SØFARTSSTYRELSEN

Strategi for Søfartssektorens Cyber- og Informationssikkerhed

2019 - 2022

Aske Hegelund Myrfeld (EM-DEP)

Indholdsfortegnelse

1 Indledning 2

2 Afgrænsning 2

3 Trusler, risici og sårbarheder for søfartssektoren 3

3.1 CFCS trusselsvurdering 3

3.2 Risiko- og Sårbarhedsanalyse af søfartssektoren 3

3.2.1 Generelle observationer 4

3.2.2 Identificerede risici 4

3.2.3 Anbefalinger 4

4 Styrket indsats for at styrke cyber- og informationssikkerheden i søfartssektoren 5

4.1.1 Søfartens cyber- og informationssikkerhedsenhed 5

4.1.2 Implementering af EU- og International lovgivning 5

4.1.3 Brugervenlige anbefalinger til søfartssektorens aktører 6

4.1.4 It-sikkerhedskultur og awareness 7

4.1.5 Fokusering på standardiserede processer i relation til cyber- og Informationssikkerhedsledelse 7

4.1.6 Sikre et vedvarende og robust cyber- og informationssikkerhedsberedskab i søfartssektoren 8

4.1.7 Udvekslingspunkt mellem søfartssektorens aktører og CFCS 8

4.1.8 Indstationering af søfartsmedarbejder hos CFCS 9

4.2 Det maritime cyber- og informationssikkerhedsforum 9

4.2.1 Øget awareness-niveau gennem samarbejde og vidensdeling i søfartssektoren 9

4.2.2 Fælles beredskabs- og varslingsplan til håndtering af It-sikkerhedshændelser 10

4.2.3 Planlægning og gennemførelse af fælles cyber-og informationssikkerhedsøvelser 10

5 Afslutning 10

5.1 Tidshorisont 11

1 Indledning

Regeringen vil med forsvarsforliget 2018-2023 bl.a. styrke beskyttelsen af Danmark mod cybertrusler markant, og har på baggrund heraf fastlagt den nationale strategi for cyber- og informationssikkerhed. Med strategien igangsætter regeringen en række initiativer, der skal løfte de samfundskritiske sektorers arbejde med cyber- og informationssikkerhed. Søfart er udpeget som en af disse sektorer, der har særlig betydning for cyber- og informationssikkerheden i Danmark. Derfor skal det sikres, at der ligger en klar plan for arbejdet med cyber- og informationssikkerhed i sektoren, og det er formålet med denne strategi.

Cyber- og informationssikkerheden i søfartssektoren 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.

Søfartsstyrelsens strategiske målsætning med delstrategien for cyber- og informationssikkerhed er *at sikkerheden om bord i danske skibe samt i danske farvande ikke kompromitteres som følge af cyberangreb.* Søfartssektorens cyber- og informationssikkerhedsudfordringer vil indgå som en integreret del af Søfartsstyrelsens arbejde med maritim sikkerhed, 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.

Det bemærkes, at delstrategien vil supplere implementeringen af NIS-direktivet med konkrete initiativer, som med udgangspunkt i sektorens sårbarheder og trusselsbilledet for søfart bidrager til øget robusthed over for cyberangreb og dermed øget cybersikkerhed i søfartssektoren. Givet søfartssektorens globale karakter kan det ligeledes være nødvendigt at etablere kontakt til pålidelige internationale samarbejdspartnere, med hvem Danmark kan dele erfaringer og viden inden for cyber- og informationssikkerhedsområdet.

2 Afgrænsning

I regeringens nationale strategi for cyber- og informationssikkerhed lægges der vægt på, at fordelingen af ansvaret for arbejdet med cyber- og informationssikkerhed i Danmark bygger på sektoransvarsprincippet: Den myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret under cyber- og informationssikkerhedshændelser. Ansvaret for cyber- og informationssikkerhed i søfartssektoren ligger således hos Søfartsstyrelsen og omfatter sejladssikkerheden i danske farvande samt sikkerheden om bord i danske skibe, som omfatter skibssystemer og software til skibets drift, herunder til fremdrivning og navigation, jf. lov om sikkerhed til søs. Cyber- og informationssikkerhed for søfartssektoren omfatter derudover tjenester som trafikovervågning, advarsler og information til skibsfarten samt andre systemer med sammenhæng til skibets sikre sejlads.

Begrebet ”Informationssikkerhed” dækker i denne strategi over de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

Når der i denne strategi tales om ”cybersikkerhed” så omfatter dette beskyttelse 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.

3 Trusler, risici og sårbarheder for søfartssektoren

For at kunne styrke cyber- og informationssikkerheden i sektoren er det nødvendigt at beskrive det aktuelle trusselsbillede, som sektoren står overfor. Det er endvidere nødvendigt at identificere og beskrive sektorens sårbarheder over for truslerne.

Nedenfor beskrives derfor først den konkrete trusselsvurdering for søfartssektoren med afsæt i de gældende trusselsvurderinger[1] fra Center fra Cybersikkerhed (CFCS). Trusselsvurderingerne giver et overblik over de trusler, som søfartssektoren særligt står over for, og hvor det skal overvejes, om der skal sættes ind med forebyggelse. Dette ud fra en vurdering af, hvor stor en sårbarhed søfartssektoren har over for de konkrete trusler. Herefter præsenteres konklusionerne fra den risiko- og sårbarhedsanalyse, som Søfartsstyrelsen har fået gennemført af en ekstern konsulentvirksomhed i november 2018. Analysen giver et overblik over de risici og sårbarheder, som søfartssektoren står overfor, som følge af det aktuelle trusselsbillede og som følge af den stigende anvendelse af automatiserede skibssystemer samt anvendelse af net- og informationstjenester.

3.1 CFCS trusselsvurdering

CFCS vurderer i sin trusselsvurdering, at:

- cybertruslen mod den maritime sektor primært er rettet mod kommercielle virksomheder og pt. ikke udgør en direkte trussel mod de maritime operationer,

- truslen fra destruktive cyberangreb mod søfartssektoren er lav. Maritime kommunikationslinjer, herunder skibe og havne, kan dog være mål for destruktive cyberangreb i tilfælde af konflikter,

- truslen fra cyberspionage mod søfartssektoren er meget høj, og det vurderes, at stater anvender systematisk cyberspionage som middel til at opnå industrielle og forretningsmæssige fordele samt til at fremme politiske og økonomiske interesser,

- truslen fra cyberkriminalitet mod søfartssektoren er meget høj. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra myndigheder, virksomheder og borgere (ransomware). Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet, og statsstøttede hackere står sandsynligvis også bag cyberkriminalitet,

- truslen fra cyberaktivisme mod søfartssektoren vurderes at være lav. Shipping industrien er ikke i søgelyset hos cyberaktivister og betragtes ikke som et mål af høj værdi,

- truslen fra cyberterror mod søfartssektoren vurderes at være lav. Terroristgrupper har kun vist begrænset interesse for søfartssektoren. Derudover har terroristgrupperne kun begrænsede evner og ressourcer til at udføre alvorlige cyberangreb mod søfartssektoren.

3.2 Risiko- og Sårbarhedsanalyse af søfartssektoren

Formålet med analysen er at afdække de væsentlige sårbarheder, som søfartssektoren står overfor, som følge af stigende anvendelse af automatiserede skibssystemer samt anvendelse af net- og informationstjenester. Analysen har blandt andet identificeret operatører af maritime tjenester, herunder deres tjenester, funktioner og systemer, som er særligt kritiske for søfartssektoren. Hertil har analysen identificeret en række områder, hvor der bør ydes en særlig målrettet indsats for at sikre cyber- og informationssikkerheden. Risiko- og sårbarhedsanalysen er udarbejdet i tæt dialog med aktørerne i søfartssektoren, herunder Danske Rederier og andre statslige myndigheder.

[1] Cybertruslen mod Danmark" – Maj 2018 og "The Cyber threat against the maritime sector" – Marts 2017)

3.2.1 Generelle observationer

I takt med en stigende anvendelse af IT på skibe, er der opstået en betydelig afhængighed af IT i varetagelsen af kerneopgaver i søfartssektoren. Det fremgår af analysen, at de adspurgte aktører arbejder med cybersikkerhed på forskellige niveauer. Nogle aktører, herunder de offentlige myndigheder, arbejder som udgangspunkt med ISO 27001 standarden ift. cybersikkerhed. De private aktører arbejder mere bredt med cybersikkerhed, da de både søger inspiration i anerkendte standarder som fx ISO 27001 men de henter samtidig inspiration fra specifikke teknologier og andre sikkerhedsrelaterede discipliner som fx fysisk sikkerhed.

3.2.2 Identificerede risici

I forhold til cyber- og informationssikkerhed er der ifølge analysen tre risici, som søfartssektoren selv vurderer som særligt signifikante:

- Manglende rettidig respons på tekniske sårbarheder: Det er nævnt, at der er en teknologikløft blandt de anvendte informationsteknologier (IT - fx administrative systemer) og operationelteknologier (OT- fx fremdrivningssystemer), der anvendes på skibe versus landbaseret IT- og OT-teknologi. Landbaserede systemer er generelt bedre opdateret end de tilsvarende skibsbaserede systemer. Ved manglende fokusering på mulige risici og trusler samt på grund af manglende opdateringer af de skibsbaserede systemer, er der risiko for, at IT- og OT-anvendelsen på skibe lettere kan påvirkes af cyberangreb.

- Manglende proces for opgraderinger: Det er nævnt, at der blandt andet anvendes procedurer for opgradering af OT-udstyr, som ligger uden for de retningslinjer, der anvendes blandt IT-teknologier. Der er således risiko for fejlede opgraderinger af fx SCADA-systemer der anvendes til overvågning og styring af industrielle processer.

- Sikring af kritiske systemer: Det er nævnt, at systemer, herunder databaser og register, der er baseret på ældre teknologi kan være særlig sårbare over for målrettet angreb med henblik på at kompromittere og/eller slette kritiske data. Konsekvensen kan være tab af data, manglende datapålidelighed, tab af omdømme og ikke mindst et muligt økonomisk tab. Søfartsstyrelsens skibsregistre repræsenterer fx en risiko ift. hæftning af pant på skibe for den danske stat. Der kan i denne forbindelse være risiko for økonomisk skade, hvis et sådant register bliver ødelagt eller kompromitteret.

3.2.3 Anbefalinger

I analysen beskrives en række styrker vedrørende aktørernes evne til at varetage og imødekomme cybersikkerhed. Blandt de adspurgte aktører er det observeret, at de analoge færdigheder og muligheder er gode, defineret som mulighederne for at agere uden brug af IT-systemer. De analoge færdigheder og muligheder vil kunne træde til og opretholde drift og services, i tilfælde af nedbrud af IT- og OT-systemer. Mange af de adspurgte aktører har arbejdet fokuseret med cybersikkerhed og er derfor også meget opmærksomme på deres svagheder og styrker.

Analysen anbefaler at:

- der i søfartssektoren anvendes teknologier, der kan modstå cybertrusler – f.eks. kryptering af navigation og kommunikationsinfrastruktur,

- der anvendes anerkendte it-sikkerhedsstandarder. Ved efterlevelse af eller inspiration fra standarder, såsom ISO 27001, i forbindelse med cyber- og informationssikkerhed, opnår aktørerne, gennem deres til- og fravalg i ”Statement of Applicability” (SoA), at implementere de sikkerheds – og sikringsforanstaltninger, der netop er tilpasset deres specifikke risikoprofil. Standarder forstås og opfattes ens blandt internationale aktører, hvilket gør sikkerhedsarbejdet og forståelsen af IT-anvendelsen på tværs af sektoren transparent,

- der er skærpet opmærksomhed på IT-sikkerhed blandt de ansatte i sektoren. Det er observeret, at IT-awareness og uddannelse ikke er stærkt forankret på skibene. Søfartssektoren er i forvejen præget af at have uddannelse og rutiner inden for øvrig sikkerhed - f.eks. brandinstrukser. Denne tankegang bør således overføres på IT-anvendelsen,

- kommunikationen, styringen og vejledningen af IT-sikkerhed bør komme fra topledelsen. Et skib eller en afdeling bør aldrig agere isoleret vedrørende IT-sikkerhed,

- der arbejdes med en styrkelse af leverandørstyringen (Supply Chain Management). Fartøjer bliver i stigende grad digitaliserede og de nyeste fartøjer opdateres og vedligeholdes direkte af de leverandører, der har leveret systemerne. Kompleksiteten af disse systemer betyder dog, at vedligeholdelsen i stigende grad outsources. Det anbefales, at der stilles specifikke krav til leverandørers sikkerhedsniveau og opfølgning på leverandørernes kvalitet.

- der samarbejdes omkring cybersikkerhed i systemer, services, teknologier og data, der benyttes på tværs af de samfundskritiske sektorer. Fællesindsatser på tværs af sektorerne vil give god mening, men forudsætter koordinering og målrettet regulering i forhold til et minimums sikkerhedsniveau.

4 Styrket indsats for at styrke cyber- og informationssikkerheden i søfartssektoren

På baggrund af trusselsvurderingen og sårbarhedsanalysen iværksættes der følgende tiltag, der skal styrke cyber- og informationssikkerheden i sektoren. Disse er beskrevet nærmere i afsnit 4.1.1.- 4.1.8.

4.1.1 Søfartens cyber- og informationssikkerhedsenhed

Til at håndtere opgaven med at implementere søfartssektorens strategi for cyber- og informationssikkerhed har Søfartsstyrelsen etableret Søfartens cyber- og informationssikkerhedsenhed, hvis formål det er at sikre, at strategiens initiativer udføres. Enheden skal på baggrund af aktuelle trusselsvurderinger og gennem et indgående kendskab til søfartssektoren (aktører, tjenester og infrastruktur) rådgive og fungere som et samlende kommunikationspunkt vedr. cyber- og Informationssikkerhed for hele søfartssektoren samt have en intern ekspertfunktion vedr. cyber- og informationssikkerhed i Søfartsstyrelsen.

De primære opgaver i denne forbindelse vil være at formidle, efterspørge, skabe og validere IT-sikkerhedsrelateret information mellem søfartssektorens aktører. Andre opgaver vil fx være koordination og gennemførelse af faglige workshops og konferencer, relateret til specifikke IT-sikkerhedsproblemstillinger i søfartssektoren. Der vil blive udarbejdet en handlingsplan for de konkrete indsatser, som skal gennemføres i tæt samarbejde med sektoren, fx om kompetenceudvikling, håndhævelse, regulering, leverandørstyring og informationsindsatser.

4.1.2 Implementering af EU- og International lovgivning

EU's Net- og informationssikkerhedsdirektiv (NIS-direktivet) trådte i kraft den 9. maj 2018 og har til formål at øge sikkerheden i de tjenester, der er afhængige af net- og informationsteknologi. Som én af sektorerne nævnt i direktivet skal søfartssektoren leve op til direktivets krav om bl.a. udpegning af operatører af væsentlige tjenester og indberetning af sikkerhedshændelser. Det følger af NIS-direktivet, at operatører af væsentlige maritime tjenester i søfartssektoren hurtigst muligt skal indberette hændelser, der har haft væsentlige konsekvenser for kontinuiteten af den maritime tjeneste, til Søfartsstyrelsen (Søfartens cyber- og informationssikkerhedsenhed) og til CFCS.

Søfartsstyrelsen udsteder derfor primo 2019 en bekendtgørelse om sikkerhed i net- og informationssystemer af betydning for skibes sikkerhed og deres sejlads, der implementerer NIS-direktivet i Danmark på dette område. Det følger af bekendtgørelsen, at der fastsættes 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 har konsekvenser for skibenes sikkerhed og deres sejllads.

Større lastskibe og passagerskibe er omfattet af den internationale kode for sikker skibsdrift (ISM), og skal efter disse regler allerede tage hensyn til cybersikkerhed. 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.

Baseret på den ovennævnte risiko- og sårbarhedsanalyse vil Søfartsstyrelsen fastlægge hvilke andre skibe, som bør omfattes af cyber- og informationssikkerhedskrav. Herudover anvender skibe i dansk farvand en række digitale maritime tjenester, som forsyner skibene med data, eller som overvåger skibenes færden. Det omfatter bl.a. Vessel Traffic Service (VTS), der overvåget skibstrafikken i hhv. Storebælt og Øresund, sejladsinformation (navigationsadvarsler) til skibsfarten i danske farvande og informationsudvekslings-systemer som AIS (Automatic Identification System). Efter bekendtgørelsens ikrafttrædelse vil Søfartsstyrelsen udarbejde en liste over operatører af maritime tjenester, som er omfattet af bekendtgørelsen. Denne liste vil også blive fremsendt til EU-Kommissionen. Mindst hvert andet år vil Søfartsstyrelsen foretage denne vurdering og opdatere listen.

Tilsynet med skibe og rederier vil indgå i de periodiske syn, som Søfartsstyrelsen allerede i dag udfører, og der vil fremadrettet også blive ført tilsyn med maritime tjenester.

4.1.2.1 Søfartsstyrelsens internationale indsats:

For dansk søfart og Søfartsstyrelsen er det vigtigt, at reguleringen af søfartssektoren i udgangspunktet foregår på internationalt niveau. Det skyldes, at søfarten i sin natur er global. Det er derfor en grundlæggende dansk prioritet, at dansk søfartsregulering er i overensstemmelse med internationale regler, og således at der er fælles globale regler for cybersikkerhed for alle rederier og 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 informationssikkerhedsområdet. Det vil desuden skade danske rederier og søfart generelt, hvis Danmark eller EU fastsætter strengere eller bare anderledes krav end resten af verden, da det vil kunne medføre konkurrenceforvridende rammevilkår.

Søfartsstyrelsen vil derfor arbejde for, at søfartssektorens rammer for cyber- og informationssikkerhed bliver globale og forhandles i regi af FN's Søfartsorganisation (IMO), og der etableres relevante samarbejder både internationalt og i EU landene, så danske rederier kan anvendes samme globale standarder til at forebygge cyberangreb.

4.1.3 Brugervenlige anbefalinger til søfartssektorens aktører

Digitalisering og automatisering af systemer og processer inden for søfartssektoren understøtter blandt andet målsætninger om sikker og effektiv godshåndtering, forøget sejladssikkerhed, minimering af brændstofforbrug, forbedrede kundeoplevelser i form af fleksible og brugervenlige kundeplatforme, men også målsætninger om overholdelse af internationale regler om fx skibssyn, beredskabsplanlægning, miljøhensyn, personsikkerhed og transport af farligt gods. Den øgede afhængighed af digitale løsninger introducerer, som nævnt i risiko- og sårbarhedsanalysen, imidlertid en række sårbarheder, der kan resultere i hændelser, som kan føre til nedbrud af skibs- og logistiksystemer, person- og materielskade, påvirke fremkommeligheden negativt eller påvirke kommunikationen til kunderne.

Konkret iværksættes følgende initiativer:

Søfartsstyrelsen vil udarbejde konkrete og brugervenlige anbefalinger, der skal medvirke til et øget fokus på cyber- og informationssikkerhed i sektoren. Det drejer sig bl.a. om følgende overordnede anbefalinger:

- cyber- og informationssikkerhed kræver ledelsens opmærksomhed og prioritering,

- fundamentet for arbejdet med cyber- og informationssikkerhed udspringer af et kontinuerligt fokus på risiko-og sårbarhedsvurdering,

- der bør gennemføres årlige beredskabsøvelser i de enkelte organisationer og

- der bør hos maritime operatører af væsentlige tjenester altid forefindes Business Continuity Planer for alle kritiske systemer og forretningsprocesser.

- Derudover skal Søfartens cyber- og informationssikkerhedsenhed, gennem konkrete anbefalinger støtte og rådgive søfartssektorens aktører til at kvalificere deres videre indsats for at styrke cyber- og informationssikkerheden i de enkelte organisationer.

Initiativerne udmøntes og implementeres gennem et tæt samarbejde med fx Danske Rederier samt gennem direkte møder med erhvervets aktører, herunder fx rederier og udstyrsproducenter.

4.1.4 It-sikkerhedskultur og awareness

Søfartssektoren har altid haft stor fokus på sikkerhed og er derfor nået langt i arbejdet med den generelle sikkerhed i forbindelse med søfart. Fokus på fx medarbejder-, transport-, gods-, og ikke mindst sejlads- og søsikkerhed har ført til, at der i dag er en god sikkerhedskultur i søfartssektoren. Denne sikkerhedskultur skal nu udbygges til også at omfatte cyber- og informationssikkerhedsområdet, der involverer mennesker, teknologier og processer 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 sikkerheds- og awareness program, som igen fremmer sikkerhed på alle niveauer og alle områder i organisationen. En god cyber- og informationssikkerhedskultur skabes dog ikke kun via regler og procedurer, men i meget høj grad af mennesker i deres daglige arbejde, herunder den adfærd, som efterspørges og udøves. Derfor er sikkerhedskultur båret af sikkerhedskommunikation og sikkerhedsledelse er en vigtig forudsætning for opnåelse af et højt awareness-niveau blandt søfartssektorens aktører.

Konkret iværksættes følgende initiativer:

Søfartsstyrelsen vil gennem målrettet og fagligt funderede awareness-kampagner øge det generelle awareness-niveau i søfartssektoren. I tæt samarbejde med sektorens aktører skal der årligt gennemføres awareness-kampagner på tværs af sektoren. Det kan fx være informationskampagner om GDPR compliance, men kan også være gennemførelse af mere direkte og fokuserede kampagner om beskyttelse mod phishing mail eller, hvordan man opnår den størst mulige mobilsikkerhed.

4.1.5 Fokusering på standardiserede processer i relation til cyber- og Informationssikkerhedsledelse

Det er i dag obligatorisk for alle danske statslige myndigheder at følge ISO 27001 standarden, der er en anerkendt og udbredt international sikkerhedsstandard, der blandt andet fastsætter best practice for styring af informationssikkerhed. ISO 27001 standarden kan dog med fordel suppleres med National Institute of Standards and Technologys (NIST) rammeværktøj for cybersikkerhed. Hvor ISO 27001 standarden typisk anvendes i Europa, anvendes NIST's rammeværktøj ofte i en mere global kontekst. Selvom de to standarder naturligvis overlapper en

del, har de dog forskellige styrker. ISO 27001 standarden fokuserer primært på styring og processer, mens NIST har et stærkere fokus på de tekniske sikkerhedstiltag. Således komplementerer de to standarder hinanden.

Gennem anvendelse af anerkendte It-sikkerhedsstandarder kan søfartssektoren opnå en effektiv It-sikkerhedsledelse, der passer til søfartssektorens særlige behov samt sikre, at denne effektivitet fastholdes gennem en standardiserede proces for løbende forbedring. Det betyder, at it-sikkerheden løbende opdateres, således at søfartssektoren er i stand til at håndtere udfordringerne i en digital verden under konstant forandring og angreb.

Konkret iværksættes følgende initiativer:

- Arbejdet med cyber- og informationssikkerhedsledelse i søfartssektoren skal styrkes gennem fokusering på standardiserede processer i relation til cyber- og informationssikkerhedsledelse, herunder anvendelse af anerkendte IT-sikkerhedsstandarder, der stiller krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for It-sikkerhed.

- Der skal anvendes en risikostyret proces, der sikrer og bevarer fortrolighed, integritet og tilgængelighed af information således, at der opnås bedst mulig beskyttelse af informationer mod uautoriseret videregivelse eller adgang.

4.1.6 Sikre et vedvarende og robust cyber- og informationssikkerhedsberedskab i søfartssektoren

"*Det er ikke et spørgsmål, om en organisation bliver ramt af en It-sikkerhedshændelse, men om hvornår. Ja måske er organisationen allerede ramt, men er bare ikke klar over det.*" Uanset hvor godt man som organisation sikrer sig, vil der på et eller andet tidspunkt ske en It-sikkerhedshændelse. Det kan fx være et utilsigtet nedbrud af et administrativt system, et brud på persondataloven eller en fuldstændig lammelse af produktionsapparatet pga. et udefrakommende cyberangreb. Uanset, hvordan en It-sikkerhedshændelse udmønter sig, er det vigtig at have systemer klar til at sikre overblik samt have etableret og afprøvet et passende beredskab, der kan håndtere de It-sikkerhedshændelse man risikerer at blive ramt af.

It-beredskabsstyring eller Business Continuity Management handler om at sikre en organisation i tilfælde af It-sikkerhedshændelse, der rammer produktionsapparatet, herunder forretningskritiske processer, systemer og produkter. Dette omtales også som Respond & Recover og skal sikre, at organisationens IT-understøttelse kan genetableres i tilstrækkelig grad inden for en ønsket tidsperiode med udgangspunkt i, hvornår opgavevaretagelsen bliver truet i en grad, hvor konsekvenserne er uacceptable.

Konkret iværksættes følgende initiativ:

Et vedvarende og robust cyber- og informationssikkerhedsberedskab i søfartssektoren opnås ved at Søfartsstyrelsen rådgiver sektoren generelt om IT-beredskabsstyring, herunder vigtigheden af en beredskabsplanlægning, der sikrer, at planerne fx omfatter alvorlige IT-sikkerhedshændelser, der fuldstændig lammer alle former for IT-systemer samt sikrer, at alle involverede medarbejdere kender deres funktioner og er i stand til at udføre dem.

4.1.7 Udvekslingspunkt mellem søfartssektorens aktører og CFCS

Søfartsstyrelsen vil fungere som udvekslingspunkt mellem søfartssektorens aktører og CFCS. De primære opgaver i denne forbindelse vil være at formidle, efterspørge, skabe og validere IT-sikkerhedsrelateret information mellem parterne. Andre opgaver vil fx være koordination og gennemførelse af faglige workshops og konferencer, relateret til specifikke IT-sikkerhedsproblemstillinger i søfartssektoren.

Givet søfartssektorens globale karakter kan det være nødvendigt at etablere kontakt til pålidelige internationale samarbejdspartnere med, hvem man kan dele erfaringer og viden inde for IT sikkerhedsområdet. Der er blandt andet

fra USA tilkendegivet interesse for indsigt i den danske regerings cyber- og informationssikkerhedsstrategi, og det vil derfor være hensigtsmæssigt at fremme en global koordinering med væsentlige aktører inden for området.

Konkret iværksættes følgende initiativer:

Søfartsstyrelsen ønsker:

- I tæt samarbejde med CFCS at kunne analysere og formidle trusselsbilleder for søfartssektoren, således at cybertrusler kan imødegås hurtigt og effektivt,

- at bidrage til udarbejdelse af trusselsvurderinger i samarbejde med CFCSs trusselsvurderingsenhed,

- at stå for den løbende kontakt (gateway) til de relevante aktører i søfartssektoren og bidrage til, at viden direkte kan understøtte arbejdet med cybersikkerhed i sikkerhedsorganisationerne hos sektorens myndigheder og virksomheder

- at bidrage til øget globalt fokus og samarbejde vedr. maritim cybersikkerhed.

4.1.8 Indstationering af søfartsmedarbejder hos CFCS

Der indstationeres en søfartsmedarbejder CFCS. Dette skal sikre og understøtte, at CFCS har den nødvendige viden om søfarten og kompetencer til rådighed, som Søfartsstyrelsen og søfartssektoren herefter kan drage nytte af i sit arbejde med at sikre et højt cyber- og informationssikkerhedsniveau.

4.2 Det maritime cyber- og informationssikkerhedsforum

For at muliggøre erfaringsudveksling og vidensdeling på tværs af søfartssektoren, etableres det maritime cyber- og informationssikkerhedsforum.

Forummet skal bestå af It-sikkerhedsrepræsentanter fra danske myndigheder med direkte berøring til det maritime område. Søfartsstyrelsen vil varetage koordinations- og sekretærfunktionen i det maritime cyber- og informationssikkerhedsforum, og det forventes, at medlemmerne skal kunne udveksle erfaringer med hinanden i forhold til konkrete IT-sikkerhedstiltag. Forummet skal fx kunne bruges til at drøfte, hvordan forskellige sikkerhedshændelser er blevet håndteret af de berørte parter, således at alle forummets medlemmer kan drage nytte af de erfaringer man har gjort sig i de givne situationer.

Forummets primære formål er at;

- stå for koordination af håndteringen af cyber- og informationssikkerhed på tværs af søfartssektoren,

- gennem vidensdeling at identificere og konkretisere områder, hvor der i fællesskab kan iværksættes initiativer, der styrker søfartssektorens cyber- og informationssikkerhed.

Det maritime cyber- og informationssikkerhedsforum skal gennemføre en række initiativer gennem strategiens levetid. Disse er beskrevet nærmere i afsnit 4.2.1.-4.2.3.

4.2.1 Øget awareness-niveau gennem samarbejde og vidensdeling i søfartssektoren

Vidensdeling i søfartssektoren handler om at samarbejde på tværs af fagområder samt om at udnytte den cyber- og informationssikkerhedsviden, der allerede eksisterer i de enkelte myndigheder inden for søfartssektoren. Dette skal opnås ved at sikre, at aktører der har behov for viden, får adgang til viden.

Søfartens cyber- og informationssikkerhedsforum skal:

- gennem møder og workshops sikre samarbejde og vidensdeling om cyber- og informationssikkerhed på tværs af søfartssektorens aktører,

- gennem vidensdeling identificere om der, på tværs af ressortområder, er særlige udfordringer, der i fællesskab kan/skal imødegås i relation til cyber- og informationssikkerhed,

- identificere eventuelle grænseflader til allerede eksisterende cyber- og informationssikkerhedsfora, nationalt som internationalt.

4.2.2 Fælles beredskabs- og varslingsplan til håndtering af It-sikkerhedshændelser

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 deles og bringes videre hurtigst muligt, så også andre myndigheder kan bruge denne viden med det samme. Søfartens cyber- og informationssikkerhedsforum skal:

- etablere en fælles beredskabsplan til håndtering af IT-sikkerhedshændelser og for varsling af andre relevante myndigheder i tilfælde af beredskabets aktivering,

- på sigt afdække behovet og mulighederne for udvikling af et digitalt samlingspunkt/en kommunikationsplatform, hvor cyber- og informationssikkerhedsviden bliver gjort tilgængelig og søgbar for søfartssektorens myndigheder og interessenter.

4.2.3 Planlægning og gennemførelse af fælles cyber-og informationssikkerhedsøvelser

Cyber- og informationssikkerhedsøvelser bør være en central del af alle myndigheders cyberberedskab. Formålet med disse øvelser er at afprøve og udvikle myndighedernes medarbejdere, planer, procedurer og teknologi samt samarbejdsrelationer. Alle søfartssektorens myndigheder bør derfor som standard planlægge og afholde regelmæssige og varierede øvelser, for at forberede håndteringen af relevante og aktuelle cybertrusler. Dette sker bedst ved, at myndighederne både afholder egne interne øvelser samt deltager i tværgående øvelser med fokus på samarbejde.

Søfartens cyber- og informationssikkerhedsforum skal:

- udarbejde beredskabsplaner til imødegåelse af relevante og aktuelle cybertrusler,

- koordinere fælles cyber-og informationssikkerhedsøvelser. Der skal fx gennemføres tværgående beredskabsøvelser, hvor der trænes scenarier, hvor flere aktører på tværs af søfartssektoren bliver ramt af samtidige cyber- og informationssikkerhedshændelser.

5 Afslutning

Søfartssektorens cyber- og informationssikkerhedsudfordringer vil indgå som en integreret del af styrelsens arbejde med maritim sikkerhed og kan 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. Søfartsstyrelsens strategiske målsætning med delstrategien for Cyber- og informationssikkerhed er således:

at sikkerheden om bord i danske skibe samt i danske farvande ikke kompromitteres, som følge af cyberangreb.

Søfartsstyrelsens arbejde med at bidrage til cyber- og informationssikkerhed i søfartssektoren vil indgå som en integreret del af det almindelige sikkerhedsarbejde i styrelsen, herunder håndhævelse af gældende krav og regler, i forhold til forebyggelse og håndtering af hændelser.

Delstrategien supplerer implementeringen af NIS-direktivet med konkrete initiativer, som med udgangspunkt i sektorens sårbarheder og aktuelle modenhed bidrager til øget robusthed over for cyberangreb og dermed øget cybersikkerhed i søfartssektoren.

Søfartssektorens cyber- og informationssikkerhedsenhed er etableret medio 2018 og skal blandt andet fungere som udvekslingspunkt mellem søfartssektorens aktører og CFCS. De primære opgaver i denne forbindelse vil være at rådgive, formidle, efterspørge, skabe og validere It-sikkerhedsrelateret information mellem søfartssektorens aktører. Andre opgaver vil fx være undervisning, koordination og gennemførelse af faglige workshops og konferencer, relateret til specifikke It-sikkerhedsproblemstillinger i søfartssektoren.

5.1 Tidshorisont

Tidshorisont for de strategiske målsætninger og initiativer der gennemføres i relation til strategi for søfartssektorens cyber- og informationssikkerhed:

Kort sigt (2019)

Pkt. 4.1.1 Etablering af Søfartens cyber- og informationssikkerhedsenhed (juni 2018)

Pkt. 4.1.2: EU- og International lovgivning

Pkt. 4.1.7: Udvekslingspunkt mellem søfartssektorens aktører og CFCS

Pkt. 4.1.8: Indstationering af søfartsmedarbejder hos CFCS

Pkt. 4.2.1: Øget awareness niveau gennem samarbejde og vidensdeling i søfartssektoren

Mellemlang sigt (2020 – 2021)

Pkt. 4.1.3: Konkrete målsætninger og brugervenlige anbefalinger til søfartssektorens aktører

Pkt. 4.1.4: It-sikkerhedskultur og Awareness

Pkt. 4.1.5: Fokusering på standardiserede processer i relation til cyber- og Informationssikkerhedsledelse

Pkt. 4.1.6: Sikre et vedvarende og robust cyber- og informationssikkerhedsberedskab i søfartssektoren

Pkt. 4.2.2: Fælles beredskabs- og varslingsplan til håndtering af It-sikkerhedshændelser

Pkt. 4.2.3: Planlægning og gennemførelse af fælles cyber-og informationssikkerhedsøvelser

Langt sigt (2022)

Afdækket behovet og mulighederne for udvikling af et digitalt samlingspunkt/en kommunikationsplatform, hvor cyber- og informationssikkerhedsviden bliver gjort tilgængelig og søgbar for søfartssektorens myndigheder og interessenter.