CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod forsvarsindustrien

Formålet med denne vurdering er at informere beslutningstagere i forsvarsindustrien i Danmark om cybertruslen. Vurderingen er udarbejdet i dialog med Forsvars- og Aerospaceindustrien i Danmark (FAD).

Dato: 23. juni 2020

Sagsnr.: 2017/000191
Dok. nr.: 178323

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 66
E-mail: fe@fe-mail.dk
www.fe-ddis.dk

Hovedvurdering

- Der er en **MEGET HØJ** trussel fra cyberspionage. Flere lande har udført cyberspionage mod forsvarsindustrien verden rundt. På grund af overlap i teknologier er truslen fra cyberspionage forbundet med truslen mod beslægtede sektorer, særligt indenfor sø-, luft- og rumfart.

- Der er en **MEGET HØJ** trussel fra cyberkriminalitet. CFCS vurderer, at den generelle trussel fra cyberkriminalitet mod virksomheder og myndigheder i Danmark også er gældende for sektoren. Cyberkriminelle har dog generelt ikke et særligt fokus på sektoren.

- 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 regioner præget af konflikter, er mere udsatte for truslen.

- Der er en **LAV** trussel fra cyberaktivisme. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, og cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder.

- 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.

Analyse

Denne rapport vurderer cybertruslen mod forsvarsindustrien i Danmark. Vurderingen af cybertruslen er opdelt i trusler fra cyberangreb, der understøtter spionage, kriminalitet, aktivisme og terrorisme samt destruktive cyberangreb.

Forsvarsindustrien defineres i denne vurdering til at gælde virksomheder, der producerer udstyr og komponenter til systemer og platforme anvendt til militære formål.

Da mange komponenter og teknologier anvendt i sådanne systemer og platforme bruges til både civile og militære formål, såkaldt dual-use, er der ofte et overlap mellem forsvarsindustrien og andre industrier og sektorer.

Det bliver bl.a. afspejlet af, at virksomheder i sektoren både kan have civile og militære produkter og kunder. Overlappet bliver også afspejlet organisatorisk af, at nogle danske udstyrsleverandører inden for bl.a. søfart er del af internationale virksomheder, der også beskæftiger sig med forsvarsteknologi. Flere udenlandske virksomheder i sektoren har også afdelinger i Danmark.

Dette overlap betyder, at truslen mod forsvarsindustrien hænger sammen med truslen fra overlappende industrier, da cyberspionage mod eksempelvis en international forsvarsindustrikoncern kan blive rettet mod et dansk datterselskab, eller at cyberspionage mod teknologier med dual-use egenskaber kan ramme såvel civile som militære producenter.

Cyberspionage
Der er en **MEGET HØJ** trussel fra cyberspionage. Det betyder, at det er meget sandsynligt, at virksomheder i forsvarsindustrien i Danmark vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Flere stater har udført cyberspionage mod forsvarsindustrien verden rundt.

Disse stater benytter bl.a. cyberspionage som et middel til at opnå industrielle og forretningsmæssige fordele samt styrke deres sikkerhedspolitiske position. Spionagen mod forsvarsindustrien er derfor sandsynligvis både økonomisk og sikkerhedspolitisk motiveret.

For staterne, der står bag cyberspionagen, kan de stjålne informationer både misbruges kommercielt til at fremme deres egne virksomheder og give et indblik i militære teknologier og systemer, som benyttes af andre lande.

Teknologiernes mulige anvendelse til både civile og militære formål kan betyde, at både kommercielle og sikkerhedspolitiske behov kan blive dækket på samme tid. Nogle lande, der har en stor 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).

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

På grund af overlap i teknologier og organisering er truslen fra cyberspionage som nævnt forbundet med truslen mod beslægtede sektorer. Hændelser globalt viser især et overlap med truslen mod virksomheder indenfor sø-, luft- og rumfart. CFCS har i separate vurderinger for henholdsvis søfart og luftfart vurderet, at der også er en **MEGET HØJ** trussel fra cyberspionage mod disse sektorer i Danmark.

Virksomheder og organisationer i forsvarsindustrien kan også blive anvendt som platform for angreb mod andre ofre, i og uden for sektoren.

Hackergrupper har i udlandet eksempelvis oprettet falske hjemmesider og domæner, der efterligner forsvarsindustrivirksomheder, flåde- og flyudstillinger og brancheorganisationer med henblik på at kompromittere andre virksomheder eller myndigheder.

Der har i de seneste år også været eksempler på, at kendte hackergrupper har brugt falske jobopslag fra forsvarsindustrivirksomheder i bl.a. USA og Indien som lokkemad i phishing-angreb.

I et andet eksempel brugte en hackergruppe dokumenter og militære systemer som lokkemiddel i et phishing-angreb rettet mod sikkerhedsgodkendte medarbejdere i amerikanske forsvarsindustrivirksomheder.

Cyberspionage kan finde sted i samspil med traditionelle former for spionage og forsøg på indkøb af eksportkontrollerede varer.

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

Cyberkriminalitet er i denne vurdering en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk berigelse.

CFCS vurderer, at den generelle trussel fra cyberkriminalitet mod virksomheder og myndigheder i Danmark også er gældende for sektoren.

Det bliver bl.a. afspejlet af, at der er flere offentligt kendte eksempler på cyberangreb udført af kriminelle mod sektoren verden rundt. CFCS vurderer dog, at cyberkriminelle generelt ikke har et særligt fokus på sektoren.

Cyberkriminalitet udgør en vedvarende og aktiv trussel mod alle danske myndigheder, virksomheder og borgere. Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på en gang, bl.a. gennem phishing-angreb. Der findes dog også netværk med kapacitet til at udføre mere avancerede og tidskrævende cyberangreb, herunder målrettede ransomware-angreb.

Cyberangreb fra kriminelle grupper starter typisk, uden at aktøren på forhånd har udset sig et specifikt offer. De fleste cyberangreb starter som opportunistiske angreb, hvor eksempelvis phishing-mails bliver spredt til tusinder af ofre, eller hvor kriminelle misbruger it-systemer og enheder med kendte sårbarheder.

Der er dog en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder. I målrettede ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af offerets it-systemer ved hjælp af ransomware.

Målrettede ransomware-angreb har ramt danske virksomheder, og angreb sker nu relativt hyppigt. I Danmark blev pumpeproducenten Desmi, der også er leverandør til Forsvaret, udsat for et ransomware-angreb i 2020.

I udlandet blev producenten af flydele, ASCO, ramt af ransomware i 2019. Angrebet medførte betydelige forstyrrelser i produktionen. ASCO leverer bl.a. flydele til militære fly, herunder F-35. Tidligere på året blev Mitsubishi Heavy Industries Canada Aerospace, der også producerer flydele, ramt af et lignende angreb.

Kriminelle kan også true med at lække stjålne informationer eller sælge dem. I Australien forsøgte kriminelle hackere i 2018 eksempelvis at afpresse Austal, der producerer skibe til både militær og civil brug, for penge ved hjælp af stjålne informationer. Hackerne forsøgte at sælge oplysningerne, som hackerne påstod handlede om militære fartøjer, på nettet.

Siden slutningen af 2019 har hackere, der har stået bag målrettede ransomware-angreb, også af og til truet med at lække følsomme data indsamlet fra det ramte system, hvis offeret ikke betaler løsesummen.

Destruktive cyberangreb
Der er en **LAV** trussel fra destruktive cyberangreb. Det betyder, at det er mindre sandsynligt, at virksomheder i forsvarsindustrien 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.

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

Det er her vigtigt at bemærke, at CFCS' definition af destruktive cyberangreb dækker cyberangreb med meget forskellige konsekvenser. Langt de fleste af de destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data ved at slette eller kryptere dem uden mulighed for

at genskabe dem. Destruktive cyberangreb er selv inden for denne brede definition relativt sjældne.

Flere stater har dog betydelige kapaciteter til at udføre destruktive cyberangreb, og de udvikler deres kapaciteter løbende. Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

Det er muligt, at danske virksomheder og myndigheder, som har aktiviteter i regioner præget af konflikter, kan blive udsat for følgevirkningerne af et destruktivt cyberangreb. Indtil nu har de fleste angreb fundet sted i Ukraine og Saudi Arabien.

Danske virksomheder med aktiviteter i særligt Ukraine og Saudi Arabien kan i enkelte tilfælde også blive udset som direkte mål for destruktive cyberangreb. Det blev illustreret af angrebet, der slettede data hos den italienske virksomhed Saipem i 2018. Saipem er underleverandør til den saudiske nationale olieproducent Saudi Aramco. Saudi Aramco har selv været udsat for destruktive cyberangreb både i 2012, 2016 og 2017.

Cyberaktivisme
Der er en **LAV** trussel fra cyberaktivisme. Det betyder, at det er mindre sandsynligt, at virksomheder i forsvarsindustrien i Danmark vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Truslen kommer særligt til udtryk i forbindelse med begivenheder eller enkeltsager, der tiltrækker cyberaktivisters opmærksomhed.

Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en sag. Cyberaktivister opnår dette mål med forskellige midler, og angrebsmetoderne varierer meget i kompleksitet – fra relativt simple DDoS-angreb til mere ressourcekrævende hack og læk af informationer fra myndigheder og virksomheder.

Cyberterror
Der er **INGEN** trussel fra cyberterror. Det betyder, at det er usandsynligt, at Danmark, herunder virksomheder i forsvarsindustrien 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

"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.

Fordelingsliste

Til:
Forsvars- og Aerospaceindustrien i Danmark

Kopi til:
Justitsministeriet

Forsvarsministeriet

Forsvarsministeriets Materiel- og Indkøbsstyrelse

Forsvarskommandoen

Politiets Efterretningstjeneste