CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod danske havne og logistikvirksomheder

1. udgave april 2023

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave april 2023.

Cybertruslen mod danske havne og logistikvirksomheder

Formålet med denne trusselsvurdering er at beskrive cybertruslen mod de danske erhvervshavne og logistikvirksomheder. Vurderingen kan bl.a. indgå som en del af grundlaget for havnenes og virksomhedernes risikovurderinger på cybersikkerhedsområdet. Målgruppen for trusselsvurderingen er primært ledelsen og it-medarbejdere hos de danske havne og logistikvirksomheder.

Hovedvurdering

- Truslen fra cyberspionage mod danske havne og logistikvirksomheder er **MEGET HØJ.** Truslen fra cyberspionage fører løbende til cyberangreb mod danske mål, herunder havne og logistikvirksomheder.

- Truslen fra cyberkriminalitet mod danske havne og logistikvirksomheder er **MEGET HØJ.** Den mest alvorlige trussel fra cyberkriminalitet kommer fra ransomware-angreb, men havne og logistikvirksomheder oplever også et højt antal forsøg på spear phishing og BEC-scams.

- Truslen fra cyberaktivisme mod danske havne og logistikvirksomheder er **HØJ.** Truslen udgår særligt fra pro-russiske hackere, der har øget deres aktivitetsniveau efter Ruslands invasion af Ukraine, og løbende rammer mål i Vesten – også i Danmark. Det er sandsynligt, at særligt aktivistiske hackere vil gå efter mål i Danmark, herunder havne og logistikvirksomheder.

- Truslen fra destruktive cyberangreb mod danske havne og logistikvirksomheder er **LAV**. Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark, herunder danske havne og logistik-virksomheder. CFCS vurderer dog, at hackergrupper tilknyttet fremmede stater forbereder sig for at kunne udføre destruktive cyberangreb mod danske mål med kort varsel.

- Truslen fra cyberterror mod danske havne og logistikvirksomheder er **INGEN.**

Indledning

Trusselsvurderingen beskriver den cybertrussel, der er rettet imod havne og logistikvirksomheder i Danmark. Trusselsvurderingen gælder for alle erhvervshavne i Danmark, uanset ejerforhold. Lystbådehavne er ikke medtaget. Logistikvirksomheder er virksomheder, hvis kerneforretning er at fragte gods og varer for kunder. I Danmark foregår hovedvægten af denne fragt via vej eller bane, men der er også logistikvirksomheder, der transporterer via fly. Vurderingen omfatter ikke den trussel, der er imod de anvendte transportmidler f.eks. fly, toge og lastbiler, men udelukkende imod logistikvirksomhederne og deres systemer. Søfart er ikke medtaget i trusselsvurderingen, da søfart behandles som en selvstændig sektor af danske myndigheder.

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. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Vurderingen tager afsæt i analyser af danske og internationale eksempler på cyberangreb mod havne og logistikvirksomheder. Det sammenholdes med viden om trusselsaktørers kapacitet og intention. Trusselsvurderingen er udarbejdet bl.a. på baggrund af dialog med flere havne og logistikvirksomheder i Danmark.

Den største trussel mod havne og logistikvirksomheder i Danmark er cyberspionage og cyberkriminalitet. Her udgør cyberspionage en alvorlig trussel, da havne og logistikvirksomheder kan være i besiddelse af kritiske informationer, ikke kun for samfundet men også for Forsvaret. Det kan derfor medføre, at fremmede stater får adgang til informationer af sikkerhedspolitisk betydning for Danmark.

Derudover udgør cyberkriminalitet en alvorlig trussel for havne og logistikvirksomheder i Danmark. Her er ransomware den mest alvorlige trussel, da ransomware-angreb fortsat er en udbredt angrebsmetode på tværs af de samfundsvigtige sektorer. Et ransomware-angreb kan desuden få store økonomiske konsekvenser for de danske havne og logistikvirksomheder, derudover kan angreb også i yderste tilfælde forstyrre leveringen af samfundsvigtige ydelser.

Havne og logistikvirksomheder er centrale for de danske forsyningskæder
Covid-19 pandemien viste, at fødevaremangel og mangel på nødvendige forsyninger af f.eks. medicin og teknologi er en reel bekymring hos den danske befolkning. Da krisen brød ud, viste nyhederne billeder fra dagligvarebutikker, hvor danskere hamstrede toiletpapir, håndsprit og gær, og flere dagligvarebutikker meldte udsolgt på almindelige husholdningsartikler. Derudover blev leverancetiden af nye biler og elektronik forhøjet markant, og det blev tydeligt, at en løbende forsyning til de danske forbrugere er vigtig for det danske samfund.

Desuden er Danmark verdens sjettestørste søfartsnation målt på opereret tonnage. Omkring 780 handelsskibe er danskflagede og knap 2.000 skibe opereres fra Danmark. Med mere end 100.000 årlige skibsanløb sikrer erhvervshavnene rundt om i Danmark forsyninger til landet. 70 procent af den danske import fragtes gennem havnene. Det er derfor vigtigt, at de danske havne og logistikvirksomheder er robuste overfor cyberangreb, som i værste fald kan få konsekvenser for den danske forsyning af varer og gods.

Endelig har krigen i Ukraine vist, at en stabil forsyningskæde kan blive et vigtigt element i en krisesituation, og at havne og logistikvirksomheder spiller en helt central rolle i forhold til at sikre den nødvendige forsyning af varer og udstyr til forsvaret.

Den teknologiske udvikling kan få stor betydning for sektoren
Mange havne og logistikvirksomheder i Danmark er opstået i en tid, hvor digitale løsninger og it-drevne systemer ikke var en del af den daglige drift. Derfor er den teknologiske udvikling i virksomhederne sket gradvist og indenfor de seneste år. Det betyder, at eksempelvis flere havne fortsat er i stand til at overgå til manuel drift i tilfælde af it-nedbrud eller hackerangreb.

I takt med at den teknologiske udvikling gør havne og logistikvirksomheder mere afhængige af digitale løsninger, opstår der imidlertid nye angrebsflader for hackere. Arbejdsgange og systemer, der tidligere har været personafhængige og analoge, er i stigende grad forbundet til eller styret af it-systemer, hvilket hackere i værste fald kan udnytte til at angribe. Det kan resultere i store økonomiske tab, tab af omdømme for virksomhederne eller afbrydelse af samfundsvigtig infrastruktur.

Cyberspionage

Truslen fra cyberspionage mod havne og logistikvirksomheder i Danmark er **MEGET HØJ**. Det er meget sandsynligt, at havne og logistikvirksomheder i Danmark vil blive udsat for cyberspionage inden for de næste to år. Truslen fra cyberspionage er vedvarende og fører løbende til cyberangreb mod danske mål, herunder havne og logistikvirksomheder.

CFCS vurderer, at der inden for de seneste år har været en forhøjet cyberspionage-aktivitet rettet mod havne og logistikvirksomheder, både i Danmark og i udlandet.

Havne og logistikvirksomheder er centrale under en militær konflikt
Den alvorlige trussel fra cyberspionage skyldes, at fremmede stater, herunder især Rusland og Kina, har en særlig interesse for viden om udenrigs-, sikkerheds- og forsvarspolitik. Spionage mod havne og logistikvirksomheder kan derfor være motiveret af sikkerhedspolitiske interesser, eksempelvis viden relateret til NATO eller det arktiske område.

I forbindelse med militære konflikter kan den rolle, civile virksomheder i sektoren spiller for forsyningssikkerhed og støtte til forsvaret, ændres. Havne og logistikvirksomheder kan blive kritiske, ikke kun for samfundet men også for Forsvaret. I det omfang at havne eller logistikvirksomheder støtter dansk forsvar eller andre landes militær, eksempelvis transport af militært personel til missioner i udlandet eller militær brug af civile trafikknudepunkter, kan dette altså have fremmede staters interesse.

Indhentning af information om havne og logistikvirksomheder, som er en del af dansk kritisk infrastruktur, kan også benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.

Havne og virksomheder kan pludseligt blive oplagte spionagemål
Selvom havne eller logistikvirksomheder ikke tidligere har oplevet cyber- spionage, eller anser sig selv som oplagte mål for cyberspionage, kan dette hurtigt ændres. Det kan for eksempel ske, hvis en virksomhed indgår en stor kontrakt med et andet lands forsvar, besidder en central fysisk lokation i forbindelse med en militær øvelse eller er et centralt knudepunkt for ny forskning og innovation.

Eksempelvis har USA vist interesse for at bruge Esbjerg Havn til deployering af allierede styrker til Østersøområdet og Baltikum. Derudover skal Europas største Power-to-X-anlæg planmæssigt opføres i Esbjerg. Anlægget skal omdanne hav-vindmøllestrøm til CO2-fri ammoniak, som kan bruges til gødning og grønt brændstof til skibe.

CFCS vurderer, at Ruslands invasion af Ukraine ikke har medført en ændring i truslen fra cyberspionage mod havne og logistikvirksomheder i Danmark. Tilbagemeldingen fra de fleste danske havne og logistikvirksomheder er, at der ikke har været en mærkbar stigning i antallet af observerede forsøg på cyberangreb siden krigens begyndelse. Det er meget sandsynligt, at Rusland efter invasionen af Ukraine forsat har det samme fokus på at udføre cyberspionage mod myndigheder og organisationer i Danmark, herunder havne og logistikvirksomheder. Endelig kan Ruslands brug af cyberspionage intensiveres, såfremt konflikten mellem NATO og Rusland forværres.

Havne og logistikvirksomheder kan blive trædesten til andre virksomheder
Cyberspionage kan også blive rettet mod havne og logistikvirksomheder, der kan misbruges som trædesten i angreb mod de organisationer, der er de egentlige mål.

Havne og logistikvirksomheder kan være attraktive mål for hackere, da de ofte har en stor berøringsflade med andre store virksomheder, og har kunder på tværs af mange sektorer. Ved blot at kompromittere én havn eller logistikvirksomhed kan en aktør potentielt få mulighed for at bevæge sig på tværs af adskillige kunders netværk og data, og således skabe en adgang til det egentlige offer. Fremmede stater kan dermed potentielt bruge kompromitteringer via logistikvirksomheder eller havne til at få adgang til virksomheder, der f.eks. arbejder med nye teknologier, medicinsk research eller anden omkostningstung forskning.

Endelig har havne og logistikvirksomheder i nogle sammenhænge adgang til oplysninger om vareleveringer, passagerer og rejsemønstre, som fremmede staters efterretningstjenester kan anvende til at følge bestemte personer.

Et setup med mange angrebsflader
I takt med den teknologiske udvikling er cybersikkerheden ikke længere begrænset til IT. Den stigende digitalisering, som moderne samfund undergår, betyder, at det ikke kun er vores informationer, der holder til i det digitale domæne. Store dele af samfundets produktion og drift er nu også forbundet til internettet. Havne og logistikvirksomheder har foruden de centrale IT-systemer, som styrer HR, økonomi og logistikplanlægning, et stort OT-setup forbundet med den fysiske drift. Det kan f.eks. være overvågningskameraer, adgangskontrolsystemer, bomme, kraner, kommunikations- og fejlmeldingssystemer, som ofte er koblet på internetvendte flader. Det betyder, at de danske havne og logistikvirksomheder har mange potentielle angrebsflader.

Det har særligt været debatteret, hvorvidt udenlandske overvågningskameraer kan bruges til cyberspionage. Flere medier har bl.a. rettet opmærksomhed mod den kinesiske teknologivirksomhed, Hikvision, som er kendt for at levere kameraer og teknologi, der bl.a. anvendes af Kina til at overvåge landets indbyggere. På den baggrund vedtog USA i 2019 en lov, der forbyder føderale myndigheder at anvende teknologi fra Hikvision.

De fleste overvågningssystemer indeholder sårbarheder, der potentielt kan give uautoriseret adgang til udstyret. Overvågningskameraer, uanset producent, kan derfor udgøre en sikkerhedstrussel.

IT, OT og IOT – kært barn har mange sårbarheder

Herunder er CFCS' overordnede definitioner på IT, OT og IOT:

IT: Informationsteknologi. IT-systemer omfatter hardware og software og kan være både uafhængige eller forbundet med andre systemer i et netværk.

OT: Operationel teknologi. Systemer, der anvendes til overvågning og styring af mekaniske systemer, herunder industrielle kontrolsystemer (ICS).

IOT: Internet Of Things. Et udtryk for komponenter, der er koblet til internettet. Det drejer sig om alt fra termostater til hverdagsobjekter som f.eks. køleskabe eller kameraer. Når OT-enheder benytter IP-netværk og eventuelt er forbundet via internettet, kaldes det Industrial Internet of Things (IIoT).

Cyberkriminalitet

Truslen fra cyberkriminalitet mod havne og logistikvirksomheder i Danmark er **MEGET HØJ.** Det er meget sandsynligt, at havne og logistikvirksomheder i Danmark vil blive ramt af angreb fra cyberkriminelle inden for to år.

CFCS bruger begrebet cyberkriminalitet som en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse. Særlig ransomware-angreb og BEC-scams udgør en alvorlig trussel for havne og logistikvirksomheder, da ransomware-angreb og BEC-scams fortsat er en udbredt angrebsmetode på tværs af de samfundsvigtige sektorer. CFCS har kendskab til en række ransomware-angreb og forsøg på BEC-scams blandt danske havne og logistikvirksomheder indenfor de seneste år.

Ruslands invasion af Ukraine har skabt flere reaktioner internt i det kriminelle miljø. I Ukraine og Polen har man i oktober 2022 oplevet en række ransomware-angreb rettet mod havne og logistikvirksomheder. CFCS vurderer dog, at invasionen ikke i væsentlig grad har påvirket truslen fra cyberkriminalitet mod Danmark, herunder de danske havne og logistikvirksomheder. Det er også den generelle tilbagemelding blandt de fleste danske havne og logistikvirksomheder, at der ikke har været en reel stigning i antallet af observerede forsøg på cyberangreb.

Uskyldig phishing kan føre til alvorlige ransomware-angreb
Havne og logistikvirksomheder er generelt meget afhængige af mailkorrespondancer. En stor del af virksomhedernes bestillinger og faktureringer af kunder og eksterne forretningspartnere foregår via mail, og phishing og spear phishing er et udbredt fænomen blandt virksomhederne. En virksomhed i sektoren beskriver f.eks., at der ugentligt sendes mere end 1,5 mio. mails alene i deres virksomhed, hvorfor phishing og spear phishing udgør en reel risiko for virksomheden. Risikoen for, at en medarbejder lader sig narre af en phishing-mail, afhænger både af, hvor godt mailen er udformet, og hvilken træning medarbejderen har modtaget i at opdage forsøg på phishing.

Phishing og spear phishing kan bl.a. bruges som den indledende kompromittering i forbindelse med et ransomware-angreb. Og lykkes det de cyberkriminelle at komme ind i nogle af de centrale systemer, kan det have store konsekvenser for virksomhederne. De driftssystemer, som særligt logistikvirksomheder benytter, hvor al logistik- og trafikplanlægning foregår, er i mange tilfælde centrale for virksomhedernes daglige drift. Det betyder, at angreb kan få alvorlige konsekvenser. CFCS har kendskab til flere ransomware-angreb blandt logistikvirksomheder, herunder danske. Og det er sandsynligt, at de cyberkriminelle forventer, at der er en stor chance for, at virksomhederne er villige til at udbetale løsesummer i tilfælde af ransomware-angreb på grund af systemernes kritiske funktion for virksomhedernes drift.

Både i udlandet og i Danmark har der været en del ransomware-angreb bl.a. mod havne og logistikvirksomheder, hvor de cyberkriminelle er kommet ind via phishing. I 2020 blev Port of Kennewick i USA f.eks. ramt af et ransomware-angreb, hvor systemerne blev låst, og havnen mistede adgang til sine servere. De kriminelle kom ifølge åbne kilder ind via phishing, og det tog mere end en uge, før systemerne blev genoprettet.

Mange mails betyder mange forsøg på phishing, spear phishing og BEC-scams
Spear phishing minder om almindelige phishing-forsøg, men adskiller sig ved, at modtagerne ikke er tilfældige, men udvalgte. Hackerne anvender ofte social engineering for at målrette indholdet til den enkelte modtager. Mails er typisk udformet, så de virker særligt relevante, overbevisende og troværdige for modtageren. Det kan eksempelvis være ved at anvende modtagerens navn, personspecifik information eller andre oplysninger, som er fundet ved forudgående rekognoscering. Spear phishing er ofte forstadiet til forskellige typer angreb som f.eks. BEC-scams. CFCS har kendskab til, at flere havne og logistikvirksomheder løbende bliver forsøgt angrebet via spear phishing. For eksempel har Copenhagen-Malmö Port oplevet flere spear phishing-forsøg, hvor medarbejdernes navne og informationer har været en del af angrebsforsøgene.

Bedrageri i form af såkaldte BEC-scams er fortsat en trussel på tværs af sektorer. BEC-scams har til formål at franarre virksomheder og myndigheder penge via bedrageriske mails, der indeholder instrukser om at gennemføre pengeoverførsler til de kriminelle. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også CEO-fraud eller direktørsvindel. BEC-scams kan medføre betydelige økonomiske tab for den berørte virksomhed eller myndighed.

CFCS kender til flere forsøg på BEC-scams blandt de danske havne og logistikvirksomheder. Blue Water Shipping har eksempelvis oplevet, at en højtstående medarbejder i Australien modtog en betalingsanmodning fra en højtstående medarbejder i Danmark via WhatsApp. Medarbejderen reagerede dog hurtigt, og angrebet blev afværget. Derudover fortæller Kalundborg Havn, at de har været udsat for et sofistikeret forsøg på CEO-fraud, hvor den berørte medarbejders navn fremgik samt central viden om medarbejderens kalender. Også her blev angrebet afværget.

Logistikvirksomhedernes gode navn misbruges af kriminelle

Flere logistikvirksomheder fortæller, at deres navn er blevet misbrugt i forbindelse med ikke-cyberrelateret økonomisk svindel af privatpersoner.

I svindelnummeret har kriminelle taget kontakt til deres offer i forbindelse med køb og salg af dyre varer, som f.eks. motorcykler mv. Derefter har de kriminelle henvist til en falsk hjemmeside, som til forveksling har lignet virksomhedernes legitime hjemmeside, og fået ofrene til at indtaste deres betalingsoplysninger. Herefter har de kriminelle høstet oplysningerne og misbrugt kundens informationer.

Logistikvirksomhederne fortæller, at de løbende holder øje med nyoprettede domæner, der har overlap til deres virksomheder. Virksomhederne beretter desuden, at det er et stort problem, da de i sidste ende kan få negative konsekvenser for deres omdømme blandt kunderne. Selvom disse svindelnumre ikke kan kategoriseres som cyberangreb, så viser de, at de kriminelle hackere har et fokus på havne og logistikvirksomheder generelt.

Cyberaktivisme

Truslen fra cyberaktivisme mod havne og logistikvirksomheder i Danmark er **HØJ**. Det er sandsynligt, at havne og logistikvirksomheder i Danmark vil blive ramt af et cyberaktivistisk angreb inden for de næste to år.

CFCS hævede d. 31. januar 2023 trusselsniveauet for cyberaktivisme fra **MIDDEL** til **HØJ**, bl.a. på baggrund af pro-russiske aktivistiske hackergruppers høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet.

Når trusselsniveauet for cyberaktivisme er **HØJ** grundet 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.

Cyberaktivister opfordrer til angreb mod havne og logistikvirksomheder
Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag eller symbolske mål.

Med krigen i Ukraine er der opstået aktivistiske miljøer, der på sociale medier som den russisk-udviklede applikation Telegram opfordrer hinanden til og koordinerer udførelsen af aktivistiske cyberangreb mod personer og organisationer, som de opfatter som modstandere af deres sag. Blandt andet har pro-russiske grupper udpeget ukrainske og vestlige virksomheder, de vurderer vil være særligt relevante at angribe. Her har de ad flere omgange opfordret til at ramme havne og logistikvirksomheder. Eksempelvis opfordrede en pro-russisk aktivistgruppe i oktober 2022 til, at andre hackere skulle ramme marineterminaler og logistikvirksomheder i USA med DDoS-angreb.

CFCS har ikke kendskab til, at de pro-russiske cyberaktivister har opfordret til at ramme specifikke danske havne eller logistikvirksomheder. Men da der opfordres til at ramme havne og logistikvirksomheder i andre NATO-lande, er det sandsynligt, at danske havne og logistikvirksomheder også vil blive mål for de cyberaktivistiske hackere.

Kundevendte flader kan være oplagte mål for DDoS-angreb
Cyberaktivistiske hackere benytter sig ofte af DDoS-angreb. DDoS-angreb foregår ved, at hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside eller et netværk. Formålet er at gøre hjemmesiden eller netværket utilgængeligt for legitim trafik, mens angrebet står på. DDoS-angreb kan være alvorlige, hvis de rettes mod kundevendte flader. Det kan i værste tilfælde betyde, at havne og logistikvirksomheder mister potentielle kunder og kørsler, da bestillingerne ikke kan foretages via hjemmesiden.

Desuden kan denne form for angreb have en skadelig effekt på havne- og logistikvirksomheders omdømme i offentligheden, pga. manglende tilgængelighed af de ramte systemer. Det vil i sidste ende også kunne få en effekt på virksomhedernes omsætning.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod havne og logistikvirksomheder i Danmark er **LAV**. Det er mindre sandsynligt, at havne og logistikvirksomheder i Danmark vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Selvom CFCS vurderer, at det er mindre sandsynligt, at fremmede stater aktuelt har intention om at udføre destruktive cyberangreb mod Danmark, er det alligevel sandsynligt, at statsstøttede hackergrupper, særligt fra Rusland, forbereder sig på at kunne udføre destruktive angreb mod kritisk infrastruktur i Danmark. På den måde kan hackergrupperne med kort eller intet varsel iværksætte destruktive angreb, såfremt intentionen skulle ændre sig.

En række lande har cyberkapaciteter, der kan bruges destruktivt mod samfundsvigtig infrastruktur såsom havne og logistikvirksomheder. 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.

Destruktive angreb bruges i forbindelse med konflikter
Siden Rusland invaderede Ukraine i februar 2022, har bekymringen over russiske cyberangreb mod Danmark fyldt meget i den offentlige debat. Den fysiske sabotage mod Nord Stream 1 og 2 gasrørene i Østersøen i september 2022 har styrket en bekymring for, at kritisk dansk infrastruktur bliver en del af konflikten.

Ukraine har i 2022 været ramt af forskellige destruktive cyberangreb. Rusland har ifølge flere IT-sikkerhedsfirmaer udført en række såkaldte wiper-angreb mod ukrainske myndigheder og virksomheder, som har fået slettet data permanent. I Polen og Ukraine blev flere logistikvirksomheder i oktober 2022 ramt af ransomware-lignende angreb, som ifølge Microsoft er udført af den russiske statsstøttede hackergruppe Sandworm. Den gruppe har tidligere udført destruktive cyberangreb både i og uden for Ukraine. Malwaren, som går under navnet Prestige, blev rettet mod flere forskellige logistikvirksomheder på tværs af de to lande og blev udført hen over et tidspænd på få timer. Angrebene viser, at hackergrupper viser interesse for de europæiske logistikvirksomheder, der forestår transport af humanitær og militær assistance til Ukraine.

Det er mindre sandsynligt, at fremmede stater, herunder Rusland, aktuelt har intentioner om at udføre destruktive cyberangreb mod Danmark, herunder danske havne og logistikvirksomheder. Det er dog muligt, at danske myndigheder og virksomheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske logistikvirksomheder, der er til stede i konfliktområder, hvor fremmede stater med kapacitet til at udføre destruktive cyberangreb har interesser, såsom Ukraine eller i Mellemøsten. Eksempelvis blev den iranske havn Sharid Rajai i 2020 ramt af et hackerangreb, som bl.a. ramte de it-systemer, der stod for al logistik af lastbiler, varer og containere.

Destruktive angreb kan sprede sig
CFCS vurderer, at der i forbindelse med konfliktsituationer er en øget risiko for, at destruktive cyberangreb kan sprede sig og ramme ofre uden for selve konfliktzonen. Det er muligt, at danske virksomheder og myndigheder, der er til stede i særligt Ukraine og Mellemøsten, vil blive ramt af destruktive cyberangreb eller følgevirkninger deraf, såsom strømafbrydelser og manglende internetadgang. Størstedelen af de destruktive angreb, som har ramt Ukraine i 2022, har dog været afgrænsede og har ikke spredt sig ud over landets grænser. Det var imidlertid ikke tilfældet med cyberangrebet mod Viasat, en amerikansk udbyder af satellitkommunikation.

På dagen for Ruslands invasion af Ukraine blev Viasat ramt af et wiper-angreb med malware kaldet AcidRain, der blandt andet resulterede i, at tusindvis af satellitmodemmer, særligt i Europa, fik slettet deres opsætning. Danmark har sammen med EU og en række nære allierede offentligt udtrykt, at Rusland stod bag angrebet, og at Rusland var velvidende om, at angrebet ville have destruktive konsekvenser også uden for Ukraine. Angrebet havde sandsynligvis til formål at besværliggøre det ukrainske forsvars evne til at kommunikere. Angrebet mod Viasat viste, hvordan destruktive cyberangreb kan have konsekvenser for mange andre end det umiddelbare offer.

Flere havne og logistikvirksomheder er blevet ramt af destruktive cyberangreb, som var rettet mod andre ofre. I juni 2017 blev flere virksomheder i transportsektoren eksempelvis ramt af NotPetya-angrebet, der var et destruktivt cyberangreb forklædt som ransomware. Logistikvirksomhederne FedEx og Deutsche Post DHL Group og DAMCO blev bl.a. ramt med store økonomiske tab.

I Danmark betød NotPetya-angrebet, at Aarhus Havn oplevede udfordringer. Havnen undgik imidlertid stor kødannelse blandt lastbilerne, da der hurtig blev kommunikeret ud til vognmændene, at de ikke skulle møde op på havnen efter de aftalte transporter.

Stater udvikler løbende deres kapacitet til at udføre destruktive cyberangreb
CFCS vurderer, at fremmede stater løbende udvikler deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel. Stater bruger bl.a. cyberspionage til at forberede destruktive cyberangreb, der f.eks. vil kunne iværksættes i tilfælde af en eskalerende krise eller krig.

Cyberspionage kan give adgang til kritisk infrastruktur, som stater kan forsøge at ødelægge eller forstyrre i en alvorlig krise eller krig.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder. Ved at opnå viden om organisationer og systemer kan hackere udvikle specialiseret malware. Derudover kan hackere etablere såkaldte bagdøre på kompromitterede systemer, som de kan benytte i senere destruktive angreb.

Cyberterror

Truslen fra cyberterror mod havne og logistikvirksomheder i Danmark er **INGEN**.
Det er usandsynligt, at danske havne og logistikvirksomheder 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.

CFCS vurderer, at militante ekstremister har begrænset hensigt til at udføre cyber-angreb med samme effekt som konventionel terror, samt at de ikke har den fornødne kapacitet.

Konventionel terror er mere effektiv end cyberterror
Selvom der er en alvorlig trussel fra konventionel terror, og militante ekstremister i årevis har udnyttet internettet til at understøtte deres aktiviteter, planlægge konventionel terror og udføre simple aktivistiske cyberangreb som DDoS-angreb og defacement, har der endnu ikke været nogen eksempler på, at terrorister har udført cyberangreb med en effekt, der svarer til konventionel terror.

Blandt de danske havne er der også højere bevidsthed om truslen fra konventionel terror end truslen fra cyberterror, og de fleste havne nævner ISPS-kravene (den Internationale Maritime Organisations krav om sikring af havnefaciliteter) som en central del af deres sikkerhedsbillede.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.

FE bruger denne skala for sandsynligheder i analyser:

En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed.
"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.