CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod skibes operationelle systemer

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod skibes operationelle systemer

Formålet med denne trusselsvurdering er at informere myndigheder og rederier om cybertruslen mod operationelle systemer på danskflagede skibe. Cyberangreb kan påvirke de operationelle systemer og derved have negativ indflydelse på sejlads- og skibssikkerheden. Vurderingen supplerer den generelle vurdering af cybertruslen mod søfart og kan bruges som input til rederiernes risikovurdering.

April 2020
1. udgave

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Hovedvurdering

- CFCS vurderer, at den samlede trussel fra cyberangreb mod danske skibes operationelle systemer er **HØJ**.
- De operationelle systemer trues især af finansielt motiverede cyberkriminelle. De har generelt ikke specifik interesse i operationelle systemer på skibe, men angriber opportunistisk mål på tværs af samfundets sektorer.
- Operationelle systemer trues desuden af enkeltpersoner, der af nysgerrighed eller teknisk interesse forsøger at få adgang til disse systemer.
- Trusselsaktører kan udnytte kompromitterede udstyrsleverandører som trædesten til at angribe operationelle systemer på skibe.
- Der er en potentiel trussel fra destruktive cyberangreb udført af statslige aktører mod operationelle systemer på skibe. Truslen kan være højere for skibe, som opererer i bestemte konfliktområder, eller hvis skibets rederi sejler for virksomheder eller stater, der er mål for destruktive cyberangreb.

Indledning

Digitalisering og opkobling gør skibe mere sårbare

Indtil for 15-20 år siden var skibe isolerede enheder, der primært kommunikerede via VHF-radio og en spinkel satellitforbindelse. Operationel teknologi og systemer, der driver fremdrift, navigation, styring m.v., var fysisk isolerede fra internettet. Digitalisering samt billigere og bedre kommunikationsforbindelser til søs har betydet, at skibene ikke længere er isolerede.

De operationelle systemer har typisk været adskilt (segmenteret) fra de internetforbundne administrative netværk og har derfor som udgangspunkt været bedre beskyttet mod angreb. Isoleringen og segmenteringen af operationelle systemer gennembrydes i stigende grad af forbindelser til skibenes administrative systemer og videre til rederikontoret, ligesom udstyrsleverandørerne oftere har adgang til monitorering og opdatering af systemerne.

Operationelle systemer
Operationelle systemer om bord på skibe omfatter i denne vurdering systemer, der tilsammen gør skibet funktionsdygtigt og anvendeligt til sikker sejlads. Det drejer sig eksempelvis om systemer til fremdrift, navigation, styring og kommunikation. Systemerne går ofte under betegnelsen OT - operational technology.

Udviklingen har givet mange forretningsfordele for rederierne og udstyrsleverandørerne, men det muliggør samtidig cyberangreb fra aktører, der udnytter de sårbarheder, som digitaliseringen og opkoblingen bringer. Operationelle systemer er særligt sårbare på skibe, hvis installation af nye systemer eller ændringer i segmenteringen sker uden fokus på cybersikkerhed.

Cyberangreb mod skibes operationelle systemer kan med eller uden hensigt påvirke systemernes funktion og dermed have negativ indflydelse på sejlads- og skibssikkerheden. Derfor er truslen fra cyberangreb relevant at inddrage i rederiernes risikovurdering for det enkelte skib.

Mørketal vanskeliggør vurderingen
Antallet og detaljeringsgraden af offentligt omtalte cyberangreb mod skibes operationelle systemer er generelt begrænset. Det er der sandsynligvis flere medvirkende forklaringer på. En forklaring kan være, at segmenteringen og cybersikkerheden generelt er så god, at cyberangreb mod disse systemer er vanskelige at udføre. En anden forklaring er manglende interesse i systemerne fra typiske trusselsaktører, der normalt går efter administrative systemer.

Det lave antal omtalte hændelser dækker dog sandsynligvis også over væsentlige mørketal, enten fordi rederierne er tilbageholdende med at indrapportere og tale offentligt om hændelserne, eller fordi angrebene ikke bliver opdaget. Mange rederier monitorerer og scanner ikke deres operationelle systemer, og malware kan derfor ligge uidentificeret hen.

Den 1. februar 2019 trådte en ny bekendtgørelse i kraft for danskflagede skibe omfattet af ISM-koden (International Safety Management-code). Bekendtgørelsen betyder, at rederierne skal underrette Søfartsstyrelsen og Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) om cyberhændelser, som har konsekvenser for skibes sikkerhed og deres sejlads.

Denne vurdering baseres primært på offentligt omtalte cyberangreb og information fra samarbejdspartnere og aktører i søfartssektoren i Danmark.

Cybertruslen

CFCS vurderer, at cybertruslen mod danske skibes operationelle systemer er **HØJ**. Det betyder, at der inden for de næste to år sandsynligvis vil ske forsøg på cyberangreb på operationelle systemer på et eller flere af de over 700 danskflagede handelsskibe. Flere eksempler på sådanne angreb rundt om i verden afspejler truslen. Truslen er også gældende for skibe, som danske rederier opererer under andet flag end dansk.

Det er sandsynligt, at de operationelle systemer er udsat for cybertrusler fra en række aktører med forskellige hensigter og metoder. Uanset hensigt og metode ved det enkelte angreb kan alle typer angreb, der rammer et skibs operationelle systemer, påvirke driften af skibet.

Cybertruslen beskrives i de følgende afsnit efterfulgt af en beskrivelse af angrebsveje mod de operationelle systemer.

Operationelle systemer trues af angreb på tværs af sektorer
CFCS vurderer, at den største cybertrussel kommer fra finansielt motivrede cyberkriminelle. Denne brede gruppe aktører har generelt ikke specifik interesse i operationelle systemer på skibe, men angriber mål på tværs af samfundets sektorer.

Kriminelle hackere er generelt opportunister, og CFCS vurderer, at de gerne angriber operationelle systemer, der eksempelvis kan nås via en kompromittering af forbundne administrative netværk, eller som er sårbare overfor angreb direkte fra internettet.

Kontrolenhed blev ramt af botnet-malware
Antennekontrolenheden på en satellitkommunikationsterminal på et skib blev i 2018 ifølge et it-sikkerhedsfirma inficeret med malware. Malwaren, kaldet Mirai, bliver brugt til at opbygge såkaldte botnet med et meget højt antal kompromitterede computere og enheder med forbindelse til internettet såsom routere, overvågningskameraer og i dette tilfælde også antennekontrolenheder.

Enhederne i et botnet kan bl.a. misbruges til overbelastningsangreb, såkaldte DDoS-angreb, mod bl.a. hjemmesider, som hackeren ønsker at bringe ud af funktion, eller i distribution af spam og malware. Der findes eksempler på, at hackere utilsigtet har forstyrret enheders funktion, fordi de ikke har haft viden om konsekvenserne af deres hacking. I 2016 udnyttede en hacker f.eks. 900.000 hjemmeroutere fra et Mirai-botnet i et DDoS-angreb. Det endte ved en fejl med i to døgn at afbryde internetforbindelsen for de 900.000 kompromitterede kunder hos Deutsche Telekom.

En del af truslen kommer fra kriminelle hackere, der kompromitterer computere, it-systemer og digitale enheder for at udnytte deres maskinkraft, lager- og kommunikationskapacitet til økonomisk vinding. Kompromitterede systemer kan eksempelvis misbruges af kriminelle til at generere kryptovaluta gennem såkaldte kryptominere eller som platform til at angribe andre.

Der er også en trussel fra cyberkriminelle, der kompromitterer systemer for at kryptere dem med ransomware og holde systemerne gidsel, indtil der betales løsesum.

CFCS vurderer, at cyberkriminelle, der udfører ransomware-angreb, ikke har en særlig interesse i operationelle systemer på skibe. De angriber computere og it-systemer på tværs af sektorer, som er sårbare over for deres angrebsmetoder og malware.

Operationelle systemer på skibe kan være attraktive for kriminelle afpressere, da systemerne er vigtige for rederiet, og derfor kan øge muligheden for at lægge pres på offeret og aftvinge en løsesum. Nogle typer ransomware er desuden programmeret til at sprede sig autonomt til forbundne systemer og netværk. Det skete eksempelvis under WannaCry-angrebene i 2017, hvor mere end 300.000 computere verden over blev ramt af ransomware.

Infektion af administrative systemer kan sprede sig
I 2017 spredte et ransomware-angreb sig fra en skibsførers computer til skibets operationelle systemer og slukkede for strømforsyningen. Besætningen kunne ikke selv få systemerne tilbage i drift, så de blev nødt til at få fløjet it-assistance ud til skibet. Først efter tre dage fik de strømforsyningen i funktion igen. Ransomwaren havde spredt sig til trods for en segmentering af netværkene.

I et eksempel fra 2019 oplevede et containerskib med rute mod New York, at deres skibsnetværk var stærkt svækket af malware. Den amerikanske kystvagt og forbundspolitiet FBI besøgte skibet, inden det nåede i havn. De konstaterede, at malwaren, kaldet Emotet, ikke havde påvirket essentielle operationelle systemer. Myndighedernes undersøgelser afslørede dog flere alvorlige it-sikkerhedsforhold, heriblandt væsentlige sårbarheder for kritiske kontrolsystemer på skibet.

Der er kriminelle hackere, der sender phishing-mails målrettet specifikke skibe og deres besætninger. CFCS vurderer, at disse angreb generelt ikke er målrettet de operationelle systemer på skibene. Angrebene har, ligesom de bredere kampagner, finansiel vinding som mål, og hackerne benytter sig af metoder, der er gængse på tværs af sektorer.

CFCS har bl.a. kendskab til phishing-mails sendt til modtagere på skibe, der har haft til formål at sprede malware, som typisk bruges til tyveri af finansielle oplysninger og spredning af ransomware.

Enkeltpersoner udgør også en trussel
Mens CFCS vurderer, at hackere generelt ikke går målrettet efter skibes operationelle systemer, findes der undtagelser. CFCS vurderer, at operationelle systemer, som er eksponeret på internettet og dårligt beskyttet, trues af enkeltpersoner, der af nysgerrighed eller teknisk interesse forsøger at få adgang til operationelle systemer og eventuelt manipulere dem.

Cybersikkerhedsforskere og -virksomheder har demonstreret, at det i nogle tilfælde er muligt uden særligt høje tekniske kompetencer at kompromittere operationelle systemer på skibe.

En nysgerrig person fandt ifølge åbne kilder i 2019 et såkaldt dynamisk positioneringssystem på en flydende boreplatform ved hjælp af søgemaskinen Shodan. Systemet var sårbart for hackerangreb, og personen formåede utilsigtet at slukke systemet. Der findes ingen rapportering om konsekvensen for den konkrete boreplatform, men andre eksempler på konsekvenser er tilgængelige i åbne kilder. For eksempel fik et cyberangreb indvirkning på en flydende boreplatform ud for Afrika. I det tilfælde hældede platformen så meget, at produktionen måtte lukke i en uge, før de havde identificeret og løst problemet.

Der er en potentiel trussel fra destruktive angreb fra stater
Der er en potentiel trussel fra destruktive cyberangreb udført af statslige aktører mod operationelle systemer på skibe, særligt i forbindelse med en militær konflikt. CFCS vurderer dog, at der på nuværende tidspunkt ikke er stater, der har til hensigt at udføre destruktive cyberangreb målrettet danske skibe.

Truslen for destruktive cyberangreb kan være højere mod skibe, der opererer i konfliktområder, hvor stater bruger destruktive cyberangreb mod civile mål. NotPetya-angrebet i 2017, der bl.a. ramte Mærsk, var netop rettet mod virksomheder med aktiviteter i Ukraine. Under konflikten mellem Ukraine og Rusland har der været flere tilfælde af destruktive cyberangreb i landet. Andre lande, herunder Saudi-Arabien og Sydkorea, har også været ramt af destruktive cyberangreb.

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

Maritime udstyrsleverandører er særligt udsat for cyberspionage. Hackere kan 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.

Opdatering var angrebsvej for NotPetya
NotPetya-angrebet havde sit udspring hos en kompromitteret ukrainsk softwarevirksomhed, som har udviklet softwaren M.E.Doc. Hackere leverede NotPetya-malwaren til virksomheder gennem en softwareopdatering til M.E.Doc. Malwaren var en såkaldt orm, der efterfølgende hurtigt spredte sig til øvrige dele af de berørte virksomheders it-infrastruktur samt til andre virksomheder.

Cyberspionage mod rederier forekommer også. Spionagen kan ligeledes misbruges som trædesten for destruktive cyberangreb mod operationelle systemer på skibe, hvis der er forbindelser mellem rederiet og operationelle systemer på skibe.

Forstyrrelse af GNSS-signaler er også en trussel
En anden type trussel mod skibes operationelle systemer er forstyrrelse af GNSS-signaler, såsom GPS, der bl.a. benyttes til positionering i skibes navigationssystemer. GNSS-forstyrrelser udgør en trussel mod de skibssystemer, der benytter signalerne.

Forstyrrelser af GNSS-signaler sker ved lokalt at udsende elektroniske signaler, der overdøver de legitime signaler. Det kan være ved at udsende støjsignaler, hvilket kaldes jamming, eller ved at sende alternative signaler, således at positionen eksempelvis ændres. Dette kaldes spoofing.

Forsvarets Efterretningstjeneste kategoriserer angrebsmetoderne som elektronisk krigsførelse, og der har været mange tilfælde af forstyrrelser af GNSS-signaler i farvande nær bl.a. Rusland, Iran, Syrien og Kina. NATO's maritime kommando følger forstyrrelser af GNSS-signaler rundt om i verden, og skibe kan indrapportere forstyrrelser hertil.

Metoden udføres som udgangspunkt både af stater og kriminelle. CFCS vurderer, at motiverne bag disse forstyrrelser varierer. Et motiv kan eksempelvis være at beskytte et område mod dronetrafik, der benytter GNSS-signaler. Det kan f.eks. være myndigheder, der vil undgå droner, som forstyrrer flytrafikken ved en lufthavn. Det kan også være kriminelle smuglere, der vil undgå droner, som overvåger f.eks. grænseovergange. I forbindelse med en konflikt kan formålet være at forstyrre lufts- og skibstrafik.

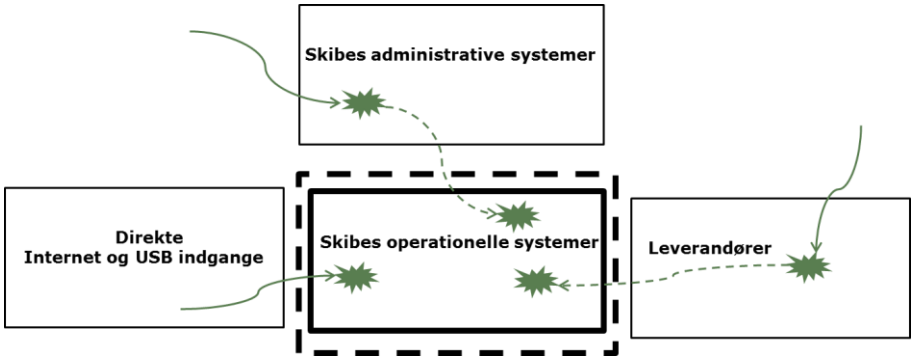
CFCS er ikke bekendt med hændelser, hvor hackere har kompromitteret systemer med det formål at forstyrre GNSS-signaler.

Flere angrebsveje til skibes operationelle systemer

De forskellige trusselsaktører rammer skibenes operationelle systemer på forskellige måder og gennem forskellige angrebsveje. Angrebsvejene kan generelt inddeles i tre grupper:

1. Angreb gennem eksterne enheder eller forbindelser til internettet.
2. Angreb gennem forbindelser til administrative systemer.
3. Angreb gennem udstyrsleverandørernes adgange til operationelle systemer.

Kombinationer af angrebsvejene forekommer også.



Figur 1. Angrebsveje til skibes operationelle systemer (illustreret).

Sårbare systemer kan angribes direkte fra bl.a. internettet
Operationelle systemer kan være sårbare overfor forholdsvis simple cyberangreb direkte fra internettet eller gennem eksterne enheder, såsom USB-enheder, mobiltelefoner og lignende, der kobles til systemerne. Disse angreb forudsætter ikke forudgående kompromittering af eksempelvis rederiet eller underleverandører.

Systemerne er særligt sårbare, hvis de uden tilstrækkelig beskyttelse er koblet direkte på internettet, eller hvis de ikke er beskyttet mod overførsler af malware via eksterne enheder. Der har i søfartssektoren i de seneste år været stor fokus på risikoen for inficeringer med malware via åbne USB-indgange på hardwaren til operationelle systemer.

En anden udbredt metode blandt hackere er at overtage styringen med digitale enheder, som benytter kendte standardpasswords eller svage passwords. Det gør de ved at scanne internettet for sådanne digitale enheder og gætte deres password. Disse hackere har ofte ikke en særlig interesse i søfart, men ønsker at kompromittere og misbruge enheder uafhængigt af deres normale funktion eller betydning.

Leverandør inficerer system via USB-forbindelse
Skibsrederforeningen BIMCO beskriver i deres retningslinjer fra december 2018 et eksempel, hvor strømstyringssystemet på et skib blev inficeret med malware overført i forbindelse med en systemopdatering udført af en leverandørs tekniker. Inficeringen skete utilsigtet via teknikerens brug af en USB-forbindelse til skibets systemer.

Forbindelser muliggør angreb gennem administrative systemer
Administrative systemer på skibe er i lighed med systemer på land udsat for en vedvarende trussel fra især cyberkriminelle. Der findes derfor en række eksempler på angreb på skibes administrative systemer.

Ved kompromittering af de administrative systemer kan angrebet sprede sig til operationelle systemer, hvis der er forbindelse mellem systemerne, eller angriberne er i stand til at bryde en eventuel segmentering.

Selv hvis angreb mod administrative systemer ikke breder sig, kan angreb, der låser eller forstyrrer de administrative systemer, eksempelvis ransomware-angreb, påvirke den forretningsmæssige drift af skibet. Det kan eksempelvis ske, hvis personalet pga. angrebet ikke har adgang til fragt- eller passagersystemer.

Udstyrsleverandører kan bruges som trædesten
Leverandører af operationelle systemer har i stigende grad netværksadgang til skibene for at følge og opdatere de leverede systemer. Det åbner op for cyberangreb gennem udstyrsleverandører, som rederiet har tillid til.

Nogle af leverandørerne af specialiseret skibsudstyr har meget store markedsandele på globalt plan. Et cyberangreb gennem en sådan leverandør kan derfor få effekt på drift og sikkerhed på et stort antal skibe globalt på tværs af sektoren.

Der findes eksempler på forstyrrelser af skibes operationelle systemer gennem opdateringer fra udstyrsleverandører. Et klassifikationsselskab beskrev i 2017 en hændelse, hvor navigationssystemet ECDIS på to bulkskibe lukkede ned i forbindelse med kortopdateringer fra en kortleverandør. Opdateringen skete med en tilsendt fil, der blev overført via et USB-flashdrive. ECDIS lukkede først ned på det ene skib. Idet besætningen ikke rapporterede om hændelsen, skete det samme senere, da besætningen på søsterskibet opdaterede ECDIS med samme fil. Der er modstridende meldinger om, hvorvidt opdateringen var inficeret med malware, eller om den var behæftet med fejl. Uanset årsagen viser hændelsen, hvordan en sårbarhed kan påvirke skibets sikkerhed.

Truslen gennem leverandører og underleverandører kaldes for supply-chain-truslen. CFCS har i 2019 beskrevet denne trussel mere uddybende i trusselvurderingen Cyberangreb mod leverandører, der er tilgængelig på CFCS's hjemmeside.

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