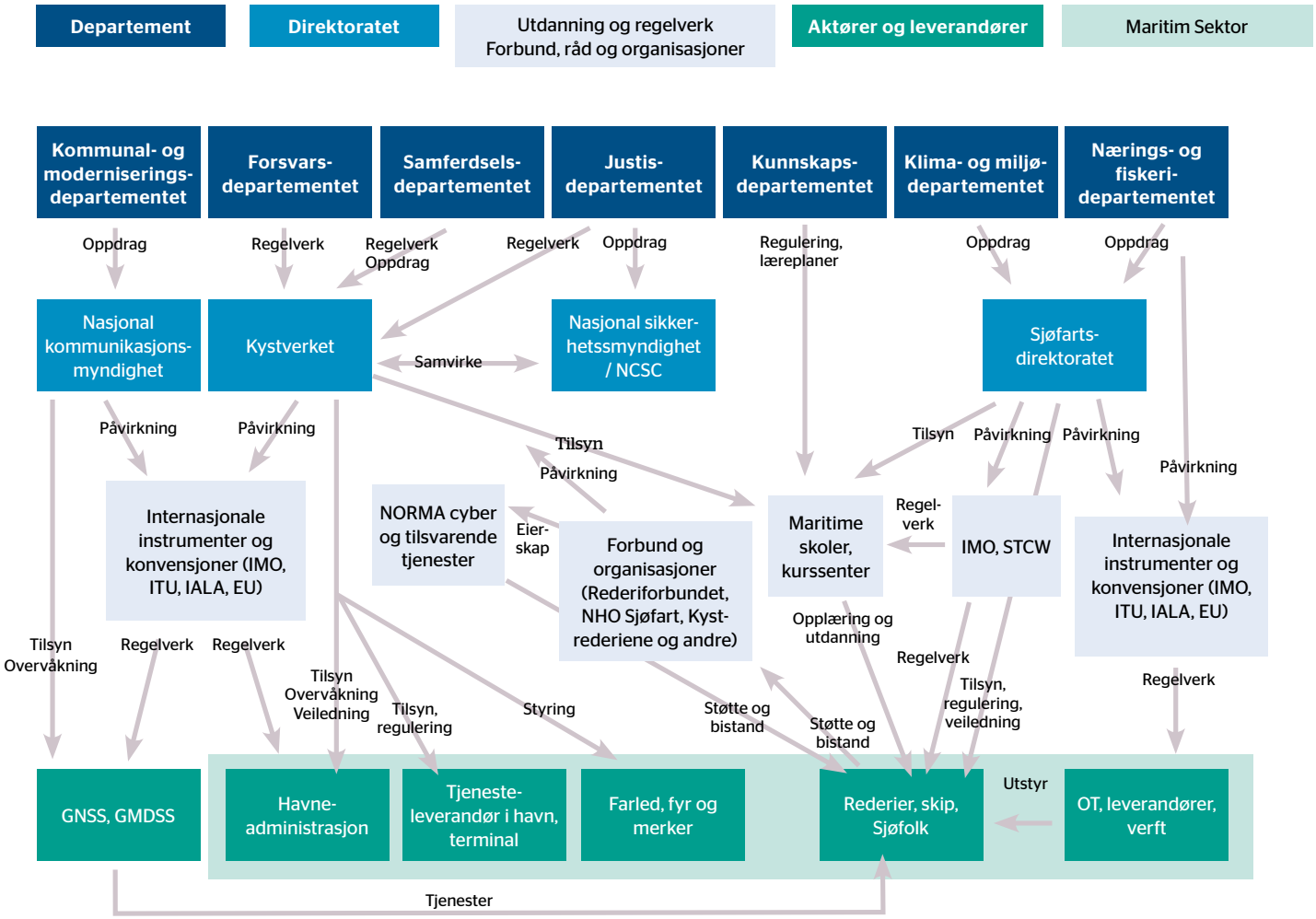
Figur 4 - Generelle kommunikasjonskanaler til og fra havn

15 SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet

3. Definisjon av maritim digital sikkerhet

Maritim digital sikkerhet omfatter håndtering av risiko, sikkerhetsmessige utfordringer og vurdering av konfidensialitet, integritet, tilgjengelighet knyttet til de digitale systemer som er nødvendig for sikker seilas, drift, operasjon, og systemer for håndtering av informasjon om fartøy, last og personer om bord.

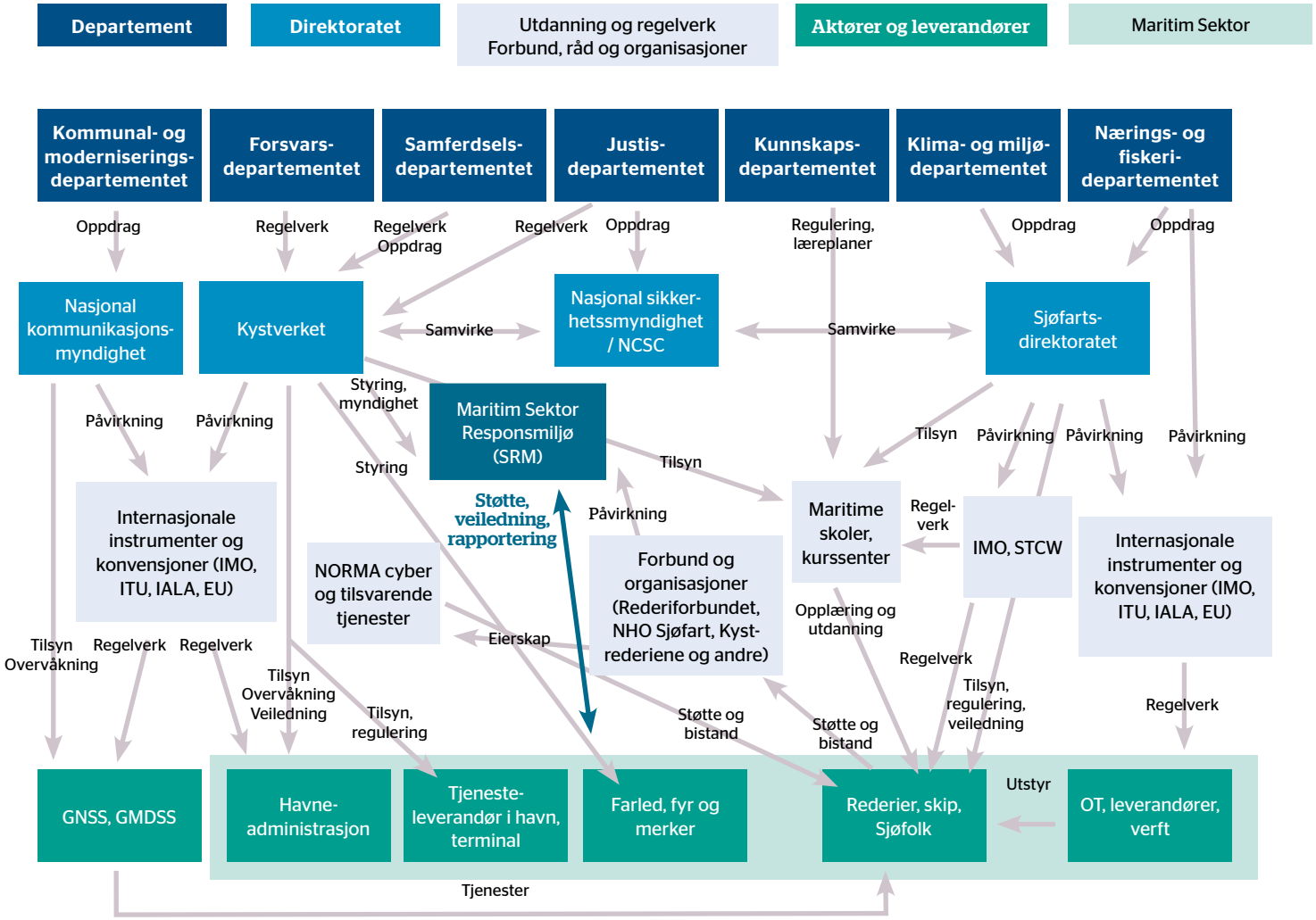
Med dette menes all informasjon, alle systemer om bord og all kommunikasjon til og fra skipet. Dette inkluderer også systemer på land som har potensiale til å direkte eller indirekte skade sikker seilas, drift og operasjon av skip, havner og farled.



Figur 5 - Aktørkart - Maritime digitale avhengigheter og samhandlinger ved inngangen til strategiperioden

4. Aktørkart

Figur 4 viser aktørkartet for avhengigheter i maritim sektor for digitale systemer, ved inngang til strategiperioden. Den angir myndighetsrollene som tilsyn- og veiledningsorgan, regelverkspåvirkning, utvikling og samhandling mellom myndighetsaktører, skip, sjøfolk, utdanningsinstitusjoner, leverandører, tjenesteleverandører, havner og farledsaktører. Figur 5 viser aktørkart ved utgang av strategiperioden, med et opprettet responsmiljø for maritim sektor.



Figur 6 - Aktørkart - Maritime digitale avhengigheter og samhandlinger ved utgangen av strategiperioden

Foto: Bjarne Hovland 2017

5. Strategimål

Strategien skal gi grunnlag til at

5.1. Digitalisering i maritim sektor er gjennomgående sikker og tillitvekkende

Digitalisering og den generelle utviklingen av teknologi i maritim sektor foregår kontinuerlig. Endrede fremdriftssystemer, nye energibærere, nye kommunikasjonsbehov og mer automatisering av fartøy er blant trendene som driver utviklingen. Målet er at digital sikkerhet skal bidra til effektiv og trygg utvikling. Digital sikkerhet bør være del av enhver digitalisering av maritim sektor.

I Norge er det et stort antall prosjekter knyttet til utvikling av og mot økende grad av autonomi for fartøyer. Det gjøres testing på mange modeller og mindre testfartøyer under kontrollerte forhold. I tillegg bygges det flere fartøyer, hvor ubemannet operasjon i kommersiell drift er målsetning. Det er derfor grunn til å tro at vi innen kort tid ser fartøy med høy grad av autonomi og ubemannet operasjon seilende sammen med konvensjonelle fartøy.

For å oppnå dette målet settes følgende delmål:

- Virksomhetene kjenner verdiene, verdikjedene og risikoen knyttet til sine digitale løsninger.
- Et omforent internasjonalt regelverk, som setter krav og støtter opp om sikker digitalisering, til alle ledd i sektoren, inkludert leverandørene, foreligger
- Virksomhetene i maritim sektor har tilgang til, og benytter seg av tilgjengelig rammeverk og beste praksis for digital sikkerhet

5.2. Den maritime sektoren understøttes av pålitelig og sikker digital infrastruktur

Maritim sektor har en samfunnskritisk funksjon gjennom sin rolle som transportør av last og passasjerer, der omtrent 75% av alt gods som fraktes til eller fra Norge fraktes på skip[16]. En robust og pålitelig digital infrastruktur for kommunikasjon, navigasjon og i havn og farled er viktig for å opprettholde samfunnsfunksjonen.

I tillegg til ulike kommunikasjonssystemer utgjør særlig satellittnavigasjonssignaler og sjøtrafikksentraltjeneste med trafikkovervåking en viktig del av den digitale infrastrukturen. I likhet med andre tilbydere av samfunnsviktige tjenester er sjøtrafikksentraltjenesten omfattet av NIS-direktivet. I likhet med andre tilbydere av samfunnsviktige tjenester er VTS omfattet av NIS-direktivet.

For å oppnå dette målet settes følgende delmål:

- Det er tydelig ansvarsfordeling og oversikt over kritisk digital infrastruktur for maritim sektor
- Eiere av kritisk digital infrastruktur i sektoren gjennomfører risiko og sårbarhetsvurderinger og nødvendige sikringstiltak
- Myndighetene fører tilsyn med at den digitale sikkerheten er ivaretatt i kritisk maritim infrastruktur
- Virksomhetene har tillit til digitale tjenester og infrastruktur

5.3. Styrket samarbeid og erfaringsutveksling gir den maritime sektoren forbedret evne til å avdekke, håndtere og motvirke digitale angrep

Samarbeid og deling av informasjon er essensielt for å forhindre, avdekke og respondere ved et angrep. Behovet for samarbeid går på tvers av offentlig og private aktører, samtidig som ansvarsroller må være tydelige. Nasjonal strategi for digital sikkerhet peker på viktigheten av offentlig og privat samarbeid for å forhindre konsekvenser av digitale trusler. Det er også pekt på behovet for samarbeid opp mot digitale trusler i maritim sektor gjennom Rammeverk for håndtering av IKT-hendelser, utgitt av Justisdepartementet. Innføringen av NIS-direktivet i norsk lovgivning vil også stille krav til økt samarbeid.

For å oppnå dette målet settes følgende delmål:

- Sektoren har gjennom et maritimt responsmiljø tilgang til:
  - et tydelig, helhetlig og omforent aktør-, rolle- og ansvarskart for maritim sektor
  - et oppdatert situasjons- og risikobilde for maritim sektor, og felles forståelse av dette
  - en samarbeidsarena for informasjonsdeling, varsling, håndtering, læring og erfaringer fra digitale trusler og angrep
  - regelmessige øvelser på sektorovergripende hendelser og øvelser på internasjonalt nivå

16 SSB - https://www.ssb.no/statbank/table/08812/

5.4 Den enkelte virksomhet i maritim sektor har evne til egenbeskyttelse mot digitale hendelser

Hver enkelt virksomhet må ha et bevisst forhold til egenbeskyttelse knyttet til digital sikkerhet. Økt egenbeskyttelse oppnås gjennom helhetlig sikkerhetsstyring, planer, rutiner og systemforståelse. 1. januar 2021 stiller ISM-koden krav til at det utarbeides planer for håndtering av digital sikkerhetsrisiko for skip og rederier. God egenbeskyttelse vil bidra til å forhindre angrep, dempe spredning og redusere konsekvenser av digitale trusler. Sjøfartsdirektoratet vil fra 1. januar 2021 føre tilsyn med at rederier og skip har inkludert planer for digital sikkerhetsrisiko som en del av sikkerhetsstyringssystemet (ISM).

ISPS-koden stiller krav om at for alle skip som går i internasjonal fart, og for de havneanlegg som betjener disse, skal den obligatoriske sikringsrisikoanalysen omfatte datasystemer og nettverk, og i den utstrekning denne avdekker en risiko som må håndteres, skal det utarbeides sikringsplaner som adresserer denne.

Også NIS-direktivet[17] påpeker at rederier og havner/havneanlegg, i den utstrekning de tilbyr en samfunnsviktig tjeneste, skal gjennomføre en risikovurdering av de nettverk og informasjonssystemer som benyttes for å levere tjenesten. For å redusere den avdekte risikoen skal disse virksomhetene iverksette hensiktsmessig og proporsjonale tekniske og organisatoriske sikringstiltak. Videre skal virksomhetene, for å opprettholde tjenesteleveransen, iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser. På europeisk nivå har blant annet ENISA TRANSSEC Expert Group[18] arbeidet med disse problemstillingene.

For å oppnå dette målet settes følgende delmål:

- Den enkelte virksomhet kjenner egne verdier, avhengigheter, eksterne innsatsfaktorer og risikoer og utarbeider krise- og beredskapsplaner for digitale trusler og hendelser.
- Virksomhetene i sektoren benytter anbefalte verktøy og metoder for utføring av risikovurderinger med grunnlag i sin vurdering av konfidensialitet, integritet, tilgjengelighet og kritikalitet i sine informasjonsbehandlingssystemer
- Virksomhetene i sektoren har inkludert håndtering av digital sikkerhetsrisiko i sitt sikkerhetsstyringssystem
- Virksomhetene i sektoren har høyt fokus på kompetanse, intern sikkerhetskultur og sikkerhetsstyring knyttet til digital sårbarhet.
- Virksomhetene i sektoren er forberedt på at uønskede hendelser kan skje og øver regelmessig på digitale hendelser og inkluderer sine ansatte

5.5. Sjøfolk og personell har nødvendig digital sikkerhetskompetanse

For å redusere omfanget av utbredelse, spredning og å minimere konsekvensene av digitale trusler, er det behov for digital sikkerhetskompetanse blant sjøfolk og personell i maritim sektor. Få eller ingen skip har personell med spesifikk IT-kompetanse om bord. Samtidig skiller IT-systemer i den maritime sektoren seg lite fra IT-systemer i andre bransjer. IT-systemer er bygget på forholdsvis moden teknologi når det kommer til IKT-sikkerhet, sammenlignet med OT-systemer hvor også konsekvensen av en hendelse kan være stor[19]. Digital sikkerhetskompetanse blant sjøfolk og personell vil derfor være nødvendig.

Ifølge SSB var det ved utgangen av 2019 i overkant av 26.000[20] maritime lønnstakere i Norge, hvor arbeidet utføres til sjøs på fartøy eller flyttbare innretninger. I overkant av 700 starter som lærlinger i matros-, motormann- og skipselektrikerfaget hvert år, i tillegg til rundt 500 på offisersutdanning[21]. Utdanningen av sjøfolk bygger på regler som er beskrevet i internasjonal norm for opplæring, sertifikater og vakthold for sjøfolk i STCW-konvensjonen. Tilbakemeldingene fra maritime utdanningsinstitusjoner er at det er i dag er lite fokus på digital sikkerhet i utdanning av sjøfolk. Nasjonal strategi for digital sikkerhetskompetanse viser til NIFU-rapporten,[22] som retter søkelys på akutt behov for digital sikkerhetskompetanse, samtidig som at etter- og videreutdanningstilbudet innenfor digital sikkerhet synes å være begrenset. Det er dermed et stort behov for etter- og videreutdanning innen digital sikkerhetskompetanse i maritim sektor.

17 Regjeringen - https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
18 ENISA - https://resilience.enisa.europa.eu/transport-security
19 DNV GL - 2020-09-15 ROS-analyse for maritim digital sikkerhet
20 SSB - https://www.ssb.no/statbank/table/12749/
21 Tall fra Maritimt opplæringskontor
22 NIFU IKT-sikkerhetskompetanse i arbeidslivet - behov og tilbud. Rapport 2017:32

For å oppnå dette målet settes følgende delmål:

- utdanning av sjøfolk i Norge og globalt, og personell i maritim sektor i Norge inkluderer fagområdet digital sikkerhet
- relevante utdanningsinstitusjoner har et etter- og videreutdanningstilbud innenfor digital sikkerhet for sjøfolk og personell i maritim sektor for å dekke kompetansegapet
- internasjonalt maritimt regelverk har tilstrekkelig krav til digital sikkerhetskompetanse for sjøfolk
- Spesialisering innen digital sikkerhet i maritim sektor er en del av utdanningsmulighetene i utdanninger der IKT har en sentral plass

6. Vedlegg

1. Overordnet risikobilde og tiltaksplan
2. Rapporter
- SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet
- DNV GL - ROS-analyse for maritim digital sikkerhet

Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

Vedlegg 1 - Det digitale risikobildet i maritim sektor og tiltaksplan

Innhold

1. Det digitale risikobildet – maritim sektor

1.1. Målgruppe

Dette risikobildet er laget for å understøtte arbeidet med nasjonal strategi for digital sikkerhet i maritim sektor og gi et grunnlag for å foreslå og prioritere tiltakene i dette dokumentet. Beskrivelsen er derfor avgrenset til forhold som er særlig relevante for denne sektoren og den er på et overordnet nivå. For utdypende beskrivelser og eksempler viser vi til vedlagte rapporter: ROS-analyse for maritim digital sikkerhet utført av DNV GL og Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet utført av SINTEF.

Det har de senere årene vært en økende grad av cyberrelaterte angrep innenfor maritim sektor. Det er forutsatt at lesere har kjennskap til det generelle digitale risikobildet som gjelder alle sektorer. For den enkelte aktør i maritim sektor er det nødvendig å ta hensyn til virksomhetens verdier, egenart og aktivitet når man skal vurdere hvilke trusler som bør prioriteres i virksomhetens egen risikohåndtering.

1.2. Avgrensning av sektoren

Begrepet maritim sektor er i strategien avgrenset til følgende hoveddeler:

- For skipsfart som virksomhet, er strategien avgrenset til fartøy registrert i skipsregistrene NOR og NIS, også når fartøyene opererer utenfor norsk farvann.
- All skipsfart i norske farvann, med særlig vekt på trafikken i farleden langs kysten og de norske sjøtrafikksentralene.
- Alle norske havner som benyttes av den over nevnte skipstrafikk.
- Norske farledsaktører og myndigheter
- Det er ikke utarbeidet egne tiltak for totalforsvaret, nordområdene og eller endringer i skipsfarten utover den daglige driften sektoren operer i fredstid.

1.3. Kort beskrivelse av verdiene i maritim sektor

Skipsfart er en av Norges eldste næringsaktiviteter og sysselsetter i dag rundt 90 000 personer og skaper verdier for til sammen 140 mrd. Regjeringen satser på hav og Norge har tatt en internasjonal lederrolle i globale havspørsmål. Mer enn 200 000 nordmenn jobber innenfor olje, sjømat eller maritim sektor, og i 2017 skapte havnæringene verdier for 680 milliarder kroner.

Maritim sektor har sterke internasjonale knytninger, der norske skip seiler i internasjonalt farvann, og norsk maritim infrastruktur og farled benyttes av skip med utenlandsk flagg. Rundt tre fjerdedeler av godstransport inn eller ut av Norge gjøres på skip. I 2019 var total eksport på sjø fra Norge i overkant av 120 millioner tonn, mens den totale importen på sjø var i overkant 30 millioner tonn[23]. I tillegg fraktes rundt 55 millioner passasjerer innenriks og mer enn 6 millioner passasjerer reiste i 2019 mellom norsk og utenlandsk havn[24]. Mer enn halvparten av skipstransport som går til, fra og mellom norske havner skjer med skip med utenlandsk flagg. I 2019 registrerte Kystverket i overkant av 121.000[25] meldepliktige ankomster til 810 ulike norske lokasjoner. Disse tallene inkluderer ikke innenriks rutegående bil- og persontransport. Rundt

23 SSB - Tonnmengder som eksporteres gjennom norsker havner https://www.ssb.no/statbank/table/10916/
24 SSB - https://www.ssb.no/statbank/table/04225/
25 Kystverket

70% av disse ankomstene hadde annen norsk havn som sitt forrige anløpssted. Omtrent 55 % av anløpene var lasteskip, 20% offshore/spesial, 10% tankskip, 10% passasjerfartøy og rundt 5% fiskefartøy. Meld.St.35 (2015-2016) «På rett kurs – Forebyggende sjøsikkerhet og beredskap mot akutt forurensning» inneholder en analyse av skipstrafikken i norsk farvann som bidrar til å beskrive verdiene maritim sektor representerer. Også Meld.St.33 (2016-2017) «Nasjonal transportplan 2018-2029» bidrar til beskrivelsen av dette trafikkbildet.

1.4. Generelt om trusselbildet

Trusselbildet for maritim sektor omfatter direkte trusler mot nasjonale interesser, virksomhetene i sektoren og aktiviteten som skjer i sektoren. Maritim sektor representerer en så stor del av verdikjeden for det norske samfunnet med transport av gods og passasjerer til, fra og mellom norske havner, at maritim sektor også kan være et mål for trusselaktører som ønsker å ramme virksomheter i andre sektorer.

Tyveri av gods under transport er en vesentlig trussel. Fartøyene med mannskap og last representerer store verdier og kan kapres for å kreve løsepenger. Dette er ikke rene digitale trusler, men sammensatte trusler hvor en trusselaktør benytter digitale virkemidler for å nå et mål. Det er også viktig å være oppmerksom på at et stort antall virksomheter tilfeldig kan rammes av digitale angrep trusselaktører har rettet mot andre mål. Det er derfor svært viktig å ta hensyn til det generelle digitale risikobildet som nevnt innledningsvis.

En opplisting av eksempler på relevante uønskede hendelser i maritim sektor finnes i de vedlagte rapportene fra DNV GL og SINTEF. Det er viktig å merke seg at ny teknologi som for eksempel utviklingen av autonome fartøy gjør det nødvendig å være oppmerksom på at dette vil gi nye utfordringer i trusselbildet.

1.5. Trusselbildet omfatter fred, krise og krig

Norge er avhengig av at maritim sektor kan opprettholde virksomhet i krise og krig. Dette krever at virksomhetene i sektoren har beredskapsplaner for som tar høyde for trusselbilder som kan oppstå i slike situasjoner. I dette risikobildet har vi ikke behandlet slike trusselbilder spesielt, men vi forutsetter at risikovurdering for den digitale sikkerheten tar høyde for at det kan oppstå tilstander hvor trusselaktørene har svært høy yteevne. Maritim sektor omfatter norsk skipsfart i alle farvann. Dette betyr at selv om det er en normal tilstand i norskefarvann kan norske skip være underveis eller ligge i havner i områder hvor det er krise eller krigstilstand.

1.6. Typer av trusselaktører

Det er hensiktsmessig å dele trusselaktører inn i noen få grupper for å få en viss forståelse for bredden av evner og motiver de forskjellige trusselaktørene kan ha.

Statlige aktører er aktører som ofte har stor yteevne og som har ressurser til å gjennomføre operasjoner som går over lang tid. Motivene kan være etterretning, påvirkning eller å hindre skipstrafikk inn til, ut fra eller gjennom et område. Operasjoner kan være rettet mot skipstrafikk eller forsøke å bruke fartøy som et virkemiddel i operasjoner rettet mot andre mål. Dette betyr at et skip med norsk flagg kan bli et mål for en statlig aktør på grunn av faktorer som flagg, last den har om bord eller skal hente, hvilken havn den seiler fra eller til, eller farvannet det seiler gjennom.

Terrororganisasjoner eller organisasjoner med politiske hovedmål kan bruke digitale eller sammensatte operasjoner for å ramme sine motstandere eller for å nå sine politiske mål. Disse trusselaktørene kan også bruke vinningskriminalitet for å finansiere sin egen virksomhet og er en type aktører som kan gjennomføre kapring av skip både som politisk virkemiddel og som vinningskriminalitet.

Organisert kriminalitet er trusselaktører som kan ha relativt stor yteevne. Denne typen aktører gjennomfører både rene digitale operasjoner og utnytter digitale virkemidler for å gjennomføre sammensatte operasjoner. Et eksempel vil være at digitale virkemidler bidrar til å gjennomføre tyveri av gods, smugling eller kapring av skip. Motivasjonen er alltid vinningskriminalitet og ressursene som brukes på hver enkelt operasjon vil som regel begrenses av forventet utbytte.

Digital vinningskriminalitet er trusselaktører som kun gjennomfører rene digitale operasjoner. Disse aktørene kan ha relativt stor yteevne. Enkelte operasjoner er automatisert slik at de rettes mot et større antall ofre. Kriminaliteten kan omfatte tyveri av opplysninger som kan selges til andre, tyveri av databehandlingskapasitet som kan selges til andre eller brukes til andre formål, forskjellige typer operasjoner hvor formålet er å kreve penger fra offeret og lignende aktiviteter. Et eksempel på slik kriminalitet er bruk av løsepengevirus. Digital vinningskriminalitet omfatter også salg eller utleie av verktøy, infrastruktur eller kompetanse til andre trusselaktører.

Løst organiserte grupper og enkeltpersoner er en type trusselaktører med moderat til lav yteevne og som kan ha dels politiske og dels personlige motiver for sin aktivitet. I noen tilfeller er motivasjonen en kombinasjon av nysgjerrighet og tilfeldighet hvor personer leter etter tjenester med kjente sårbarheter som er eksponert på nett. Denne typen aktivitet gir risiko for sikkerhetsbrudd eller driftsforstyrrelser i virksomhetene som eier tjenestene.

1.7. Digitale systemer og infrastruktur i maritim sektor

Begrepet maritim digital sikkerhet er definert i strategidokumentet. Digitale system kan deles inn i IT-systemer og OT-systemer, hvor OT står for operasjonsteknologi og er beslektet med industrielle styrings- og kontrollsystemer. OT-system kan i praksis inneholde vanlig IT-teknologi som kommuniserer med standard nettverksteknologi og som kan kobles til det åpne internettet. Det kan også være teknologi som er spesielt utviklet for formålet og som bruker bransjespesifikke standarder for kommunikasjon.

For et skip kan OT-systemer brukes for navigasjon, manøvrering, fremdrift, lastehåndtering og lignende. Digitale angrep rettet mot IT- eller OT-systemer kan forstyrre eller hindre utførelsen av skipets oppdrag. Angrep rettet mot OT-system kan få konsekvenser for sjødyktighet, manøvreringsevne eller fremdrift. Digitale angrep mot OT-systemer kan også påvirke navigasjon og medføre situasjoner med fare for grunnstøting og sammenstøt med annen

skipstrafikk. En utfordring knyttet til OT-systemer er at teknologien og systemene som er i bruk på forskjellige skip representerer et spenn på flere tiår i alder.

Både IT- og OT-systemer kan kommunisere med rederi, operatør eller leverandør via satellittsystemer, via mobilt bredbånd i farvann nær kysten og via mobilt bredbånd eller fast tilknytning når skipet ligger ved havn. Normalt er det ikke ønskelig at OT-systemer kobles direkte opp mot det åpne internettet, men ved skanning av nettet er slike tilkoblinger observert. Som følge av COVID-19 er det sett en økning av tilkobling av OT-systemer til nett for å muliggjøre vedlikehold og tilsyn uten fysisk tilstedeværelse[26]. En mer detaljert beskrivelse av digitale systemer på skip finnes i de vedlagte rapportene fra DNV GL og SINTEF.

For havner vil det også være en tilsvarende inndeling av IT- og OT-systemer hvor de sistnevnte gjerne brukes til håndtering av last. For trusselaktører kan IT-systemer i havner gi tilgang til opplysninger om hvor verdifullt gods er oppstilt og hvilke skip de forskjellige kontainere eller varer skal lastes på eller er losset fra. Angrep som forstyrrer IT- og OT-systemer i havner, kan som konsekvens forstyrre skipstrafikken og godstransporten til og fra havnen.

Den digitale infrastrukturen knyttet til sjøtrafikksentralene eies og drives av offentlig myndighet og er i hovedsak landbasert selv om den overvåker farleden og navigasjonsinstallasjoner i langs farleden.

1.8. Overordnet risikobilde

Eventuell stans i utskiping av gods fra Norge vil spesielt få betydning for bedrifter langs kysten inkludert for eksport av olje fra Kårstø, Mongstad, Sture og Melkøya. Stans i import, særlig med tanke på ferger, containerskip og havner i Oslofjorden, kan få betydning for innføring av kritiske varer til landet. Rundt 20-25% av all import av stykkgods og containergods til Norge går på skip eller ferge inn Oslofjorden[27], og avhenger av tilgang på skip og at havner og farvann er åpent. Drivstoffterminalen på Sjursøya i Oslo er særlig kritisk for drivstoffleveranser til fly på Gardermoen og drivstoff i det sentrale østlandsområdet[28].

I den vedlagte rapporten fra DNV GL, er det gjennomført en risiko-, sårbarhet- og modenhetsanalyse for maritim digital sikkerhet med fokus på skipsdrift. Sammendraget i denne rapporten gir et overordnet risikobilde for denne delen av maritim sektor. Anbefalingen i rapporten er at de kritiske systemene for å opprettholde sikker skipsdrift bør prioriteres. For OT-systemer er risikoen vurdert som middels til høy. I den vedlagte rapporten fra SINTEF er det beskrevet en rekke eksempler på uønskede hendelser, og denne rapporten omtaler også digital sikkerhet for havner.

Det er viktig å se det digitale risikobildet i sammenheng med det generelle risikobildet for maritim sektor. En analyse av det generelle risikobildet for maritim sektor finnes i Meld.St.35 (2015-2016) «På rett kurs – Forebyggende sjøsikkerhet og beredskap mot akutt forurensning». I rapportens kapittel 4 om forebyggende sjøsikkerhet er flere av de risikoreduserende tiltakene, eller deler av tiltakene, digitale løsninger. Da blir digital sikkerhet en forutsetning for at de forebyggende tiltakene har tilsiktet effekt.

Mange av de uønskede hendelsene som beskrives i de over nevnte rapporter er avgrenset til å få konsekvenser for enkelte skip, men den største hendelsen som er beskrevet på side

26 NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems" https://us-cert.cisa.gov/ncas/alerts/aa20-205a
27 TØI, Kystverket 2009
28 Sårbarhet og beredskap i godstransport TØI rapport 1324/2014 - https://www.toi.no/getfile.php?mmfileid=38962

19 i rapporten til SINTEF, cyberhendelse A15 som fant sted i 2017, fikk konsekvenser for «nær en femtedel av verdens shipping-operasjoner, inkludert 76 havner». De fem havnene i Norge med størst antall meldepliktige anløp har i gjennomsnitt 88 meldepliktige anløp per uke. Konsekvensen av hendelser som rammer en enkelt havn, vil i de fleste tilfeller være begrenset ettersom skipstrafikk kan benytte alternative havner. Hendelser som rammer flere havner samtidig over lengre tid kan bli utfordrende for varetransport.

Introduksjonen av autonome fartøy vil medføre en utvikling av risikobildet som tilsier at prinsippet om innebygd sikkerhet følges i utviklingen av de digitale løsningene. Med autonome fartøy er det nødvendig å ta høyde for en risiko for uønskede hendelser som rammer flere fartøy samtidig i større grad enn i dag.

2. Tiltaksplan

Med grunnlag i risikobildet beskrevet over, analysene utført av Sintef og DNV GL, innspill fra referansegruppen, Justistisdepartementet sitt rammeverk for håndtering av IKT-hendelser, Nasjonal strategi for digital sikkerhet og NIS-direktivet, fremmer prosjektgruppen følgende tiltak for å oppnå målene i strategi for maritim digital sikkerhet.

2.1. Tiltak hovedmål 1 – Digitalisering i maritim sektor er gjennomgående sikker og tillitvekkende

2.1.1. Tiltak 1 Autonomi

Kystverket og Sjøfartsdirektoratet skal følge utviklingen av autonomi i skipsfarten tett og påvirke utviklingen av internasjonalt regelverk på området, etablere norsk regelverk og infrastruktur i Norge for å ivareta digital sikkerhet for autonome fartøy.

Sjøfartsdirektoratets RSV 12-2020 «Føringer i forbindelse med bygging eller installering av automatisert funksjonalitet, med hensikt å kunne utføre ubemannet eller delvis ubemannet drift» legger føringer for slike fartøyer. Sjøfartsdirektoratet må sørge for at digital sikkerhet er i fokus for denne utviklingen og at det er en integrert del av all digitalisering av skipsfart. Det må gjøres systematiske vurderinger av digital sikkerhet i kommunikasjon med andre fartøyer og landorganisasjon og aktører, kommunikasjon mellom systemer om bord og for navigasjonssystemer. Kystverket må sørge for at autonome fartøy kan kommunisere med instanser for farledskontroll og havner.

2.1.2. Tiltak 2 Digital sikkerhet i ytelseskrav

Ytelseskrav og typegodkjenninger bør inkludere krav til digital sikkerhet. Kommunikasjons- og navigasjonssystemer reguleres i dag gjennom Forskrift av 30. august 2016 nr. 1042 om skipsutstyr. Sjøfartsdirektoratet bør ta initiativ, sammen med aktuelle klasseselskaper, til at fremtidige utarbeidelser og oppdateringer av internasjonale ytelsesstandarder for kommunikasjons- og navigasjonssystemer inneholder krav til digital sikkerhet. Det bør også vurderes om dette skal inkludere kontrollsystemer.

2.2. Tiltak hovedmål 2 - Den maritime sektoren understøttes av pålitelig og sikker digital infrastruktur

2.2.1. Tiltak 3 Digital sikkerhet i maritim kommunikasjon

Mange av de maritime informasjons- og sjøsikkerhetstjenestene er utviklet og standardisert for mange år siden, og digital sikkerhet er ivaretatt i varierende grad. Internasjonale standardiseringsorganisasjoner, ledet an av IMO, arbeider med å digitalisere de maritime tjenestene som en del av E-navigasjonskonseptet. I Norge tester prosjektet CySiMS Public Key-sertifikater for å sikre kommunikasjon mellom skip og mellom skip og land. Relevante norske myndigheter skal ta nødvendige initiativ i IMO, ITU, IALA og andre relevante internasjonale organisasjoner og arbeide aktivt for at de kommende digitale tjenester og den tilhørende infrastruktur ivaretar digital sikkerhet på en god måte. Dette inkluderer at maritim kommunikasjon beskyttes mot uønskede inngrep og inneholder sikker autentisering av identitet for deltakere i maritim kommunikasjon.

2.2.2. Tiltak 4 Overvåke signalene fra satellittnavigasjonssystemene

Satellittnavigasjon har over tid utviklet seg til å bli en viktig kilde til posisjonsbestemmelse av skip. I 2018 utarbeidet Samferdselsdepartementet en nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse (På rett sted til rett tid)[29], med tiltak rettet mot å redusere samfunnets sårbarhet mot svikt i satellittnavigasjonssystemene.

Det er viktig at navigatørene raskt får kjennskap til feil og upålitelighet i satellitt-navigasjonssignalene, slik at andre navigasjonsmetoder kan tas i bruk. NKOM og Kystverket skal sikre at satellittnavigasjonssignalene som brukes av skip i norske farvann overvåkes systematisk, og at der er gode varslingsrutiner til skip om feil eller upålitelighet i GNSS.

2.2.3. Tiltak 5 Digitalisering av kommunikasjon

En del av den maritime kommunikasjonen er fortsatt analog gjennom tale i VHF/MF/HF-systemene, uten mulighet for autentisering av de som kommuniserer, og uten mulighet til konfidensialitet i tilfeller der dette behøves. Kystverket og Sjøfartsdirektoratet skal blant annet gjennom arbeid i internasjonale organisasjoner, bidra til at denne kommunikasjonen digitaliseres slik at autentisitet og konfidensialitet kan ivaretas. Det er imidlertid viktig at dette gjøres uten å svekke sikkerhetsgevinst for alle aktører som kommer fra åpen kommunikasjon.

2.2.4. Tiltak 6 AIS integritet

AIS-systemet er et av de aldrende maritime kommunikasjonssystemene nevnt under tiltak 4. AIS er et viktig anti-kollisjonssystem for skip i dag og informasjon om skipsbevegelser fra systemet utgjør også en viktig del av grunnlaget for mange av oppgavene til maritime myndigheter. Tilsiktet deaktivering eller manipulering av AIS-utstyr på skip sammen med tekniske feil utgjør en fare for sikkerheten.

Kystverket skal etablere et system for å systematisk oppdage feil eller manipulering av informasjon i AIS-systemet, og følge opp at feil rettes og sørge for å varsle myndighetene som bruker AIS i sin overvåking.

29 https://www.regjeringen.no/contentassets/abd1dec7647a4c22aaef7d93046e3f2b/pa-rett-sted-til-rett-tid.pdf

2.2.5. Tiltak 7 Kritisk maritim infrastruktur

Kystverket og Sjøfartsdirektoratet skal arbeide for at aktører med ansvar for kritiske deler av maritim digital infrastruktur har oversikt over sine verdikjeder, eksterne innsatsfaktorer og ansvarsrolle.

2.2.6. Tiltak 8 NIS-direktivet

Ved innføringen av NIS-direktivet i nasjonal lovgivning skal relevante myndigheter, deriblant Sjøfartsdirektoratet og Kystverket, forskriftsfeste hvilke tilbydere som omfattes av dette regelverket, samt gi nærmere bestemmelser som gjelder krav til sikkerhet.

2.3. Tiltak hovedmål 3 – Styrket samarbeid og erfaringsutveksling gir den maritime sektoren forbedret evne til å avdekke, håndtere og motvirke digitale angrep

2.3.1. Tiltak 9 Responsmiljø for maritim sektor

Sektorbasert responsmiljø (SRM) opprettes for maritim sektor (fremtidig maritim CERT), som et samarbeid mellom Sjøfartsdirektoratet og Kystverket.

Sjøfartsdirektoratet og Kystverket vil samarbeide om opprettelse av et felles SRM for maritim sektor. Innhold og oppsett av senteret skal være i henhold til beskrivelse under.

Nasjonal strategi for digital sikkerhet peker i sitt tiltak 38[30] på implementering av sektorvise responsmiljøer. I rammeverket for håndtering av IKT-hendelser, utpekes departementene som ansvarlige for å oppnevne SRM i sektorene og for å sikre at SRM til enhver tid oppfyller gjeldende krav og forventninger som stilles til denne funksjonen. Kjernen i det sektorvise responsmiljøet er at de har en myndighet innenfor sektoren, og kan pålegge tiltak både ved forebygging og håndtering. Nøyaktig hvordan det sektorvise responsmiljøet skal se ut vil nødvendigvis variere innenfor de ulike sektorene.

Også gjennom NIS-direktivet settes det krav til styrket IKT-sikkerhet og samarbeid. NIS-direktivet er det første EU -direktivet som regulerer digital sikkerhet i Europa. Direktivet har som formål å styrke IKT-sikkerheten i EU, og er en av flere tiltak for å nå målene i EUs strategi for digital sikkerhet, «an Open, Safe and Secure cyberspace». Direktivet ble vedtatt av EU-parlamentet den 6. juli 2016 og trådte i kraft i august i fjor. Direktivet er et minimumsdirektiv og setter dermed minimumskrav til medlemsstatene både når det gjelder direktivets virkeområde og krav til sikkerhet. Dette medfører at medlemsstatene kan velge å innføre strengere regler enn det som fremgår av direktivet. Justisdepartementet foreslår imidlertid at den nye loven skal tilsvare kravene i direktivet.

Nasjonal sikkerhetsmyndighet (NSM) skal innen 31.12.2020 gi anbefalinger til Justisdepartementet om hvordan kravene i direktivet skal følges opp. Både Sjøfartsdirektoratet og Kystverket er i dialog med NSM om hvordan NIS-direktivet skal oppfylles innen maritim sektor, for skip og havner. En rekke tiltak og vurderinger er under arbeid, men et område som peker seg ut, er å få etablert et kontaktpunkt for støtte, veiledning og håndtering ved digitale

30 Regjeringen - www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt--nasjonal-strategi-for-digital-sikkerhet.pdf

angrep i sektoren, samt deling av beste praksis, kunnskap og informasjon om digitale trusler og styrking av den digitale sikkerheten i maritim sektor.

Når ISM-koden fra 1. januar 2021 stiller krav til at det utarbeides planer for håndtering av digital sikkerhetsrisiko, for skip og rederier, er det også et behov for et mottak for rapportering av digitale hendelser.

Tilgang på tjenester fra SRM for maritim sektor tilbys til virksomheter i maritim sektor som rederier, fartøy, nasjonale havner og havneterminaler og utstyrs- og tjenesteleverandører både nasjonalt og internasjonalt.

Anbefalt innhold og opprettelse av responsmiljø (SRM) i maritim sektor

Et sektorvis responsmiljø (SRM) for maritim sektor etableres på oppdrag fra Nærings - og fiskeridepartementet og Samferdselsdepartementet i henhold til samfunnssikkerhetsinstruksen[31] basert på krav til SRM beskrevet i Rammeverk for håndtering av IKT-sikkerhetshendelser. Responsmiljøet bør ha en offentlig styring, tilknytning og/eller eierskap, basert på at et slikt miljø bør ha en myndighetsrolle ovenfor aktørene og må være tilgjengelig for alle aktører i den maritime sektor.

SRM for maritim sektor skal være et knutepunkt for digitale sikkerhetshendelser i sektoren, og ha relasjoner både til maritime virksomheter, øvrige SRM-er i Norge og utenlands og til Nasjonalt cybersikkerhetssenter (NCSC).

SRM skal ha ansvar for å utføre løpende risikovurdering og utarbeide et oppdatert risikobilde for sektoren knyttet til digital sikkerhet, og et aktørkart over nasjonale aktører med ansvar og roller for digital sikkerhet i sektoren, både private og statlige. For å kunne ivareta sektor-rollen må SRM-en derfor ha god kunnskap om sektorens egenart, kritisk infrastruktur og kritiske samfunnsfunksjoner, og være spesielt fokusert mot digitale hendelser knyttet til sektorens OT-systemer.

SRM for maritim sektor skal etablere og iverksette rutiner og metoder/verktøy for hendelsesrapportering og håndtering, og være mottakssenter for hendelser i sektoren. Miljøet skal ha analysekapasitet for å bistå virksomhetene i sektoren ved hendelser og trusler. SRM-en skal utarbeide situasjonsrapporter under pågående hendelser. Videre skal SRM rapportere til oppdragsgiver, tilhørende virksomheter, andre responsmiljø i Norge og utlandet, og andre interessenter. Ved håndtering av hendelser har SRM ansvar for å holde oversikt over omfang av hendelsen og se hendelser innenfor samme sektor i sammenheng og gi råd om tiltak til virksomheter innenfor sektoren.

For rapportering av digitale hendelser vurderes Forskrift av 27. juni 2008 nr. 744 om

melde- og rapporteringsplikt ved sjøulykker og andre hendelser til sjøs, i tillegg til meldings- og rapporteringsplikt gjennom Sikkerhetsloven for virksomhetene det vil gjelde for, som tilstrekkelig hjemmelsgrunnlag for krav til rapportering av digitale hendelser.

En viktig del av responsmiljøets oppgaver og ansvar er læring, kunnskap og erfaringsutveksling gjennom informasjonsdeling, møter og samhandling med virksomheter i sektoren, og mellom øvrige SRM-er og NCSC. Responsmiljøet skal også bidra i evaluering av hendelser i sektoren og sørge for at sektoren og virksomheter lærer av og øker evnen til å

31 Samfunnssikkerhetsinstruksen – Lovdata - https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349

håndtere lignende hendelser. Senteret skal også være en pådriver for øvelsesvirksomhet i egen sektor og delta i øvelser i og utenfor sektor.

Senteret skal tilby døgnbemannet vaktordning ved IKT-sikkerhetshendelser/trusler. I tillegg kan senteret ha behov for å anskaffe teknisk bistand og beredskap fra 3.parts leverandører (IT-sikkerhetsspesialister).

SRM skal også ha ansvar for beredskapsplaner for håndtering av større hendelser, sikkerhetspolitiske kriser og krig knyttet til det digitale rom. Planene er koordinerte med nasjonalt planverk og rammeverk fra NCSC. Responsmiljøet bør også bidra inn mot Nasjonalt beredskapssystem (NBS) og underliggende Sivilt beredskapssystem (SBS).

I utarbeidelsen av denne strategien og spesifiseringen av dette tiltaket har prosjektgruppen sett på organisasjonsmodellene til EkomCert og kraftCert. Prosjektgruppen har i tillegg hatt møte med Norges Rederiforbund og DNK, med informasjon om deres arbeid med opprettelse av Norwegian Maritime Cyber Resilience Centre (NORMA Cyber). Basert på erfaringer fra responsmiljøene i EkomCert og kraftCert, bør SRM miljøet for maritim sektor starte med en grunnbemanning på 6-7 personer for å kunne dekke vaktordning og ansvaret beskrevet over. Videre økning i ansvar, oppgaver og bemanning bør vurderes på sikt, basert på erfaringer og behov. Dersom senteret opprettes i en organisasjon som alt vedlikeholder døgnkontinuerlig vakt for andre formål vil behovet for bemanning kunne reduseres betydelig.

Tilgang på tjenester fra SRM for maritim sektor tilbys til virksomheter i maritim sektor som rederier, utstyrsleverandører, tjenesteleverandører, farledsaktører og havner.

Kostnadene i et slikt senter vil avhenge av flere faktorer og innhold og vil bli høyere om det legges opp til sensornett, økt analysekapasitet og lignende.

Et maritimt SRM må sørge for å opprette samarbeid med aktuelle aktører, både offentlige og private, som operasjonssentre i næringen, havarikommisjonen og andre. Relasjon må avtalereguleres for virksomheter som ligger utenfor offentlige tilsynsområder. Godt samarbeid og å unngå interessekonflikter er essensielt for å få til en best mulig håndtering av digitale trusler og hendelser.sensielt for å få til en best mulig håndtering av digitale trusler og hendelser.

2.3.2. Tiltak 10 Totalforsvaret

Den maritime sivile sektor er en stor leverandør inn i Totalforsvarskonseptet, der totalforsvaret er en grunnstein for den nasjonale beredskapen i fred, krise og krig. Det nye totalforsvarskonseptet bør tuftes på fremtidsrettet digitale sikkerhetsløsninger som ivaretar sivile og militærsamfunnsoppgaver. Et fremtidsrettet maritimt nasjonalt responsmiljø bør bygge videre på et tett og godt samarbeid for å skape en proaktiv felles situasjonsforståelse innenfor digital sikkerhet i maritim sektor, og på den måten bidra til Totalforsvaret. Et maritimt digitalt responsmiljø bør bidra til å ivareta støtte i kriser Norge kan stå ovenfor, og støtte oppunder:

- rask og proaktiv informasjonsflyt med fokus på de involverte aktørene
- forsvarets operative hovedkvarter (FOH) som et proaktivt forovervendt miljø hvor informasjonsflyt på digital sikkerhet som fordeler og ivaretar de sivile og kommersielle aktørene også i en sikkerhetspolitisk krise. Og sørge for et gjensidig samarbeid med maritim sektor og et eventuelt responsmiljø i sektoren
- strategiske rammeavtaler med sivile, kommersielle aktører bør følges opp med et tett samarbeid innenfor digital sikkerhet.

2.4. Tiltak hovedmål 4 - Den enkelte virksomhet i maritim sektor har evne til egenbeskyttelse mot digitale hendelser

2.4.1. Tiltak 11 Virksomheters verdier og avhengigheter

Sjøfartsdirektoratet og Kystverket skal følge opp at virksomhetene i maritim sektor har oversikt over sine verdier, avhengigheter, eksterne innsatsfaktorer og risikoer og utarbeider krise- og beredskapsplaner for digitale trusler og hendelser.

Sjøfartsdirektoratet og Kystverket skal:

- arbeide for et tydelig og harmonisert regelverk rettet mot digital sikkerhet
- sørge for deling av beste praksis
- være tydelige i forventning til håndtering av digital sikkerhet i sikkerhetsstyringssystem i henhold til ISM-koden
- utarbeide materiell for støtte til å gjennomføre lokale risikoanalyser for digitale trusler om bord på fartøy eller i rederi og havner
- arbeide for at internasjonal lovgivning sammen med nasjonale regler harmoniseres, og kan forstås helhetlig
- være pådriver for informasjonskampanjer rettet mot virksomhetene i sektoren, som tydeliggjør behovet for fokus på digital sikkerhet, inkludert behovet for å øve regelmessig på håndtering av hendelser
- være bidragsyter i relevante forsknings- og utviklingsprosjekter for digital sikkerhet
- støtte oppunder relevante samarbeidsforumer
- aktivt arbeide for, og ta initiativ til at IMOs og EU regelverk om havnesikring skal styrkes inn mot maritim digital sikkerhet

2.4.2. Tiltak 12 Sårbarhetskartlegging

Digital sikkerhet skal i større grad være del av og fokuseres på i Sjøfartsdirektoratets og Kystverkets aktivitet, for å øke bevisstheten på området. Konkret bør Sjøfartsdirektoratet og Kystverket årlig kartlegge sårbarheter for digitale trusler og implementeringsmodenhet av digital sikkerhet. Undersøkelsen kan utføres etter mal fra undersøkelse utført i utarbeidelse av denne strategien. Resultater fra kartleggingen bør presenteres til sektoren, og vil gi innspill til hvilke tiltak det bør legges mest vekt på i videre arbeid for økt digital sikkerhet.

2.5. Tiltak hovedmål 5 – Sjøfolk og personell har nødvendig digital sikkerhetskompetanse

2.5.1. Tiltak 13 Digital sikkerhetskompetanse

Nasjonal strategi for digital sikkerhetskompetanse[31] har som mål å styrke digital sikkerhetskompetanse i tråd med samfunnets behov. For maritim sektor betyr det at sektoren, gjennom Kystverket og Sjøfartsdirektoratet, tydeliggjør sine behov ovenfor utdannings-myndighetene, spesielt knyttet til sin egenart på digital sikkerhetskompetanse, for å bidra til at:

- digital sikkerhet legges inn i eksisterende relevante fag i maritim utdanning. Egenarten til maritim sektor og sårbarhetene i IT- og OT-systemer må vektlegges. Det må også vektlegges hvilken rolle den enkelte ansatte eller sjømann har for å forhindre, oppdage, rapportere og minimere konsekvensene av et digitalt angrep. Ansatte og sjøfolk må kunne sette seg inn i og forstå relevant og oppdatert risikobildet
- forelesere og andre kursholdere må få nødvendig kompetanse på digital sikkerhet
- det utarbeides standardkurs for digital sikkerhet for etterutdanning av sjøfolk.
- det utarbeides felles nasjonale læringsmål i samarbeid med maritime fagskoler og høyskoler.
- relevante problemstillinger knyttet til maritim digital sikkerhet tilbys i bachelor-, master- og doktorgradsoppgaver til utdanning av sjøfolk og utdanninger der IKT har en sentral plass

2.5.2. Tiltak 14 Sikkerhetskompetanse i internasjonalt regelverk

Kystverket og Sjøfartsdirektoratet skal fremme behovet for økt innhold av digital sikkerhetskompetanse i internasjonalt regelverk, i relevante fora. Kystverket og Sjøfartsdirektoratet må ta initiativ overfor IMO for å få utarbeidet felles internasjonale læringsmål gjennom internasjonale konvensjon om normer for opplæring, sertifikater og vakthold for sjøfolk (STCW). Sjøfartsdirektoratet må videre følge opp implementering gjennom Forskrift av 22. desember 2011 nr. 1523 om kvalifikasjoner og sertifikater for sjøfolk. Arbeidet må i tillegg til sjøfolk også omfatte personell på havnesiden og i rederi.

2.5.3. Tiltak 15 Opplæringstiltak

Rederier og virksomheter i maritim sektor sørger for å gi nødvendig opplæring i digital sikkerhet for sine ansatte. Øvelser på håndtering av digitale hendelser skal inngå som del av sikkerhetsstyringssystemet for et skip og i et rederi. Sjøfartsdirektoratet er ansvarlig for følge opp at digital sikkerhet og øvelser er tilstrekkelig håndtert gjennom sine tilsyn med sikkerhetsstyringssystemer og anerkjente klasseselskap for de fartøygrupper som er delegert.

2.5.4. Tiltak 16 Sikkerhetskompetanse i havner

Kystverket skal gjennom sitt tilsyn i havnene sørge for at digital sikkerhetskompetanse inngår i øvelser.

31 Regjeringen - https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

Vedlegg 2 - Rapporter

1. DNV GL - 2020-09-15 ROS analyse for maritim digital sikkerhet

2. SINTEF - Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet

Kai Hansen Trykkeri

Sjøfartsdirektoratet
Norwegian Maritime Authority

Postboks 2222, 5509 Haugesund
Smedasundet 50A, N-5528 Haugesund
Tel: +47 52 74 50 00
E-mail: post@sdir.no
www.sjofartsdir.no

Kystverket
Norwegian Coastal Administration

Postboks 1502, 6025 Ålesund

E-mail: post@kystverket.no
www.kystverket.no