CENTER FOR CYBERSIKKERHED

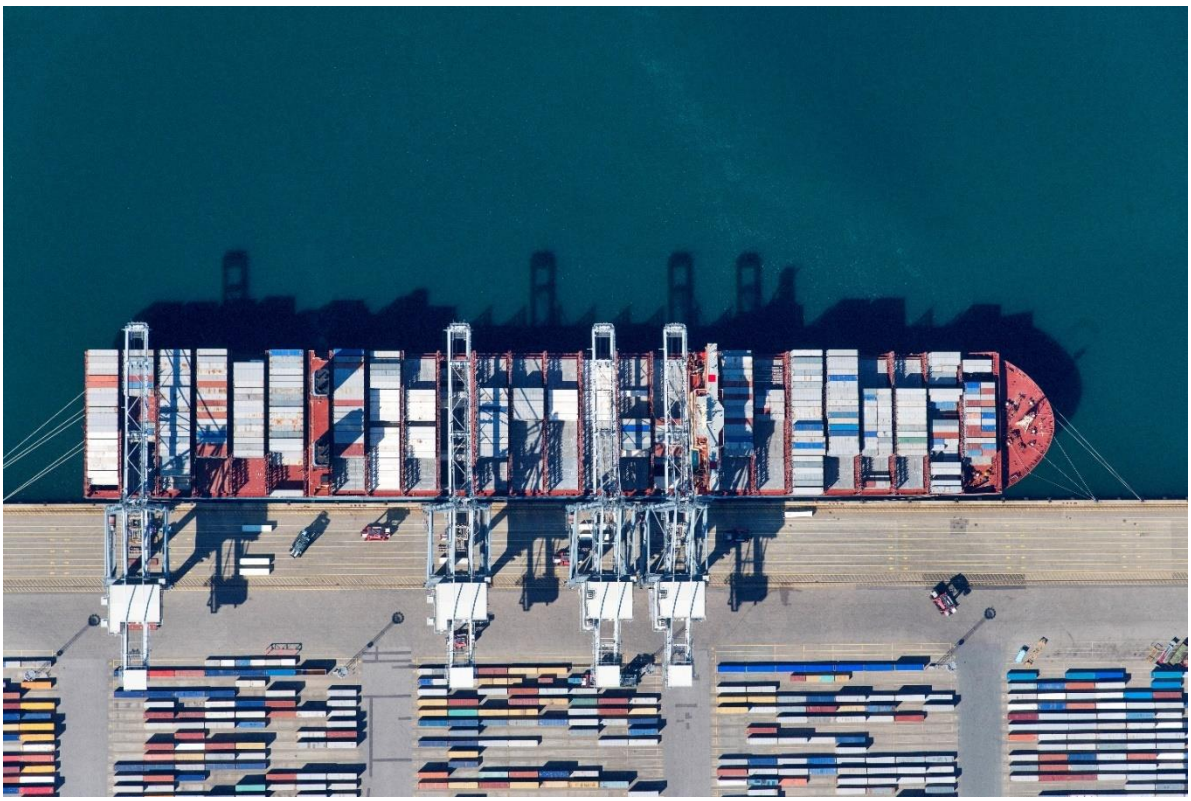

Foto: Mikkel Barker/ Ritzau Scanpix

Trusselsvurdering

Cybertruslen mod søfart og havne

Udgivet oktober 2020
Seneste opdatering juni 2022

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

2. udgave juni 2022.

CENTER FOR CYBERSIKKERHED

Center for cybersikkerhed hæver trusselsniveauet for cyberaktivisme til HØJ for søfartssektoren

Dato: 8. februar 2023

Truslen fra cyberaktivisme mod søfartssektoren hæves fra **MIDDEL** til **HØJ**. Det betyder, at det er sandsynligt, at virksomheder og myndigheder i sektoren vil blive ramt af cyberaktivistiske angreb inden for de næste to år.

CFCS hævede den 31. januar 2023 truslen fra cyberaktivisme mod Danmark. CFCS vurderer, at den øgede trussel fra cyberaktivisme også gælder for søfartssektoren.

CFCS hævede niveauet på baggrund af pro-russiske cyberaktivisters høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet.

Teksten i trusselsvurderingen er ikke opdateret, og kapitlet om cyberaktivisme afspejler ikke det gældende trusselsniveau.

For yderligere information om, hvorfor niveauet for cyberaktivisme er hævet, og hvordan truslen kommer til udtryk, henvises til CFCS' trusselsvurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra **MIDDEL** til **HØJ**" udgivet d. 31. januar 2023.

Trusselsvurderingen kan findes på www.cfcs.dk.

Trusselsvurdering: Cybertruslen mod søfart og havne

Denne trusselsvurdering har til formål at give beslutningstagere indenfor søfart og havne indsigt i de cybertrusler, som er rettet mod sektoren.

Trusselsvurderingen er blevet opdateret juni 2022 med et tilpasset kapitel om truslen fra cyberaktivisme som følge af en ændring af trusselsniveauet beskrevet i CFCS's vurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra LAV til MIDDEL" udgivet 18. maj 2022. Trusselsniveauet er hævet fra **LAV** til **MIDDEL**. Den øvrige tekst er uændret.

Hovedvurdering

- Der er en **MEGET HØJ** trussel fra cyberkriminalitet. Den generelle trussel fra cyberkriminalitet mod virksomheder og myndigheder i Danmark gælder også for søfartssektoren. Nogle af de, der hacker virksomheder på tværs af samfundet, går i perioder målrettet efter søfartssektoren. Der er også et mindre antal cyberkriminelle, som har specialiseret sig i angreb mod sektoren.

- Der er en **MEGET HØJ** trussel fra cyberspionage. Flere stater udfører cyberspionage mod søfartssektoren verden rundt. Det gør staterne bl.a. for at kunne fremme deres egen industri og økonomi. Staterne gør det også for at opnå sikkerhedspolitisk relevant viden.

- Truslen fra cyberaktivisme er hævet fra **LAV** til **MIDDEL**. CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. Det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder søfartssektoren.

- Der er en **LAV** trussel fra destruktive cyberangreb. Det er mindre sandsynligt, at fremmede stater vil udføre destruktive cyberangreb mod Danmark. Virksomheder og myndigheder, som har aktiviteter i konfliktområder, er mere udsatte for truslen.

- Der er **INGEN** trussel fra cyberterror. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som ved konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten blandt disse grupper er samtidigt begrænset.

Indledning

Trusselsvurderingen beskriver cybertruslen mod hele det såkaldte Blå Danmark og omfatter rederier, maritime udstyrsleverandører, myndigheder, havne m.v. Vurderingen gælder både organisationer i Danmark og deres aktiviteter internationalt.

Trusselsvurderingen dækker både almindelig udbredte it-systemer og sektorspecifikke systemer såsom operationelle systemer på skibe og i havne. Vurderingen beskriver det aktuelle trusselsbillede med en varslingshorisont på to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt.

Trusselsvurderingen er opdelt i trusler fra cyberangreb, der understøtter kriminalitet, spionage, aktivisme og terrorisme samt destruktive cyberangreb.

Søfart er vigtig for Danmark
Danmark er verdens femtestørste søfartsnation målt på opereret tonnage. Mere end 700 handelsskibe er danskflagede og knap 2.000 skibe opereres fra Danmark. Søfart er Danmarks største eksporterhverv, og langt de fleste aktiviteter foregår udenfor Danmark.

Det Blå Danmark består desuden af en række globalt førende og ofte højteknologiske udstyrsleverandører.

Søfarten er med til at binde Danmark sammen og giver forbindelser til vores nabolande. Danmark har flere end 50 indenrigs og 15 udenrigs færgeruter. Danske øsamfund og erhvervsliv er afhængige af stabil færgefart.

Med mere end 100.000 årlige skibsanløb sikrer erhvervshavnene rundt om i Danmark forsyninger til landet. Mere end tre fjerdedele af den danske import fragtes gennem havnene.

Årligt gennemsejles de danske stræder af omkring 70.000 skibe, heraf er mange dybgående tankskibe til og fra Østersøen. Det gør de danske farvande til nogle af de mest trafikerede i verden.

Cybersikkerhed er vigtig for søfart
Både skibe, rederier, udstyrsleverandører og havne anvender avancerede it- og ot-systemer i stigende grad. Cyberangreb mod systemerne kan potentielt forstyrre driften og skade de maritime virksomheders forretning. I værste fald kan cyberangreb mod skibe, rederier og havne også påvirke den fysiske sikkerhed. Derfor er en god cybersikkerhed vigtig for sektoren.

Mere information om cybertruslens mulige påvirkning af den fysiske sikkerhed kan findes i vurderingen Cybertruslen mod skibes operationelle systemer. Trusselsvurderingen er udgivet i marts 2020 og kan hentes på CFCS's hjemmeside.

Cyberkriminalitet

Cyberkriminelle truer søfartssektoren
Der er en **MEGET HØJ** trussel fra cyberkriminalitet. Det betyder, at det er meget sandsynligt, at organisationer i søfartssektoren i Danmark vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Kriminelle med økonomisk motiv hacker virksomheder og myndigheder på tværs af samfundet og rammer hermed også søfartsvirksomheder. Disse kriminelle hackere udgør den største cybertrussel for sektoren. Herudover er der kriminelle hackere, som laver enkeltstående kampagner rettet mod søfart eller specialiserer sig i angreb mod sektoren.

Truslen er primært rettet mod almindelige forretningssystemer såsom administrative systemer, der ikke er sektorspecifikke. Angreb kan dog også ramme eller sprede sig til operationelle systemer og i værste fald påvirke systemernes funktion.

Flere typer cyberkriminalitet er en trussel
Kriminelle hackere benytter sig af en bred palet af teknikker og måder at tjene penge på. Den enkelte hackergruppe specialiserer sig ofte i én metode til at angribe organisationer med. Men de kriminelle samarbejder også. De handler eksempelvis med adgange til kompromitterede virksomheder og værktøjer, der kan bruges i cyberangreb.

Både i Danmark og rundt om i verden er der eksempler på, at virksomheder i søfartssektoren bliver ramt af alle typer cyberkriminalitet. I de følgende afsnit beskrives et udsnit af angrebstyper og eksempler på de kriminelles indtægtskilder.

Alvorlige ransomware-angreb er blevet en del af normalbilledet
Cyberkriminelle bruger ransomware til at kryptere computere og netværk og forlanger en løsesum for at låse systemerne op igen. Det seneste år har målrettet ransomwareangreb været i fremmarch og sker nu relativt hyppigt i Danmark.

Hackere bruger i denne type angreb betydelig tid og ressourcer på at udvælge og kryptere vitale dele af kompromitterede ofres netværk. Når systemerne er låst, forlanger hackerne ofte flere millioner kroner for at låse dem op igen. Siden slutningen af 2019 truer hackere, der har stået bag målrettede ransomware-angreb, nu også af og til med at lække følsomme data indsamlet fra det ramte system, hvis offeret ikke betaler løsesummen.

Ransomwareangrebene er rettet mod virksomheder på tværs af sektorer globalt, inklusiv søfart. Hackerne går primært efter almindeligt udbredte it-systemer. Kriminelle hackere forsøger dog ofte at ramme de systemer, som er mest kritiske for ofret. Herved stiger sandsynligheden for, at ofret betaler løsesummen.

CFCS vurderer derfor, at hackere gerne krypterer eksempelvis skibes og havnes operationelle systemer, hvis det lykkes dem at få adgang hertil. En

amerikansk havnefacilitet blev eksempelvis i december 2019 angrebet med ransomwaren Ryuk. Angrebet lammede ofrets operationelle systemer og lukkede facilitetens drift i 30 timer.

Virksomheder i det Blå Danmark ramt af ransomware
DFDS blev i december 2019 ramt af et ransomwareangreb hos et opkøbt udenlandsk selskab. Det opkøbte selskabs systemer var ved at blive udfaset og overført til moderselskabet. Kriminelle hackere nåede imidlertid at finde en svaghed i datterselskabets systemer. Her installerede hackerne en ransomware kaldet Zeppelin. Angrebet nåede dog ikke ind til moderselskabet. Det var således kun datterselskabets systemer, der blev låst. DFDS afværgede de værste konsekvenser af angrebet ved at bruge backup samt fremrykke overgangen til nye systemer.

Den nordjyske pumpeleverandør DESMI blev i april 2020 ramt af et målrettet ransomwareangreb. Hackerne fik først adgang til DESMI's it-systemer via en mail med en inficeret fil. Efter hackerne havde fået adgang, brugte de en uges tid inde i systemerne til at forberede angrebet med ransomware. Først herefter låste hackerne systemerne og sendte en besked med krav om løsesum, som DESMI nægtede at betale.

DESMI oplevede, at kommunikationssystemerne var utilgængelige, mens hændelsen stod på. Systemerne måtte genetableres og hovedsystemerne var tilgængelige igen efter fire dage. De øvrige systemer blev genetableret i løbet af 30 dage.

"Jeg troede, vi var godt beskyttet. Den 3. april fortalte jeg bestyrelsen, at der ikke var nogle huller." Den 8. april låste hackere virksomhedens systemer. Fra interview med Henrik Sørensen, CEO DESMI i Shippingwatch 14. april 2020.

Enklere former for ransomwareangreb har været en udbredt trussel i en årrække. De enkle ransomwareangreb distribueres typisk via phishing. Hvis modtageren klikker på links i mailen eller åbner inficerede filer, installeres ransomwaren, der automatisk låser computer og tilknyttede systemer og enheder. Denne type angreb fanges ofte af opdateret virusbeskyttelse. Men hvis modtageren befinder sig på et sårbart netværk, kan et angreb have alvorlige konsekvenser. Det har der været flere eksempler af på skibe. Teknikere og samarbejdspartnere overfører ofte opdateringer via USB-indgange, når skibene er i havn rundt om i verden. Ransomware har eksempelvis spredt sig fra en skibsførers PC til et skibs operationelle systemer, hvilket medførte at skibets strømforsyning var lukket ned i tre dage.

BEC – Business e-mail compromise
Bedrageri og svindel, hvor kriminelle snyder ofre til at overføre penge til fremmede bankkonti, er en anden indtægtskilde. Nogle af disse svindlere bruger cyberangreb i deres bedrageri. Ved såkaldt Business e-mail compromise, BEC, kompromitterer og overvåger svindlerne eksempelvis

typisk ofrenes e-mail. Kriminelle rammer også søfartssektoren med denne type svindel.

Truslen kommer både fra svindlere, der går efter virksomheder på tværs af samfundet, og fra grupper, der har specialiseret sig i søfart.

Gold Galleon – cybersvindlere med fokus på søfart
I 2018 afslørede en it-sikkerhedsvirksomhed en kriminel gruppe fra Nigeria kaldet Gold Galleon. Gold Galleon har specialiseret sig i at kompromittere mailkorrespondenser mellem maritime partnere. De overvåger dialogen og udskifter bankkontonumre, når penge overføres, f.eks. til en agent eller havn.

Danske virksomheder har sandsynligvis været mål for Gold Galleon. En medarbejder hos rederiet Clipper fik i 2019 en mail fra en amerikansk samarbejdspartner, som vakte mistænksomhed. Medarbejderen valgte derfor at tage kontakt til samarbejdspartneren. Men svindlerne havde også kompromitteret telefonforbindelsen og ringede tilbage fra samarbejdspartnerens telefonnummer. I stedet for at tale med sin normale accent havde samarbejdspartneren nu noget, der mindede om en caribisk accent.

Clipper gennemskuede derfor svindlen og de kriminelle havde ikke held med sig i dette angreb. Gold Galleon har dog med samme metoder franarret andre ofre beløb svarende til flere millioner kroner.

Hackere misbruger computerkapacitet
Hackere kompromitterer computere og andre digitale enheder for at misbruge deres kapacitet. Kapaciteten kan give flere indtægtskilder. Den kan bl.a. misbruges til at generere kryptovaluta ved inficering med såkaldte kryptominere. Hackere misbruger også kompromitterede enheder som platform i overbelastningsangreb, såkaldte DDoS-angreb, eller til spredning af spam.

Søfartsvirksomheder er blandt ofrene for denne type misbrug. Det gælder både gennem misbrug af almindelige it-systemer og enheder som routere og servere, men også søfartsspecifikke systemer er blevet misbrugt.

I 2018 blev antennekontrolenheden på en udbredt satellitkommunikationsterminal på et skib ifølge et it-sikkerhedsfirma inficeret med malwaren Mirai. Mirai bliver brugt til at opbygge såkaldte botnet med tusindvis af enheder. Kontrolenheden blev sandsynligvis kompromitteret, fordi rederiet benyttede sig af standardkodeord.

I december 2019 blev en sårbarhed i webapplikationen til fjernkontrol af yachter offentliggjort. Få dage senere udnyttede hackere sårbarheden til at installere Mirai malware på fjernkontrolsystemerne.

Der findes eksempler på, at hackere utilsigtet har forstyrret funktionen af enheder i et botnet, fordi de ikke har overblik over konsekvenserne af deres hacking. I 2016 anvendte en hacker f.eks. 900.000 hjemmeroutere fra et Mirai-botnet i et DDoS-angreb. Angrebet var rettet mod en teleudbyder i

Liberia. Det endte med ved en fejl i to døgn at afbryde internetforbindelsen for de 900.000 kompromitterede kunder hos Deutsche Telekom.

Hackere går efter persondata
En anden indtægtskilde for hackere er at stjæle og sælge persondata, der kan misbruges af andre kriminelle. Organisationer i søfartssektoren har flere typer data, som kan være interessant for kriminelle. Passagerskibsrederier har eksempelvis en større mængde data på passagerer, samarbejdspartnere og personale.

Stena Lines, Norwegian Cruise Line og Carnival Cruises har de senere år alle fået hacket systemer med sensitive data. Eksempelvis blev data fra Norwegian Cruise Line med knap 30.000 rejseagenters loginoplysninger udbudt på kriminelle internetfora i marts 2020.

Angreb med maritimt tema
Den største cyberkriminelle trussel mod søfartssektoren kommer som nævnt fra opportunistiske angreb rettet mod ofre på tværs af samfundet. Men der findes kriminelle, såsom Gold Galleon, der specialiserer sig i angreb mod sektoren. Ligesom nogle af de, der hacker virksomheder på tværs af samfundet, i perioder går målrettet efter søfartssektoren.

De senere år er der set flere phishingangreb rettet mod søfartssektoren. I 2018 udgav hackere sig eksempelvis for at være brancheorganisationen Danske Rederier og sendte mails til medlemsvirksomhederne. De kriminelle efterspurgte loginoplysninger til medlemssektionen af Danske Rederiers hjemmeside.

I 2019 udsendte den amerikanske kystvagt en advarsel om en igangværende kampagne. Skibe med rute mod amerikanske havne modtog mails, hvor bagmændene udgav sig for at være havnemyndigheder. I de mails efterspurgte bagmændene følsom information inklusiv indholdet i havneindrapportering, notice of arrival NOA.

Ligeledes i 2019 modtog skibe under sejlads i Nordsøen sandsynligvis phishingbeskeder i skibenes telex. Telexbeskederne var målrettet kommunikationskanalen og havde et maritimt tema.

Endelig er der også eksempler på, at stærke søfartsbrands, som A.P. Møller Mærsk, misbruges i phishingangreb for at skabe falsk tillid til afsenderen.

Cyberspionage

Stater spionerer mod dansk søfart
Der er en **MEGET HØJ** trussel fra cyberspionage. Det betyder, at det er meget sandsynligt, at organisationer i søfartssektoren i Danmark vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Statsansatte hackere og hackergrupper med tilknytning til stater udfører cyberspionage. Staternes motiver for spionage mod søfartssektoren kan opdeles i to hovedformål. Dels udspionerer staterne for at kunne fremme deres egen industri og økonomi. Dels udspionerer staterne for at opnå sikkerhedspolitisk relevant viden, fra den helt overordnede strategiske viden til viden relevant for militær planlægning.

På verdensplan har der været en lang række angreb i søfartssektoren med karakter af cyberspionage. Ofrene har været en bred vifte af søfartsorganisationer lige fra forskningsinstitutioner, over udstyrsleverandører til værfter og rederier.

Som stor søfartsnation er der mange potentielle angrebsmål i Danmark. Danske organisationer i sektoren rammes jævnligt af hackerangreb, der sandsynligvis har til formål at understøtte cyberspionage.

Truslen er især rettet mod højteknologiske udstyrsleverandører, søfartsmyndigheder, store internationale rederier samt havne og havneterminaler, der er en del af den kritiske infrastruktur i Danmark eller udlandet.

Statslige hackere stjæler informationer til egen industri
Nogle stater bruger hackere til at kompromittere virksomheder i udlandet for at stjæle værdifuld information om teknologi og anden intellektuel ejendom. Staterne kan også have interesse i andre kommercielle forretningshemmeligheder. Det kan f.eks. være oplysninger i forbindelse med udbud eller indgåelse af kontrakter.

Staterne kan bruge den stjålne information til at understøtte udviklingen af deres egen nationale sektor. Med tyveri af den rette viden kan landets egne virksomheder eksempelvis springe flere led af deres innovations- og udviklingsproces over.

Både Rusland og Kina råder over meget væsentlige cyberkapaciteter og begge lande bruger deres kapaciteter aktivt på globalt plan.

Kina har i sin strategi Made In China 2025 udpeget havteknologi og højteknologiske skibe som ét af ti prioriterede industriområder. Kina sigter mod at blive globalt førende inden for feltet i 2025.

Særlig interesse i dual-use teknologi
Truslen mod søfart hænger også sammen med truslen fra cyberspionage mod forsvarsindustrien, der også er **MEGET HØJ**. Det skyldes at der inden for

søfart anvendes teknologi og udstyr, der både kan bruges civilt og milliært, såkaldt dual-use teknologi.

En stor del af det operationelle udstyr på skibe såsom navigations- og kommunikationsudstyr bruges eksempelvis både på kommercielle skibe og flådefartøjer. Tyveri af viden om dual-use teknologier kan potentielt dække både kommercielle og sikkerhedspolitiske behov hos fremmede stater på samme tid.

Nogle lande, der har en væsentlig cyberkapacitet, har endda et særligt fokus på dual-use teknologi på forsvarspolitisk niveau. Som led i moderniseringen af Kinas forsvar er der eksempelvis et erklæret mål om "civil og militær fusion" ("junmin ronghe") med fokus på bl.a. dual-use teknologier. I Rusland er udviklingen af dual-use teknologier også et erklæret mål for landets militære udviklingsorganisation Fonden for Avanceret Forskning (FPI).

Stater spionerer mod samarbejdspartnere
Nogle stater benytter sig af cyberspionage for at opnå indsigt i udenlandske samarbejdspartneres strategier og hensigter. Samarbejdspartnerne kan både være myndigheder i andre lande og udenlandske virksomheder med store aktiviteter i efterretningstjenestens hjemland.

Dansk søfarts position som maritim stormagt med betydelige aktiviteter globalt medfører, at danske søfartsvirksomheder og myndigheder kan blive mål for denne type cyberspionage. I tekstboksen herunder er et udpluk af eksempler på danske aktiviteter i Rusland og Kina, som kan motivere til cyberspionage.

Eksempler på dansk søfarts aktiviteter i Rusland og Kina
Maersk Line gennemførte i 2018 som det første containerrederi nogensinde en sejlads med Venta Maersk af nordøstpassagen i samarbejde med Ruslands atomdrevne isbryderselskab. Sejladsen havde stor bevågenhed, og nordøstpassagen er en topprioritet for præsident Putin. Generelt er Arktis et område med stor interesse fra flere stormagter, herunder Rusland og Kina.

APM Terminals ejer og driver i samarbejde med lokale partnere 74 havneterminaler rundt om i hele verden. Heraf er syv havneterminaler placeret i Kina og fem i Rusland. Havnene er strategisk placeret og en del af landenes kritiske infrastruktur.

Skibe fra danske rederier er blandt dem, der fragter flest containere ud af Kina. Derfor spiller danske rederier en vigtig rolle for Kinas eksport af varer. Samtidig blev 73 af de 100 skibe, der var på ordre fra danske rederier i 2018, bygget på kinesiske værfter.

Overvågning af skibsfart og logistik
Statslige hackere står også bag kompromitteringer af it-systemer på skibe. Herved kan der eksempelvis opnås indsigt i, hvor skibene befinder sig, og hvad de fragter. Særligt leverancer af militære forsyninger kan have fremmede landes interesse. Skibsadgangen kan også bruges som trædesten til rederiets centrale systemer.

Havne, logistik- og shippingvirksomheder kan på samme måde være mål for cyberspionage. I forbindelse med militære konflikter kan den rolle civile virksomheder i sektoren spiller for forsyningssikkerhed og støtte til militæret ændres. Skibe, havne og logistikvirksomheder kan blive kritiske, ikke kun for samfundet men også militært. Et formål med cyberspionage mod virksomhederne kan være at opbygge kapacitet til at gennemføre destruktive cyberangreb. Adgang og erfaringer vil kunne misbruges i forbindelse med en konflikt.

Leverandører som trædesten
Leverandører og samarbejdspartnere til vigtige myndigheder og virksomheder kan også blive udsat for forsøg på cyberspionage uden selv at være målet. Hackere angriber organisationer for at bruge dem som trædesten til at kompromittere kunder og samarbejdspartnere, der er interessante for den fremmede stat.

Målet med det enkelte cyberangreb er derfor ikke altid at skaffe konkret viden. Det kan også være at skaffe en specifik adgang. Visse underleverandører eller samarbejdspartnere har måske ikke en viden, der er interessant for fremmede lande. De kan til gengæld have en adgang eller troværdighed, hackerne kan udnytte til at kompromittere deres egentlige mål.

Cyberaktivisme

Truslen fra cyberaktivisme mod søfartssektoren er **MIDDEL**. Det betyder, at der er muligt, at søfartssektoren vil blive ramt af aktiviske cyberangreb inden for de næste to år.

CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine.

Når trusselsniveauet for cyberaktivisme hæves på grund af konkrete aktiviteter udført af pro-russiske cyberaktivister i forbindelse med krigen i Ukraine, betyder det ligeledes, at niveauet kan ændre sig igen med kort varsel afhængigt af krigens udvikling.

Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en sag. Cyberaktivisternes angrebsmetoder varierer meget i kompleksitet – fra relativt simple overbelastningsangreb, såkaldte DDoS-angreb, til mere ressourcekrævende hack og læk af information fra myndigheder og virksomheder.

Cyberaktivistiske angreb dækker således over en mangfoldig gruppe af aktiviteter, der spænder fra opportunistiske angreb til mere organiserede kampagner. En fællesnævner på tværs af dette spektrum er dog, at mens angrebene ofte er en reaktion på specifikke begivenheder, så findes der en kontinuitet i de temaer såsom klima og dyrevelfærd, som de forskellige aktivister forfølger.

Truslen fra simple angreb kan komme til udtryk, hvis danske myndigheder eller virksomheder kommer i aktivisternes søgelys. Tekstboksen beskriver et forsøg på et overbelastningsangreb mod A.P. Møller Mærsk i maj 2020. Det er et eksempel på, at truslen hurtigt kan komme til udtryk og at angreb kan gennemføres med enkle midler.

COVID-19 skubber klimaaktivister mod cyberangreb
Corona-nedlukningen af samfundet i foråret 2020 havde også betydning for miljøaktivister. Klimagruppen Extinction Rebellion gennemførte den 10. marts 2020, dagen inden Danmark blev lukket ned, en protestaktion i Folketingssalen. Men under nedlukningen besluttede gruppen sig for at lave virtuelle protester i form af cyberangreb i stedet.

Gruppen gennemførte ifølge deres eget nyhedsbrev i maj 2020 meget simple overbelastningsangreb mod en række virksomheder. Virksomhederne, heriblandt A.P. Møller Mærsk, var udvalgt, fordi aktivisterne mente, at virksomhederne havde en for høj udledning af CO2.

Aktivisterne benyttede sig af et let tilgængeligt værktøj. Fra deres hjemmecomputere sendte aktivisterne tusindvis af beskeder med dele af FN's klimarapport til virksomhedernes hjemmesider. Aktivisterne ville overbelaste hjemmesiderne og få dem til at lukke ned.

Destruktive cyberangreb

Der er en **LAV** trussel fra destruktive cyberangreb. Det betyder, at det er mindre sandsynligt, at virksomheder og myndigheder i søfartssektoren i Danmark vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Det skyldes, at det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at rette destruktive cyberangreb mod Danmark. Stater står bag langt den overvejende andel af destruktive cyberangreb.

CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade eller betydelig skade på fysiske objekter. Definitionen dækker også ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Langt de fleste af de destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data. Enten ved at hackeren har slettet eller krypteret data uden mulighed for at genskabe dem. Destruktive cyberangreb er selv inden for denne brede definition relativt sjældne.

Aktiviteter i konfliktområder kan højne truslen
I konfliktområder, hvor stater bruger destruktive cyberangreb mod civile mål, kan truslen for destruktive cyberangreb være højere. Dansk søfart er global, og derfor kan danske søfartsvirksomheder blive ramt af angreb, der ikke er rettet mod Danmark, men mod virksomheder der opererer i konfliktområder.

Under konflikten mellem Ukraine og Rusland har der været flere tilfælde af destruktive cyberangreb i Ukraine. NotPetya-angrebet i 2017, der bl.a. ramte A.P. Møller Mærsk, var netop rettet mod virksomheder med aktiviteter i Ukraine. Hackere leverede NotPetya-malwaren til virksomheder gennem en softwareopdatering til et skattebetalingsprogram.

Truslen kan også stige, hvis søfartsvirksomheden arbejder for virksomheder eller stater, der er mål for destruktive cyberangreb. I 2018 blev den italienske olie- og gasvirksomhed Saipem, som bl.a. opererer en række specialfartøjer, udsat for et målrettet destruktivt cyberangreb. Angrebet skete med varianter af den samme malware, der har været brugt i tidligere angreb mod det saudiarabiske olieselskab Saudi Aramco, som Saipem er leverandør til. Det destruktive cyberangreb, der ramte Saipem, slettede data på flere hundrede af virksomhedens computere rundt om i verden.

Søfartssektoren kan også blive berørt af følgevirkning af destruktive cyberangreb. Israel og Iran oplevede hen over foråret og sommeren 2020 en række cyberangreb mod deres kritiske infrastruktur. Landene har indbyrdes beskyldt hinanden for at stå bag angrebene. Et af angrebene ramte i maj 2020 havnen i Bandar Abbas i Iran. Angrebet påvirkede driften af havnen og medførte forsinkelser for skibe, der benyttede havnen.

Maritime udstyrsleverandører er som nævnt særligt udsat for cyberspionage. Hackere kan potentielt udnytte kompromitterede udstyrsleverandører som trædesten til at udføre destruktive cyberangreb mod operationelle systemer på skibe. Det kan eksempelvis ske via angreb forklædt som legitime opdateringer af systemerne.

Konsekvenserne af denne type angreb kan blive betydelige, hvis det eksempelvis sker gennem en motorproducent, en leverandør af navigationsudstyr eller lignende kritisk udstyr.

Cyberterror

Der er **INGEN** trussel fra cyberterror. Det betyder, at det er usandsynligt, at organisationer i søfartssektoren i Danmark, 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.

Så 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 sandsynligheder i analyser