SØFARTSSTYRELSEN

Strategi for Søfartssektorens Cyber- og Informationssikkerhed

2023 - 2025

Søfartens Cyber- og Informationssikkerhedsenhed

Indholdsfortegnelse

1 Søfartsstyrelsens strategiske cyber- og informationssikkerhedsmålsætning

Søfartsstyrelsens strategiske cyber- og informationssikkerhedsmålsætning er, at:

>>***sikkerheden om bord i danske skibe samt i danske farvande ikke kompromitteres som følge af cyberangreb***<<

Den Nationale Strategi for Cyber- og Informationssikkerhed (NCIS) 2022-2024 skal give et løft til den generelle cyber- og informationssikkerhed i Danmark. NCIS 2022-2024 skal sikre robuste og modstandsdygtige samfundsvigtige funktioner samt sikre et højt cyber- og informationssikkerhedsniveau i den understøttende kritiske IT-infrastruktur. Søfart er, som i den tidligere NCIS, udpeget som en sektor, der fortsat kan have en særlig betydning for cyber[1]- og informationssikkerheden[2] i Danmark.

Sektoransvaret for cyber- og informationssikkerhed i søfartssektoren ligger hos Søfartsstyrelsen og omfatter sikkerheden for sejlads i danske farvande samt sikkerheden for dansk-flagede skibe og deres besætning. Cybersikkerhed for skibe omfatter tjenester som trafikovervågning, advarsler og information til skibsfarten (AIS, NAVTEX), skibssystemer og software til skibets drift, herunder til fremdrivning og navigation.

Denne strategi vil supplere implementeringen af regulering på området med initiativer, som med udgangspunkt i sektorens sårbarheder og trusselsbilledet bidrager til øget robusthed over for cyberangreb og dermed øget cybersikkerhed i søfartssektoren.

Søfartssektorens cyber- og informationssikkerhedsudfordringer indgår som en integreret del af Søfartsstyrelsens arbejde med maritim sikkerhed i almindelighed, idet udfordringerne anskues på linje med de øvrige udfordringer og opgaver, der er forbundet med at opretholde sikkerheden om bord i danske skibe og sikkerheden forbundet med at sejle i de danske farvande.

Givet søfartssektorens globale karakter vil det fortsat være nødvendigt med et tæt samarbejde med nationale og internationale partnere, med hvem Danmark kan dele erfaringer og viden inden for cyber- og informationssikkerhedsområdet. Søfartsstyrelsen vil derfor fortsætte de etablerede samarbejder samt søge at udvide kredsen af pålidelige partnere, således at videndelingen og awareness på området bliver så omfattende som muligt, under hensyntagen til nationale sikkerhedsinteresser.

Søfartsstyrelsen vil som statslig myndighed og som systemejer af kritisk maritim infrastruktur samt samfundsvigtige funktioner fortsat efterleve en række obligatoriske minimumskrav til sikkerheden. Disse krav forventes at blive yderligere udbygget i strategiperioden og skal samlet medvirke til, at Søfartsstyrelsen er klædt på til at kunne agere hurtigt og effektivt i tilfælde af alvorlig cyberhændelser.

2 Cyber- og informationssikkerhedsregulering i søfartssektoren

For dansk søfart og for Søfartsstyrelsen er det vigtigt, at reguleringen af søfartssektoren i udgangspunktet foregår på internationalt niveau, og at der er ens rammevilkår for alle.

Det er en grundlæggende dansk prioritet, at dansk søfartsregulering er i overensstemmelse med internationale regler, og at der er fælles og ensrettede globale regler for cybersikkerhed for alle rederier og alle skibe. Dette skal medvirke til et fælles højt globalt cyber- og informationssikkerhedsniveau, da det er den eneste måde at sikre, at skibe, der sejler igennem danske farvande eller anløber danske havne, lever op til en rimelig standard på cyber- og

[1] Cybersikkerhed dækker over beskyttelsen imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.

[2] Informationssikkerhed dækker over de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

informationssikkerhedsområdet. Implementering af særlige europæiske regler på søfartsområdet skal derfor ske i samklang med de globale rammer.

Søfartsstyrelsen vil derfor arbejde for, at søfartssektorens rammer for cyber- og informationssikkerhed bliver globale og forhandles i regi af FN's Søfartsorganisation (IMO), og at der fortsat etableres relevante samarbejder både internationalt og i EU-landene, således at danske rederier kan anvende samme globale cyber- og informationssikkerhedsstandarder til at forebygge cyberangreb, uanset hvor i verden de opererer.

Med implementeringen af EU´s nye Net- og Informationssikkerhedsdirektiv (NIS-2) er der mulighed for, at danske rederier, over en vis størrelse, kan blive udpeget til at være "essentielle enheder". NIS-2 direktivet skærper derudover cybersikkerhedskravene til "essentielle enheder" ift. det gældende NIS direktiv. De skærpede krav inkluderer blandt andet risikohåndteringsforanstaltninger i forbindelse med cybersikkerhed, herunder krav til fx: Politikker for informationssikkerhed og risikoanalyse, procedurer for hændelseshåndtering, driftssikring, krisestyring, forsyningskædesikkerhed, leverandørstyring, IT-sikkerhed i forbindelse med udvikling og vedligeholdelse, håndtering og offentliggørelse af sårbarheder, evaluering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici samt brug af kryptografi og kryptering. NIS-2 direktivet indfører derudover udvidede rapporteringsforpligtelser samt et krav om brug af europæiske cybersikkerhedscertificeringsordninger.

De nye skærpede krav medfører ligeledes, at ledelsen i de udpegede "essentielle enheder" skal være bekendt med kravene i NIS-2 direktivet, herunder hele risikostyringsindsatsen. Ledelsen får således et direkte ansvar for, at cyberrisici bliver identificeret og håndteret, samt at kravene i NIS-2 direktivet overholdes.

Søfartsstyrelsen udstedte i 2019 en bekendtgørelse om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads[3], der blandt andet implementerer det gældende NIS-direktiv i Danmark inden for søfarten. Det følger af bekendtgørelsen, at der fastsættes særlige krav til rederier og skibe samt til visse udbydere af maritime tjenester. Det betyder, at danske rederier og skibe, som anvender net- og informationssystemer, skal inkludere cybersikkerhed i deres risikostyringstiltag, med henblik på at skibene kan sejle sikkert. Derudover skal de underrette Søfartsstyrelsen og CFCS om hændelser, som er omfattet af bekendtgørelsen, og som har konsekvenser for skibenes sikkerhed og sejllads.

Større lastskibe og passagerskibe er omfattet af den internationale kode for sikker skibsdrift (ISM-koden) samt den internationale kode for Ship and Port Facility Security (ISPS-koden) og skal efter disse regler allerede tage særlig hensyn til maritim sikkerhed, herunder cyber- og informationssikkerhed[4]. Andre skibe kan også have sårbare systemer, som fx elektroniske søkort og kommunikationssystemer, og skal derfor også leve op til passende sikkerhedskrav. Bekendtgørelsen indeholder derfor en hjemmel til, at Søfartsstyrelsen kan fastsætte nærmere krav til disse skibe ved behov.

Herudover anvender skibe i dansk farvand en række digitale maritime tjenester, som forsyner skibene med data, eller som overvåger skibenes færden. Det omfatter blandt andet:

- Vessel traffic service (VTS), der overvåger skibstrafikken i særlige danske farvandsafsnit.

- Sejladsinformation (navigationsadvarsler) til skibsfarten i danske farvande.

- Informationsudvekslingssystemer som det automatiske identifikations system (AIS) eller tilsvarende.

[3] BEK nr 46 af 15/01/2019

[4] IMO resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems

2.1.1 Strategiske indsatser og initiativer;

Søfartsstyrelsen vil:

- arbejde for, at reguleringen af søfartssektoren i udgangspunktet foregår på internationalt niveau, og at der altid er ens rammevilkår for alle.

- arbejde for, at søfartssektorens rammer for cyber- og informationssikkerhed bliver globale og implementeres i samklang med rammerne, som er vedtaget i FN's Søfartsorganisation (IMO), og at der fortsat etableres relevante samarbejder både internationalt og i EU-landene, så danske rederier kan anvende samme globale cyber- og informationssikkerhedstandarder til at forebygge cyberangreb.

- sikre implementering af EU´s Net- og Informationssikkerhedsdirektiv (NIS-2) for søfartssektoren i overensstemmelse med sektoransvarsprincippet, i det omfang det kan berøre sikkerheden til søs. Det betyder blandt andet, at kravene og sanktioneringen af cybersikkerhed udvides for at harmonisere og strømline sikkerhedsniveauet på tværs af EU´s medlemslande.

- gennemføre revidering af bekendtgørelse nr. 46 om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads, på baggrund af den løbende kortlægning af samfundskritiske maritime funktioner samt ny regulering.

- i relation til IMO resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, fortsat sørge for at cyber- og informationssikkerhed indgår som en integreret del af de syn, der gennemføres af Søfartsstyrelsen egne skibsinspektører, eller der gennemføres af de klassifikationsselskaber, der er autoriseret af Søfartsstyrelsen til at varetage godkendelsesopgaver og certifikatudstedelser på danske skibe.

- fastlægge, baseret på en løbende risiko- og sårbarhedsvurdering, hvilke skibe og maritime tjenester og systemer, der bør omfattes af særlige cyber- og informationssikkerhedskrav, herunder fx fjernstyrede skibe, autonome skibe eller skibe med høj grad af automatiske skibssystemer.

3 Styrket sikkerhed omkring samfundsvigtige maritime funktioner

3.1 Cyber- og informationssikkerhedstruslen mod søfartssektoren

Det vurderes ikke, at der er en særlig og specifik cyber- og informationssikkerhedstrussel, der er målrettet søfartssektoren i almindelighed og i særdeleshed ikke en cybertrussel, der er direkte målrettet danskflagede skibe eller sejladssikkerheden gennem danske farvande.

Søfartssektoren adskiller sig ikke væsentligt fra andre sektorer på cyber- og informationsområdet. Center for Cybersikkerheds (CFCS) generelle vurderinger af trusselsniveauer[5] for Danmark – i forhold til cyberspionage og cyberkriminalitet, cyberaktivisme, destruktive cyberangreb samt cyberterror – vil derfor som udgangspunkt ligeledes være gældende for søfartssektoren.

Søfartsstyrelsen forsøger løbende i samarbejde med blandt andre CFCS, søfartens aktører samt andre søfartsfaglige kilder at afdække de trusler og sårbarheder, som søfartssektoren står overfor, som følge af en stigende anvendelse af net- og informationstjenester, herunder automatiserede skibssystemer og fjernstyringsteknologier m.m.

[5] https://www.cfcs.dk/

I takt med den stigende anvendelse af IT- og OT-systemer om bord i skibene, er der således opstået en betydelig afhængighed af disse teknologier i varetagelsen af kerneopgaver i søfartssektoren. Dermed er der også opstået et større krav til modstandsdygtighed (resiliens) over for aktuelle cybertrusler, der kan påvirke disse systemer og dermed også påvirke skibs- og/eller sejladssikkerheden.

Det er Søfartsstyrelsens vurdering, at:

- Aktørerne i søfartssektoren arbejder med cybersikkerhed på flere forskellige niveauer.

- At modenheden ift. cybersikkerhed varierer fra næsten ingen beredskabsparathed eller fra kun basal cyber-hygiejne[6] og malware beskyttelse af fx de administrative systemer, til en stor beredskabsparathed med komplekse og optimerede IT-sikkerhedsledelsessystemer med en høj grad af cyberhygiejne og beskyttelse mod aktuelle cybertrusler.

- De offentlige myndigheder primært arbejder ud fra ISO 27001 standarden, hvorimod mange af de private aktører i langt højere grad arbejder mere bredt med cybersikkerhed, idet de både søger inspiration i anerkendte standarder som fx ISO 27001[7], men samtidig henter inspiration fra rammeværk som fx National Institute of Standards and Technology (NIST)[8] og Center for Internet Security (Critical Security Controls (CIS) Controls)[9] eller fra specifikke teknologier og sikkerhedsrelaterede discipliner som fx fysisk sikkerhed.

- En af de største trusler mod et skibs IT/OT-sikkerhed primært stammer fra dårligt kodet/gammelt og ikke opdateret software samt fra manglende styring/kontrol med de leverandører, der måtte komme om bord for at installere nye systemer, eller som kommer om bord for at opdatere de eksisterende systemer.

På baggrund af gældende vejledninger fra CFCS anbefaler Søfartsstyrelsen:

- At man som aktør i søfartssektoren løbende søger aktuel viden om cybertrusler- og sikkerhed i de cyber- og informationssikkerhedsvejledninger og publikationer, der blandt andet udgives af maritime brancheorganisationer, klassifikationsselskaber m.v., men også udgives af CFCS og af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

- At der er stor fokus på leverandørstyring om bord i et skib. Det er nødvendigt, at man som IT-sikkerhedsansvarlig om bord i et skib har fuld kontrol med, hvem der kommer om bord og installerer ny hardware og software og/eller kommer om bord og laver opdateringer på de enkelte systemer. Som skibets IT-sikkerhedsansvarlig skal man have fuldstændig styr på, hvad den nøjagtige ansvarsfordeling er mellem skibet og leverandøren; hvad leverandøren gør for at beskytte mod uønsket adgang; hvad der gøres for at sikre fortrolighed, integritet og tilgængelighed; samt hvad der gøres for at dokumentere leverandørens egen sikkerhed.

[6] Cyberhygiejne har til formål at opretholde hardwarens og softwarens grundlæggende funktionstilstand og sikkerhed og sikre, at de er beskyttet mod trusler som fx malware. Cyberhygiejne refererer til de trin, som brugere af computere og andre enheder kan følge for at forbedre deres generelle cybersikkerhed og dermed opretholde systemets sundhed. Cyberhygiejne betyder, at man tillægger sig en sikkerhedsfokuseret tankegang samt vaner, der hjælper enkeltpersoner og organisationer med at afbøde potentielle brud på cybersikkerheden.

[7] https://www.iso.org/

[8] https://www.nist.gov/

[9] https://www.cisecurity.org/

- Et skibs IT-sikkerhedsansvarlige skal altid sikre sig, at den software, der anvendes til fx skibskritiske systemer, er gennemtestet, inden de tages i brug, og at der altid er en beredskabsplan, der sikrer skibets fortsatte drift og sikkerhed, i det tilfælde at det skibskritiske system skulle fejle som følge af en IT-hændelse.

3.2 Sikring af et robust cyber- og informationssikkerhedsberedskab i søfartssektoren

Uanset hvor godt man som organisation sikrer sig, vil der kunne ske en IT-sikkerhedshændelse. Det kan fx være et utilsigtet nedbrud af et administrativt system, et brud på persondataloven eller en fuldstændig lammelse af et eller flere kritiske forretningssystemer pga. et udefrakommende cyberangreb. Uanset hvordan en IT-sikkerhedshændelse udmønter sig, er det vigtigt at have systemer og processer klar til at sikre det nødvendige overblik samt at have etableret og afprøvet et passende beredskab, der kan håndtere de IT-sikkerhedshændelser, man risikerer at blive ramt af.

Søfartssektoren har altid prioriteret sikkerhed og er derfor nået langt i arbejdet med den generelle sikkerhed i forbindelse med søfart. Fokus på medarbejder-, transport-, gods-, og ikke mindst skibs- og sejladssikkerhed har ført til, at der i dag er en god sikkerhedskultur og dermed et godt sikkerhedsberedskab i søfartssektoren. Denne sikkerhedskultur kan dog gennem fortsat awareness og uddannelse samt med en endnu stærkere ledelsesforankring i forhold til cyber- og informationssikkerhed fortsat udbygges, således at mennesker, teknologier og processer involveres i langt højere grad i forhold til brud på cyber- og informationssikkerheden.

En stærk ledelsesforankring i forhold til cyber- og informationssikkerhed er en synlig indikator, både eksternt og internt, for en organisations modenhed på området. En tydelig ledelsesopbakning fremmer og understøtter en positiv sikkerhedskultur, der igen understøtter et effektivt sikkerhedsberedskab, som igen fremmer sikkerhed på alle niveauer og alle områder i organisationen.

3.2.1 Strategiske indsatser og initiativer

For at sikre et robust cyber- og informationssikkerhedsberedskab i søfartssektoren vil Søfartsstyrelsen arbejde for, at cyber- og informationssikkerhedsudfordringer indgår som en integreret del af søfartssektorens arbejde med maritim sikkerhed i almindelighed. Gennem løbende uddannelse og awareness træning skal de søfarende opbygge en nødvendig og basal viden om cyberhygiejne, således at de altid er i stand til at reagere korrekt, når de bliver stillet over for It-sikkerhedshændelser, der kan have afgørende og negativ indvirkning på deres egen og skibets sikkerhed.

Søfartsstyrelsen mener, at det er vigtigt, at cyber- og informationssikkerhedsudfordringerne anskues på linje med de øvrige udfordringer og opgaver, der er forbundet med at opretholde sikkerheden om bord i et skib og sikkerheden forbundet med at sejle. Søfartsstyrelsen vil derfor fokusere på, at aktører i søfartssektoren, i forbindelse med deres generelle sikkerheds- og beredskabshåndtering, er i stand til at:

- Identificere alle sine IT-aktiver/systemer, herunder særligt de IT-aktiver/systemer, der kan være forretnings- og skibskritiske

- Gennemføre en risiko- og sårbarhedsanalyse, der giver et fundament for at opstille prioriterede forslag til nye eller supplerende risiko- og sårbarhedsreducerede tiltag

- Etablere de nødvendige forsvarsværker mod aktuelle cybertrusler, herunder adgangsstyring, malware beskyttelse, netværkssegmentering m.m.

- Etablere procedurer og anvende værktøjer, der muliggør en tidlig detektering af IT-sikkerhedshændelser, herunder cyberangreb

- Etablere beredskabsplaner og procedurer, der muliggør det nødvendige modsvar til IT-sikkerhedshændelser, herunder sikre at der fx altid er redundans på de forretnings- og skibskritiske aktiver/systemer

- Etablere backupprocedurer og anvende værktøjer, der muliggør reetablering af de enkelte systemer til normal driftsstatus.

Siden januar 2021 har det været lovpligtigt at inkludere cyberrisikostyring i ISM[10] skibes sikkerhedsledelsessystem[11] (SMS). Søfartsstyrelsen vil derfor i forbindelse med de almindelige skibssyn sørge for at fokusere på at de grundlæggende procedurer for cyber- og informationssikkerhed er inkluderet i skibets sikkerhedsledelsessystem.

Skibstilsyn gennemført af eller på vegne af Søfartsstyrelsen vil blandt andet kunne inkludere:

- Verificering af eksistensen af cyber- og informationssikkerhedspolitikker m.m.

- Identifikation af cybersikkerhedsroller og -ansvar om bord, herunder verificering af eksistensen af udviklede procedurer for cyberrisikostyring.

- Kontrol af den grundlæggende cyberhygiejne. Dette kan fx omfatte kontrol af at USB-porte på systemkritiske computere og på ECDIS[12] er låst/blokeret og om håndtering af adgangskoder sker på en betryggende vis.

- Verificering af, at softwareopdateringer og patching af fx ECDIS såvel som enhver anden skibskritisk software, udføres struktureret og gennem nedskrevne procedurer og aftaler.

- Verificering af grundlæggende netværksadskillelse ved at se på design og kontrol af besætningens internetadgang og kontrollen af administratorprofiler, brugerprofiler og adgangskoder for alle netværksbrugere.

- Kontrol af, at fysisk sikkerhed til nøglesystemer og netværkskomponenter eksisterer og vedligeholdes.

- Kontrol af, at der gennemføres basal awareness træning/øvelser i cybersikkerhed om bord;

    - kender og forstår skibets nøglebesætning til de enkelte cybersikkerhedsprocedurer?
    - er besætningen i stand til at agere korrekt ved en It-sikkerhedshændelse?
    - har skibet de nødvendige cyberberedskabsplaner på plads og testes disse regelmæssigt?
    - har skibet opdaterede kontaktoplysninger til fx teknisk support fra deres egen it-afdeling eller eksterne it-leverandører i land.

3.3 Søfartsstyrelsens systemansvar for samfundskritiske maritime funktioner

Søfartsstyrelsen forholder sig løbende til sin systemforpligtigelse ift. samfundskritisk maritim IT-infrastruktur og funktioner. Søfartsstyrelsen tager løbende stilling til, om Søfartsstyrelsen har de nødvendige beføjelser, og om Søfartsstyrelsen evt. har behov for ny lovhjemmel til at sikre det rette niveau for cyber- og informationssikkerheden for den samfundskritiske maritime IT-infrastruktur og funktioner, som Søfartsstyrelsen i overensstemmelse med sektorprincippet er ansvarlig for.

[10] ISM-koden (International Safety Management Code) er IMOs standard for sikker styring og drift af skibe til søs.

[11] Sikkerhedsledelsessystemet (SMS) er et organiseret system planlagt og implementeret af rederierne for at sikre sikkerheden for skibet og havmiljøet.

[12] ECDIS er en forkortelse for Electronic Chart Display and Information System. ECDIS-systemer viser information fra elektroniske søkort (ENCs) og integrerer information fra fx ; GPS-modtagere, radar, log- og AIS-systemer. ECDIS kan også præsenterer navigations-relateret information, såsom sejladsruter m.m.

I danske farvande kan der til tider opleves udfald og forstyrrelser på GNSS[13] signalerne. Om forstyrrelserne skyldes en forsætlig handling af en eller flere aktører eller om forstyrrelserne fx "bare" skyldes meteorologiske årsager, er det forstyrrelser, der kan have en direkte indvirkning på sejlads- og skibssikkerheden og forstyrrelser som aktører i søfartssektoren altid skal være parate til at håndterer. Om end forstyrrelser af GNSS signaler ligger i periferien af cyber- og informationssikkerhedsområdet, er det hændelser som giver anledning til en øget bekymring og et område der således er under konstant bevågenhed.

3.3.1 Strategiske indsatser og initiativer

Søfartsstyrelsen vil:

- Fortsat sikre, at Søfartsstyrelsens IT-sikkerhedsledelsessystem (ISMS) er i fuld overensstemmelse med ISO 27001 standarden, samt sikre at Søfartsstyrelsen til stadighed opfylder nuværende og fremtidige tekniske minimumskrav til statslige myndigheders IT-portefølje og infrastruktur. For at sikre fuld overensstemmelse med ISO 27001 standarden og af hensyn til drifts- og sikkerhedsmæssige forhold, bliver alt, hvad der sker på Søfartsstyrelsens kritiske IT-infrastruktur, løbende registreret. Registreringen sker på baggrund af ISMS regelsæt for logning, der dækker både egen IT-infrastruktur og IT-infrastrukturen hos Søfartsstyrelsens IT-driftsleverandør.

- I takt med den stadigt stigende anvendelse af mere og mere komplekse IT- og OT-systemer om bord i skibene fortsat sørge for, at Søfartsstyrelsens skibsinspektører modtager den nødvendige opkvalificering og kompetenceudvikling ift. gennemførelse af cybertilsyn om bord i danskflagede skibe.

- I forbindelse med implementeringen af maritim cyberregulering sikre, at udpegede operatører af essentielle maritime tjenester/funktioner og herunder udpeget kritisk maritim IT-infrastruktur, løbende bliver kortlagt for søfartssektoren. Kortlægningen vedligeholdes løbende for at sikre, at det nødvendige overblik fastholdes, således at det fx kan anvendes til prioritering og fokusering af cybersikkerhedsmæssige tiltag og i beredskabssituationer. Omfanget af denne kortlægning vurderes at blive udvidet i relation til implementeringen af NIS-2 direktivet, hvor udpegning af nye "essentielle enheder" og deraf ny kritisk maritim infrastruktur og funktioner kan blive en realitet.

- Sikre at der fortsat vil være krav om passende foranstaltninger for at forebygge og minimere konsekvensen af en hændelse, der kan have en negativ indvirkning på sikkerheden i de net- og informationssystemer, som anvendes til levering af de essentielle maritime tjenester. Er man udpeget som operatør af en maritim tjeneste, vil der fortsat være krav om certificering efter en internationalt anerkendt standard for styring af sikkerheden i net- og informationssystemer, eksempelvis ISO 27001 eller tilsvarende.

- Sikre at skibsfarten i danske farvande alarmeres, såfremt der opdages udfald og forstyrrelser på GNSS signalerne, og såfremt det vurderes at disse udfald og forstyrrelser vil have negativ indvirkning på skibs- og sejladssikkerheden.

- Løbende vurdere behovet for klassificerede kommunikationskanaler, for at sikre at der ikke deles beskyttelsesværdige oplysninger på usikker vis, fx mellem myndigheder eller mellem maritime interessenter og samarbejdspartnere. Søfartsstyrelsen deltager således aktivt i både nationale som i internationale fora og arbejdsgrupper, hvor behovet for klassificeret kommunikation drøftes.

- Blive tilsluttet CFCS sensornetværk, hvor det er muligt og giver mening samt i tæt samarbejde med Søfartsstyrelsens IT-driftsleverandør. Søfartsstyrelsen anbefaler som udgangspunkt, at alle aktører i søfartssektoren vurderer behovet for tilslutning til CFCS' sensornetværk. Udpegede operatører af maritime tjenester bør dog altid ud fra en konkret risikovurdering og i dialog med CFCS, tage aktivt stilling til behovet for tilslutning til sensornetværket, således at ved begrundet mistanke om, at en operatør er ramt af en

[13] GNSS; Global Navigation Satellite System, er en generel betegnelse for et globalt dækkende system af satellitter beregnet til navigation.

sikkerhedshændelse, vil CFCS kunne reagere og sende et varsel til den pågældende operatør af maritime tjenester.

- Vurdere behovet for involvering af CFCS i udfærdigelsen af cybersikkerhedskrav i forbindelse med indkøb og udbud af samfundskritiske IT-systemer, der understøtter samfundsvigtige funktioner.

- Fortsat vurdere behovet for indberetningspligt, sikkerhedsgodkendelser og beredskabsaftaler for de udpegede samfundskritiske IT-systemer samt for de udpegede operatører af maritime tjenester og "essentielle enheder" jf. NIS-2 direktivet.

- Sikre, at relevante anbefalinger og vejledninger, der udsendes fra CFCS, så vidt det er muligt følges, herunder fx CFCS' oversigt over cyber- og informationssikkerhedstiltag, der kan bruges i arbejdet med at sikre, at fundamentet for et solidt cyberforsvar er på plads ift. kritisk infrastruktur m.m.

- I regi af CFCS DCIS forum, aktivt deltage i planlægning og gennemførelse af tværministerielle cyber- og informationssikkerhedsøvelser, således at det generelle danske cyber- og informationssikkerhedsniveau for kritisk infrastruktur og funktioner højnes.

4 Søfartens Cyber- og Informationssikkerhedsenhed (Søfartens DCIS)

Søfartens DCIS blev etableret i forbindelse med den nationale cyber- og informationssikkerhedsstrategi af maj 2018.

Med NCIS 2022-2024 fortsættes de sektorvise DCIS aktiviteter. Søfartens DCIS vil således fortsat fungere som primær udvekslingspunkt mellem søfartssektorens aktører og CFCS. Opgaver i denne forbindelse vil være at formidle, efterspørge, skabe og validere IT-sikkerhedsrelateret information mellem parterne.

4.1.1 Strategiske indsatser og initiativer;

Søfartsstyrelsen og herunder Søfartens DCIS vil:

- Agere udvekslingspunkt mellem søfartssektorens aktører og CFCS samt levere en operationel kapacitet i dagtimerne til at koordinere sikkerhedshændelser for den eller de pågældende samfundsvigtige maritime funktioner i samspil med andre områder og det nationale IT-beredskab.

- Levere søfartsfaglig viden til "SMV" cybersikkerhedsenheden, der etableres i regi af regeringens NCIS, og som får til opgave at gennemføre en samlet og koordineret indsats for at styrke videndeling og cybersikkerhedsniveauet i SMV'erne. Enheden skal blandt andet være med til at facilitere og igangsætte nye offentlig-private initiativer, der skal bidrage til en styrkelse af SMV'ernes cybersikkerhed.

- Stille søfartsfaglig viden til rådighed for CFCS i forbindelse med udarbejdelse af fx sårbarheds- og trusselsvurderinger.

- Stille maritim cyber- og informationssikkerhedsviden til rådighed for maritime uddannelsesinstitutioner, således at der kommer et øget fokus på cyberhygiejne i søfartssektoren.

- Agere intern ekspertfunktion vedr. cyber- og informationssikkerhed i Søfartsstyrelsen herunder assistere Søfartsstyrelsens skibsinspektører i forbindelse med gennemførelse af cyber relaterede syn om bord i skibe.

- Proaktivt levere input til og fra, samt søge indflydelse i relevante nationale og internationale arbejds- og ekspertgrupper ift. maritim cyber- og informationssikkerhed, herunder:

- De nationale DCIS ERFA fora og herunder arbejdsgrupper i relation til NCIS 2022 – 2024
- Den Internationale Søfartsorganisation (IMO)
- European Maritime Safety Agency (EMSA)
- European Network and Information Security Agency (ENISA)
- Videndelingsfora vedr. trusler, fx DCIS MISP platform og diverse ERFA fora vedr. teknisk cybersikkerhed
- Relevante ekspert- og arbejdsgrupper til International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA)
- NATO´s arbejde med at styrke beskyttelsen af nationale netværk og infrastrukturer (NATO Cyber Defence Pledge).

5 Samarbejde og videndeling

Søfartsstyrelsen ønsker at udbygge og udvikle det tætte videndelingssamarbejde, der er etableret i den forudgående strategiperiode, med relevante partnere nationalt som internationalt. Denne erfaringsudveksling og vidensdeling på tværs af myndigheder og ikke mindst på tværs af aktører i søfartssektoren er afgørende for at kunne identificere og konkretisere nye områder, hvor der i fællesskab kan iværksættes initiativer, der er med til at styrke søfartssektorens cyber- og informationssikkerhed. En proaktiv og tillidsbaseret videndeling kan være medvirkende til en større resiliens over for de cyberangreb og utilsigtede IT-hændelser, der kan ramme søfartssektoren i fremtiden.

Et vigtigt maritimt cyberpartnerskab er Det Internationale Partnerskab for Maritim Cybersikkerhed (IPMC), der blev etableret i 2019 under den første udgave af den årlige internationale begivenhed om maritim cybersikkerhed i Haag, Nederlandene. Partnerskabet bestod i første omgang af repræsentanter fra Danmark, Holland og USA. Siden da er bevidstheden om et globalt samarbejde og videndeling om maritim cybersikkerheds betydning vokset, og flere ligesindede nationer er involveret i dag, herunder Australien, Singapore og Storbritannien.

IPMC sigter mod at samarbejde og dele viden og ekspertise inden for maritim cybersikkerhed. Disse aktiviteter omfatter blandt andet følgende områder:

- Samarbejde om tilrettelæggelsen af en årlig Maritime Transport System (MTS) Cybersikkerhedskonference, ledet og afholdt af et medlem af partnerskabet med fokus på videndeling og udvikling af samarbejdet.

- Deling af information relateret til maritime trusler i almindelighed.

- Deling af specifik ekspertise og ”best practice” om:

    - Ledelse og regulering
    - Håndtering af aktuelle cybersikkerhedstrusler
    - Metoder og værktøjer til informationsudveksling
    - Cyberøvelser
    - Maritime cybertilsyn

- Udveksling af erfaringer fra utilsigtede IT-hændelser.

- Gennemførelse af fælles indsatser, der kan støtte gensidige interesser.

- Planlægning og gennemførelse af fælles cyberøvelser.

Vidensdeling om cyber- og informationssikkerhed er ligeledes et spørgsmål om beredskabsplanlægning og varsling, herunder om at få den relevante viden hurtigere frem til alle. Når en myndighed fx erkender, at den er udsat for et phishing-angreb, så skal denne viden kunne deles og bringes videre hurtigst muligt, så også andre myndigheder og aktører i søfartssektoren kan bruge denne viden med det samme.

5.1.1 Strategiske indsatser og initiativer

Søfartsstyrelsen vil:

- Deltage i samt udvikle og udbygge de nationale og internationale partnerskaber for maritim cyber- og informationssikkerhed

- I regi af IMO og i samarbejde med partnerne i IMPC sætte fornyet fokus på maritim cyber- og informationssikkerhed med henblik på at fremme globale rammer.

- I regi af IMPC udveksle best practice i forhold til gennemførelse af cyber tilsyn om bord skibe.

- Formidle, efterspørge, skabe og validere IT-sikkerhedsrelateret information mellem søfartssektorens aktører.

- Fortsætte og om muligt udvikle den nuværende beredskabs- og varslingskommunikation til aktører i søfartssektoren.