CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod hjælpemidler til navigation

1. udgave november 2022

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave november 2022

Cybertruslen mod hjælpemidler til navigation

Denne trusselsvurdering har til formål at give danske myndigheder og operatører af hjælpemidler til navigation indsigt i de cybertrusler, som er rettet mod dem. Vurderingen supplerer trusselvurderingen mod søfart og havne samt trusselsvurderingen mod skibes operationelle systemer.

Hovedvurdering

- Der er en **HØJ** trussel fra cyberangreb mod hjælpemidler til navigation. I denne vurdering omfatter hjælpemidler til navigation både benyttet specialudstyr samt myndighedernes underlæggende it-infrastruktur.

- Kriminelle hackere angriber virksomheder og myndigheder på tværs af samfundet. De kan også ramme de organisationer og it-systemer, som leverer hjælpemidler til navigation.

- Stater kan også udgøre en trussel mod systemerne. Det er muligt, at staterne eksempelvis har interesse i viden om militære skibes sejladsmønstre og fragt af eksempelvis militært udstyr og forsyninger.

- I en konfliktsituation kan fremmede stater have interesse i at manipulere eller ødelægge systemerne for at forstyrre sejladsen i de danske farvande.

- Leverandører af udstyr, der bruges som hjælpemidler til navigation, kan misbruges som trædesten i angreb mod hjælpemidlerne.

Indledning

Der sejler årligt omkring 70.000 skibe gennem de danske stræder. Mange af disse er dybgående tankskibe til og fra Østersøen. Det gør de danske farvande til nogle af de mest trafikerede i verden.

En række tjenester, der tilsammen kaldes hjælpemidler til navigation, støtter navigatører og skibe med at sikre en høj sejladssikkerhed gennem farvandene til gavn for sikkerhed og miljø.

Hjælpemidler til navigation

The International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) er den internationale organisation på området. IALA beskriver "aids to navigation" (ATON) som "a device, system or service, external to vessels, designed and operated to enhance safe and efficient navigation of individual vessels and/or vessel traffic".

Begrebet omfatter både analoge hjælpemidler som fyrtårne og afmærkninger (bøjer) og mere teknologiske og digitale tjenester såsom navigationsadvarsler og Vessel Traffic Service (VTS). Begrebet kan bredes ud og også omfatte farvandsovervågning, lodstjeneste, positioneringstjenester, søkortopdateringer, meteorologiske meldinger, Efterretninger for Søfarende, kommunikationskanaler mv.

Til at generere og levere hjælpemidlerne benytter myndighederne sig af forskelligt operationelt specialudstyr og særlige it-systemer. Men myndighederne er i høj grad også afhængige af almindelige administrative it-systemer for at opretholde leverancen.

Denne vurdering omfatter hjælpemidler til navigation i den brede opfattelse, det benyttede specialudstyr samt myndighedernes underlæggende it-infrastruktur.

Navigationshjælpemidlerne giver vigtige input til sikker navigation i og gennem de danske farvande. Men hjælpemidlerne har også betydning for resten af landets infrastruktur.

Ved broerne over Storebælt og Øresund og ved Femernforbindelsen findes bemandede Vessel Traffic Service (VTS) centre, som overvåger og rådgiver skibsfarten for at sikre bro og skibe.

Cyberangreb mod de organisationer og systemer, som leverer hjælpemidlerne, kan potentielt forstyrre driften, ligesom data kan blive stjålet. I værste fald kan cyberangreb mod systemerne påvirke skibsfarten og sejladssikkerheden i de danske farvande.

Læs mere om maritime cybertrusler

Information om cybertruslens mulige påvirkning af skibes operationelle systemer findes i vurderingen Cybertruslen mod skibes operationelle systemer. Information om den generelle cybertrussel mod sektoren kan findes i vurderingen Cybertruslen mod søfart og havne. Begge trusselsvurderinger kan hentes på CFCS' hjemmeside.

Cybertruslen fra kriminelle og fremmede stater

CFCS vurderer, at der er en **HØJ** trussel fra cyberangreb mod hjælpemidler til navigation i Danmark. Det betyder, at det er sandsynligt, at det benyttede specialudstyr, som benyttes til at producere hjælpemidlerne samt myndighedernes underliggende it-infrastruktur, vil blive udsat for forsøg på cyberangreb inden for de næste to år.

Truslen kommer hovedsageligt fra kriminelle hackere med økonomisk motiv og fra hackere, som spionerer for fremmede stater.

Kriminelle hackere kan skabe forstyrrelser
CFCS vurderer, at de kriminelle hackere generelt ikke går målrettet efter de organisationer, der producerer og leverer hjælpemidler til navigation. Men de angriber virksomheder og myndigheder på tværs af samfundet. De kan derved også ramme de organisationer og it-systemer, som leverer hjælpemidler til navigation.

Cyberkriminelle benytter sig af en række forskellige angrebsmetoder for at tjene penge på at hacke såsom ransomware-angreb og tyveri af finansielle oplysninger. Fælles for alle cyberangreb er, at de med eller uden hensigt kan forstyrre de it-systemer, som er angrebet.

Målrettede ransomware-angreb er et eksempel på en angrebsmetode, hvor angrebene typisk sker til så stor gene for deres ofre som muligt. 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. De seneste år har der været en stigning i antallet af målrettede ransomware angreb i Danmark. De forekommer nu hyppigt.

Truslen fra kriminelle cyberangreb er primært rettet mod administrative it-systemer. Som nævnt i indledningen er danske myndigheder afhængige af administrative it-systemer for at opretholde leverancer, såsom udsendelse af navigationsadvarsler.

Den meget høje cybertrussel mod sådanne systemer generelt i Danmark udgør derfor også en trussel mod de administrative it-systemer, der bruges til sådanne opgaver. Selve angrebsfladen er dog begrænset, da der er tale om relativt lille gruppe statslige enheder, som stiller hjælpemidlerne til rådighed. Det sænker sandsynligheden for, at enhederne bliver ramt af mere eller mindre tilfældige angreb.

Angreb mod administrative it-systemer kan sprede sig og i værste fald påvirke driften af både administrative og operationelle systemer. Et eksempel på cyberangreb, der har denne effekt, er beskrevet i tekstboksen om et ransomware-angreb mod en amerikansk havn.

Systemer i amerikansk havn slået ud af ransomware
I december 2019 meddelte den amerikanske kystvagt, at en havnefacilitet var blevet krypteret med ransomwaren Ryuk. Hackerne angreb havnen, da en medarbejder havde klikket på et link i en phishingmail.

Hackerne krypterede de administrative it-systemer, men også kritiske industrikontrolsystemer blev krypteret. Det medførte, at offeret ikke havde forbindelse til sikkerhedskameraer, systemer til fysisk adgangskontrol samt systemer til overvågning af kritiske processer.

Havnen måtte lukke ned i mere end 30 timer, før de havde genetableret de kritiske systemer.

Et andet eksempel på en angrebsmetode, der bliver brugt af kriminelle, er såkaldte DDoS-angreb. Disse angreb har til formål at overbelaste offerets systemer, og dermed gøre dem utilgængelige. Nogle cyberkriminelle udfører disse angreb med krav om løsesum, for ikke at gøre det igen. Denne afpresningsmetode kaldes også for RDDoS eller RDoS.

Andre angrebsmetoder benyttet af cyberkriminelle har ikke til hensigt at forstyrre ofrets systemer. Det er eksempelvis tilfældet, når hackere kompromitterer it-systemer og digitale enheder for at misbruge disses kapacitet. Computerkapaciteten bliver bl.a. misbrugt af kriminelle til at udsende spam, generere kryptovaluta eller angribe andre ofre. Der er dog flere eksempler på, at den type angreb utilsigtet har forstyrret offerets it-systemer, hvis hackeren eksempelvis begår en teknisk fejl eller systemerne bliver overbelastet.

Stater kan også udgøre en trussel mod systemerne
Der er en vedvarende trussel fra cyberspionage mod civile og militære myndigheder i Danmark. Truslen er også rettet mod de myndigheder, som leverer hjælpemidlerne til navigation, herunder Forsvaret og Søfartsstyrelsen.

De fremmede staters motiver for at spionere mod myndighederne er bl.a. at stjæle viden af sikkerhedspolitisk relevans. Det er muligt, at fremmede stater har interesse i de enheder og systemer, der leverer navigationsstøtte. VTS håndterer eksempelvis oplysninger om farligt gods og militær skibstrafik, som kan være interessante for nogle stater.

Mange oplysninger om civile skibes sejladsmønstre er typisk offentligt tilgængeligt via AIS-tjenester og derfor mindre interessante mål for cyberspionage.

Systemerne kan blive mål for destruktive angreb i en konflikt
Fremmede stater kan også være interesseret i at opnå adgang til og viden om systemerne for at forberede fremtidige destruktive cyberangreb.

Det er angreb, 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.

Der er på nuværende tidspunkt en lav trussel for destruktive cyberangreb mod Danmark. Men truslen kan stige, hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation.

Som forberedelse til en eventuel fremtidig konflikt kan fremmede stater have interesse i at afsøge, om de kan få adgang til og viden om systemer til hjælpemidler til navigation.

I en konfliktsituation kan hackere i fremmede stater eksempelvis have interesse i at manipulere eller ødelægge systemerne for at forstyrre sejladsen i de danske farvande samt adgangen til Østersøen gennem de danske stræder.

Cyberangreb kan ske via leverandører

Både kriminelle og statsstøttede hackergrupper bruger kompromitterede virksomheder som trædesten til at angribe virksomhedernes kunder. Der er derfor en forbindelse mellem cybertruslen mod hjælpemidlerne til navigation og cybertruslen mod leverandørerne af disse systemer.

Det er ofte internationale leverandører af forsvarsudstyr, som leverer specialudstyr til hjælpemidler til navigation. Det er muligt, at den vedvarende cybertrussel mod forsvarsindustrien internationalt og i Danmark har en afsmittende effekt på cybertruslen mod udstyr, der bruges som hjælpemidler til navigation, idet kompromitteringer af udstyrsleverandørerne kan misbruges i angreb mod brugerne af udstyret.

Angreb kan eksempelvis ske ved at sende en inficeret softwareopdatering fra en it-leverandør ud til kunderne. Den metode blev eksempelvis brugt ved SolarWinds-angrebet i 2020.

Nogle leverandører har desuden fjernadgange direkte til udstyr hos kunderne. Hvis hackere har kompromitteret en leverandør, kan de udnytte sådanne fjernadgange til at angribe kunderne. Det kan være for at stjæle data, lave destruktive cyberangreb eller til eksempelvis at installere ransomware.

Perspektivering: Digitalisering øger vigtigheden af cybersikkerhed

Søfarten er ligesom resten af samfundet i gang med en digitalisering, der kan gøre funktioner på skibe mere automatiske og autonome. Skibene bliver gradvis mere afhængige af teknologi, og myndighedernes hjælpemidler til at støtte mere digitale skibe er også under udvikling under betegnelsen e-Navigation.

I 2020-2021 afprøvede Søfartsstyrelsen eksempelvis virtuelle afmærkninger på udvalgte steder i de danske farvande. Ligeledes er der i Danmark og andre steder i verden testområder for fjernstyrede og endda autonome skibe.

Den øgede afhængighed af teknologi til at sejle skibene kan gøre skibene mere sårbare, hvis hjælpemidlerne til navigation ikke virker, eller hvis data manipuleres. Afhængigheden kan gøre hjælpemidlerne til mere attraktive mål for både kriminelle hackere og hackere med tilknytning til fremmede stater.

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