CENTER FOR CYBERSIKKERHED

Januar 2019
Opdateret juni 2020

Trusselsvurdering: Cybertruslen mod søfartssektoren

Trusselsvurderingen redegør for cybertrusler, der er rettet mod den danske søfartssektor. Søfartssektoren i Danmark er vigtig for samfundets funktion, stabilitet og økonomi. Hensigten er at orientere søfartssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i sektorens arbejde med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurderingen er opdateret med ændringer i kapitlet om cyberterror som følge af ændret trusselsniveau i den nationale trusselsvurdering "Cybertruslen mod Danmark" udgivet juni 2020. Ligesom i den nationale vurdering er der tilføjet et trusselsniveau for destruktive cyberangreb.

Hovedvurdering

- Truslen fra cyberspionage mod den danske søfartssektor er **MEGET HØJ.** Truslen kommer særligt fra fremmede stater, der både kan have økonomisk og politisk interesse i at spionere mod virksomheder og myndigheder i søfartssektoren.
- Truslen fra cyberkriminalitet mod søfartssektoren er **MEGET HØJ.** Cyberkriminelle retter mange forskellige slags cyberangreb mod virksomheder og myndigheder i søfartssektoren. Udover at have økonomiske konsekvenser kan cyberkriminalitet i værste fald forstyrre driften i sektoren.
- Truslen fra destruktive cyberangreb mod den danske søfartssektor er **LAV**. Det er dog muligt, at den danske søfartssektor kan blive påvirket af destruktive cyberangreb i udlandet.
- Truslen fra cyberaktivisme er **LAV.** Truslen er ofte motiveret af enkeltsager, og truslen mod sektoren kan derfor stige uden eller med kort varsel. Det kan eksempelvis ske i kølvandet på politiske debatter og hændelser, der involverer søfartssektoren, såsom transport af kontroversielt gods eller olielækager fra skibe.
- Truslen fra cyberterror er **INGEN**. Denne type angreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

Indledning

Vurderingen beskriver den generelle cybertrussel, der er rettet imod den danske søfartssektor. Ligesom de fleste sektorer i Danmark er søfartssektoren i stigende grad afhængig af digitale systemer og enheder, hvilket medfører, at cyberangreb potentielt kan påvirke driften og sikkerheden i sektoren. Da søfartssektoren er en del af Danmarks samfundsvigtige infrastruktur, er det vigtigt, at myndigheder og virksomheder i sektoren er robuste overfor cyberangreb.

Søfartssektoren består af forskellige dele med varierende kompleksitet og egne særpræg og sårbarheder. Denne trusselsvurdering analyserer cybertruslen mod søfartssektoren som helhed, og der skelnes kun mellem enkeltdelene af sektoren i et begrænset omfang. Havne indgår som udgangspunkt ikke i denne trusselsvurdering, da havnene i Danmark ligger under transportsektoren og derfor er omfattet af trusselsvurderingen for den sektor. Skibsfart udført af Forsvarets enheder indgår ligeledes ikke i vurderingen.

Flere virksomheder i søfartssektoren er til stede i store dele af verden, og kæden af leverandører og samarbejdspartnere i søfartssektoren er ofte lang og kompleks. Transporten af eksempelvis en enkelt container kan involvere en lang række virksomheder og myndigheder i flere forskellige lande. Det medfører, at cyberangreb mod mål udenfor Danmark kan påvirke driften i den danske søfartssektor eller integriteten af systemer, som danske virksomheder i søfartssektoren benytter sig af. Cybertruslen mod henholdsvis den danske og den globale søfartssektor analyseres derfor i tæt sammenhæng.

Trusselsvurderingen tager udgangspunkt i Forsvarets Efterretningstjenestes Center for Cybersikkerheds (CFCS') generelle viden om cybertrusler og eksempler på cyberangreb mod søfartssektoren. CFCS har endnu et relativt begrænset indblik i sektorspecifikke forhold i søfartssektoren sammenlignet med andre samfundsvigtige sektorer.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Der er mørketal, når det gælder viden om cyberangreb mod myndigheder og virksomheder i søfartssektoren. Mørketallene skyldes bl.a., at nogle cyberangreb ikke bliver anmeldt til relevante myndigheder, enten fordi organisationen ønsker mindst mulig opmærksomhed omkring et angrebsforsøg, eller fordi de ikke er klar over, at de har været udsat for angreb. CFCS anbefaler, at virksomheder benytter sig af CFCS' underretningsordninger.

Hvad er cybertrusler

CFCS definerer cybertrusler som trusler fra cyberangreb, hvor en aktør ved hjælp af it forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet, der kan have negative konsekvenser for samfundet, såsom salg af ulovlige varer og tjenester på internettet, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. CFCS beskriver og vurderer her aktiviteter, der har til formål at udføre cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden vurderer CFCS den potentielle trussel fra destruktive cyberangreb.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Cyberspionage

Truslen fra cyberspionage mod søfartssektoren er **MEGET HØJ**. CFCS vurderer, at truslen især kommer fra fremmede stater. Cyberspionage mod virksomheder og myndigheder i søfartssektoren kan skade de berørte organisationers økonomi og integritet samt udgøre en potentiel sikkerhedspolitisk trussel mod Danmark.

Cyberspionage mod søfartssektoren kan bl.a. være motiveret af økonomiske interesser. Fremmede stater kan have interesse i at stjæle viden om ny maritim teknologi eller informationer om udbud eller forhandlinger af store kontrakter. Ved at stjæle informationer i forbindelse med store kontrakter i søfartssektoren kan fremmede stater give deres virksomheder fordele på det internationale marked.

Nogle stater udfører også cyberspionage mod virksomheder, primært fordi virksomhederne samarbejder med den fremmede stats nationale virksomheder eller myndigheder. De fremmede stater gør dette for at overvåge samarbejdspartnere og virksomheder, fordi det kan have indflydelse på nationale organisationer.

Spionage mod søfartssektoren kan også være motiveret af sikkerhedspolitiske interesser. Eksempelvis kan åbningen af nye sejlruter samt sejlads i farvande, hvor der er territorialstridigheder, have særlig interesse for fremmede stater.

Fordi søfartssektoren indgår i dansk samfundsvigtig infrastruktur, kan fremmede stater også have interesse i at opbygge viden om kapaciteter og sårbarheder i søfartssektoren, der f.eks. kan være relevante i forbindelse med en militær konflikt. Indhentning af information om kritisk infrastruktur kan benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.
I det omfang at dele af søfartssektoren støtter dansk forsvar eller andre landes militær, eksempelvis transport af tropper eller materiel, kan dette også have fremmede staters interesse. Udenlandske civile rederier, der har løst transportopgaver for det amerikanske forsvar, har været udsat for cyberspionage.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod sektoren er **MEGET HØJ**. Cyberkriminalitet dækker i denne vurdering handlinger, hvor gerningsmanden bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk vinding.

Cyberkriminelle er opfindsomme i deres forsøg på at berige sig og anvender mange forskellige typer cyberangreb, hvoraf en del fortsat bliver mere avancerede og komplekse. Nogle af disse cyberangreb sigter mod at afpresse penge fra virksomheder og myndigheder. Denne trussel kommer især til udtryk i form af ransomwareangreb, hvor hackere kræver en løsesum for at gøre data eller systemer, de har angrebet, tilgængelige igen. Ransomware er særligt problematisk, da det i værste fald kan påvirke driften i søfartssektoren.

Spear-phishing mod søfartssektoren

I oktober 2018 blev der sendt spear-phishing-mails til virksomheder i bl.a. søfartssektoren i flere lande. E-mailsene anvendte forskellig grad af social engineering for at fremstå relevante for modtagerne. En af disse e-mails omhandlede en forespørgsel om køb af maritime reservedele og blev sendt til en italiensk virksomhed i flådeindustrien. En vedhæftet fil i mailen indeholdt malware. Det er muligvis cyberkriminelle, der står bag. Kampagnen er blevet omtalt som MartyMcFly.

Driften kan eksempelvis blive påvirket, hvis operative systemer om bord på skibe bliver inficerede med ransomware. Skibe er ikke længere isolerede fra eksterne systemer. Selv når netværk om bord på skibe er segmenterede, kan de med tiden blive kompromitterede ved manuelle overførsler af data udført af mandskab, teknikere eller leverandører, for eksempel i forbindelse med vedligeholdelse. I åbne kilder er der bl.a. blevet beskrevet en hændelse i udlandet, hvor et skibs switchboard lukkede ned, efter at skibets systemer var blevet inficeret med ransomware. Et switchboard har en central funktion ift. bl.a. generatorstyring på et skib. Et it-sikkerhedsselskab har også beskrevet en hændelse i udlandet, hvor et centralt navigationsværktøj blev inficeret med malware via et USB-stik.

Driften kan ligeledes blive påvirket, hvis administrative systemer hos en maritim virksomhed bliver inficerede med ransomware. I juli 2018 blev den kinesiske shippingvirksomhed China Ocean Shipping (Group) Company, oftest omtalt som COSCO, ramt af et cyberangreb, som ifølge medieberetninger var ransomware. Cyberangrebet påvirkede bl.a. virksomhedens interne kommunikationskanaler på flere kontorer i Nord- og Sydamerika, hvilket besværliggjorde virksomhedens arbejde i en periode.

Cyberkriminelle afpresser også deres ofre på andre måder f.eks. ved hjælp af DDoS-angreb eller ved at true med at offentliggøre data, som de har stjålet ved hjælp af hacking. I november 2018 blev det offentliggjort, at det australske værft Austal var blevet hacket, og at hackerne havde forsøgt at afpresse virksomheden samt at sælge de stjålne data via internettet. Året forinden blev den britiske virksomhed Clarkson PLC ligeledes udsat for forsøg på afpresning, efter at hackere havde kompromitteret en brugerkonto hos virksomheden og fået adgang til følsomme oplysninger. Tyveri af eksempelvis personlige og finansielle oplysninger kan svække kundernes tillid til ramte virksomheder i sektoren.

Bedrageri i form af såkaldte Bussiness Email Compromise scams (BEC-scams) er fortsat en trussel på tværs af sektorer. BEC-scams har til formål at franarre virksomheder og myndigheder penge via bedrageriske e-mails, der indeholder instrukser om at gennemføre pengeoverførsler til aktøren. De bedrageriske e-mails sendes ofte fra fremmede mailkonti, men i nogle tilfælde kan bedrageriforsøget misbruge kompromitterede mailkonti. De kriminelle kan eksempelvis have hacket en ledende medarbejders mailkonto eller en af virksomhedens kunders mailkonti for at få de bedrageriske mails til at fremstå troværdige. Nogle cyberkriminelle har målrettet deres BEC-scams mod shippingvirksomheder og disses kunder, muligvis pga. at virksomheder i shippingindustrien ofte opererer i forskellige tidszoner, og transaktioner derfor koordineres via e-mail. BEC-scams kan medføre betydelige økonomiske tab for den berørte.

Cyberkriminelle spreder også malware, som misbruger ofrets computerkapacitet til at genere kryptovaluta. Malware, der generer kryptovaluta, kan påvirke it-netværk og skabe driftsforstyrrelser, længere svartider og i værste fald nedbrud på systemer.

Cyberangreb kan derudover understøtte andre former for kriminalitet rettet mod søfartssektoren. Cyberkriminelle kan bl.a. understøtte smugling, pirateri eller tyveri af gods i havne ved at hacke sig ind i virksomheders systemer og stjæle eller manipulere informationer om gods eller skibe. Udover at det kan medføre økonomiske tab for virksomheder i sektoren, kan det påvirke sikkerheden omkring transporten af gods og mennesker til søs.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod søfartssektoren er **LAV**.

Det betyder, at det er mindre sandsynligt, at søfartssektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur, såsom søfartssektoren. CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

På nuværende tidspunkt er det dog muligt, at danske myndigheder og virksomheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder fra bl.a. søfartssektoren, der er til stede i konfliktområder, hvor fremmede stater eller organiserede hackergrupper med kapacitet til at udføre destruktive cyberangreb har interesser, såsom Ukraine og Saudi Arabien.

A.P. Møller-Mærsk var en af mange virksomheder verden over, som i juni 2017 blev ramt af NotPetya-angrebet, der sandsynligvis var et destruktivt cyberangreb forklædt som ransomware. Det medførte store økonomiske tab for A.P. Møller-Mærsk. Cyberangrebet mod A.P. Møller-Mærsk reducerede også evnen til at håndtere last i havne, hvilket illustrerer, hvordan et cyberangreb, der rammer søfartssektoren, kan påvirke andre sektorer.

Cyberaktivisme

Truslen fra cyberaktivisme mod søfartssektoren er **LAV**. Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag.

Nogle hackergrupper og individer i cyberaktivistiske netværk har væsentlige evner og ressourcer til at udføre cyberangreb. Mens vi ikke ser mange eksempler på sådanne angreb i Danmark, kan truslen pludseligt stige. Hackere kan hurtigt mobiliseres omkring en sag f.eks. i kølvandet på politiske debatter og hændelser, der involverer søfartssektoren, såsom transport af kontroversielt gods eller olielækager fra skibe.

Cyberaktivister angriber også myndigheder og virksomheder, som hackerne betragter som symbolske mål. Myndigheder og virksomheder kan derfor blive angrebet, selvom de ikke har været direkte indblandet i den sag, der har fanget hackernes opmærksomhed. Angrebene kan også være tilfældige i den forstand, at hackerne angriber, hvor de kan skaffe sig adgang eller udnytte sårbarheder.

Cyberterror

Truslen fra cyberterror mod søfartssektoren er **INGEN**. Det betyder, at det er usandsynligt, at søfartssektoren, vil blive udsat for forsøg på cyberterror inden for de næste to år.

CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

Denne type alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynlighed i analyser: