CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod dansk luftfart

1. udgave november 2019
Senest opdateret juni 2022

Indhold

CENTER FOR CYBERSIKKERHED

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

4. udgave juni 2022

Cybertruslen mod dansk luftfart

Formålet med denne trusselsvurdering er at redegøre for cybertruslen mod den danske luftfartssektor. Trusselsvurderingen kan bl.a. bruges i sektorens videre arbejde med risikovurderinger. Målgruppen for trusselsvurderingen er ledelsen og it-medarbejdere i danske lufttrafikstyrings- og luftfartsmyndigheder, lufthavne, flyselskaber og underleverandører til flyproducenter.

Trusselsvurderingen er første gang opdateret i juni 2020 med ændringer i kapitlet om cyberterror som følge af en ændring af trusselsniveauet i den årlige nationale trusselsvurdering "Cybertruslen mod Danmark" udgivet i 2020, samt tilføjelsen af et trusselsniveau til vurderingen af destruktive cyberangreb. Resten af teksten er uændret.

Trusselsvurderingen er igen opdateret i september 2021 med et tilpasset kapitel om cyberspionage. Trusselsniveauet for cyberspionage blev hævet til **MEGET HØJ**. Resten af teksten er uændret.

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

Hovedvurdering

- Truslen fra cyberkriminalitet mod den danske luftfartssektor følger det overordnede niveau for cybertruslen mod Danmark og er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at virksomheder eller myndigheder i luftfartssektoren bliver ramt af forsøg på cyberkriminalitet.

- Truslen fra cyberspionage mod den danske luftfartssektor er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at virksomheder eller myndigheder i luftfartssektorens vil blive ramt af forsøg på cyberspionage.

- 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 mål i luftfartsektoren.

- Truslen fra destruktive cyberangreb mod den danske luftfartssektor er **LAV**. Det er dog muligt, at den danske luftfartssektor kan blive påvirket af destruktive cyberangreb i udlandet.

- Truslen fra cyberterror mod den danske luftfartssektor er **INGEN**.

Om trusselsvurderingen

Trusselsvurderingen beskriver cybertruslen mod den danske luftfartssektor. Vurderingen analyserer dermed truslen mod danske lufttrafikstyrings- og luftfartsmyndigheder, lufthavne, flyselskaber og underleverandører til flyproducenter.

Vurderingen tager udgangspunkt i analyser af internationale eksempler på cyberangreb mod lufthavne, flyselskaber, underleverandører og myndigheder. Det sammenholdes med danske forhold og viden om trusselsaktørers kapacitet og intention. Vurderingen er udarbejdet efter dialog med organisationer i luftfartssektoren. CFCS har fortsat begrænset viden om konkrete angreb mod den danske luftfartssektor.

Trusselsvurderingen beskriver det aktuelle trusselsbillede på kort sigt, som svarer til en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og specifikt for luftfartssektoren. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Den største trussel mod sektoren er cyberkriminalitet, herunder særligt ransomware. Ransomware-angreb kan ramme alle organisationer. Internationalt er det dog særligt flyproducenter og lufthavne, som har været ramt af ransomware. Kriminelle aktører er også interesserede i at kompromittere flyselskabers kundevendte systemer for at videresælge kreditkortinformationer eller bonuspoint fra flyselskaber.

Vurderingen beskriver også, at truslen fra cyberspionage er **MEGET HØJ**.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod luftfartssektoren er **MEGET HØJ.** Truslen kommer fra økonomisk motiverede kriminelle enkeltpersoner og netværk.

Aktørerne er interesserede i at kompromittere organisationer, hvis de vurderer, at en sårbarhed kan udnyttes til at iværksætte et cyberangreb, som kan skabe profit.

Nogle cyberkriminelle netværk går målrettet efter store organisationer, fordi angreb mod disse er mere profitable. Dette fænomen kaldes 'big game hunting'. Store lufthavne, flyselskaber, og underleverandører til flyproducenter er derfor særligt interessante for disse cyberkriminelle netværk.

Cyberkriminelle bruger ransomware til afpresning

Mange cyberkriminelle benytter sig af såkaldt ransomware. Ved et ransomware-angreb bliver data og systemer på offerets computer holdt som gidsel, da de krypteres og derved bliver utilgængelige for offeret. Aktøren bag kræver en løsesum, typisk i form af kryptovaluta såsom Bitcoin, for at give offeret adgang til sine data igen. Som regel vil aktøren bag angrebet installere malware ved hjælp af phishingmails. De fleste ransomware-angreb lykkes, fordi brugeren snydes til at klikke på et link eller en vedhæftet fil i en mail. Men ransomware-angreb kan også ske ved, at hackere f.eks. kompromitterer fjernadgange eller udnyttelse af sårbarheder i internetvendte systemer.

Der findes mange varianter af ransomware. Kriminelle hackere, der udfører målrettede ransomware-angreb, forsøger at ramme eksempelvis administrative netværk i specifikke virksomheder og myndigheder.

Ransomware-angreb kan have alvorlige konsekvenser. For eksempel medførte et ransomware-angreb mod Clevelands Hopkins Internationale Lufthavn i april 2019 forstyrrelser og nedbrud på lufthavnens informationsskærme, i bagagehåndteringen og i lufthavnens interne mailsystemer.

Flere typer af ransomware udnytter sårbarheder, som for længst er blevet løst gennem softwareopdateringer. WannaCry-ransomwaren udnytter eksempelvis en sårbarhed, som blev løst med en softwareopdatering i marts 2017. Alligevel blev mere end 300.000 computere inficeret, da det globale WannaCry-angreb ramte i maj 2017. I marts 2018 blev Boeing desuden inficeret med WannaCry, hvilket viser, at WannaCry fortsat udgør en trussel for systemer, som ikke bliver opdateret.

> WannaCry-ransomwaren begyndte at sprede sig til computere verden over i maj 2017. Ved at bruge WannaCry var hackere i stand til automatisk at kryptere filer på ofrets computer, slette originalerne og fingere at opkræve en løsesum for at dekryptere filerne igen.
>
> Samtidig installerede ransomwaren en bagdør på ofrets maskine, som gav angriberen mulighed for at installere yderligere malware. WannaCry var i stand til at sprede sig over lokalnetværk og internettet via en sårbarhed i Server Message Block, version 1 (SMBv1)-protokollen.

Cyberkriminelle stjæler kreditkortoplysninger og bonuspoint
Cyberkriminelle udviser også interesse for persondata, som kan sælges. Det gælder særligt for kreditkortdata og bonuspoint. CFCS har kendskab til, at stjålne bonuspoint bliver handlet på nettet som en form for valuta.

I perioden fra august til september 2018 blev British Airways udsat for et cyberangreb. Her fik cyberkriminelle adgang til navne og mailadresser på passagerer. De fik også adgang til passagerers kreditkortnumre og de tilhørende udløbsdatoer og CVC/CVV-numre, når kunderne indtastede disse på hjemmesiden. British Airways vurderer, at op mod 380.000 kunder blev ramt af angrebet. I forlængelse af angrebet fik British Airways i juli 2019 en bøde på 1.5 milliarder kr. for ikke at leve op til EU's databeskyttelsesforordning. Bøden blev i efteråret 2020 reduceret til 173 mio. kr.

Kriminelle aktører forsøger ofte at kompromittere eller udnytte leverandører med henblik på at skaffe sig adgang til et større mål. Det gælder også for leverandører i luftfartssektoren. Denne type angreb kaldes supply chain-angreb.

En særlig type supply chain-angreb udføres via underleverandører, der leverer software. Den form for angreb kaldes også software supply-chain angreb. I sådanne angreb kompromitteres softwarevirksomheder, så angriberen efterfølgende kan kompromittere en eller flere af de organisationer, der benytter software fra virksomheden. Aktøren kan f.eks. kompromittere brugerne af softwaren ved at levere malware via softwareopdateringer

'BEC-scams' udgør en trussel for sektoren
CFCS har kendskab til, at organisationer i den danske luftfartssektor er blevet udsat for forsøg på BEC-scams.

BEC-scams, også kendt som CEO-fraud eller direktørsvindel, er forsøg på at franarre virksomheder og organisationer penge gennem falske anmodninger om pengeoverførsler. I stedet for at sende mails til en stor gruppe tilfældige medarbejdere i en virksomhed, laver hackerne grundig research. Det gør dem i stand til at lave troværdige, målrettede mails, hvor de f.eks. udgiver sig for at være en direktør, økonomichef eller konsulent i tæt kontakt med den øverste ledelse og lokke ansatte til at agere i den tro, at det er efter ordre fra ledelsen.

Der er en potentiel insidertrussel i luftfartssektoren
Der er en potentiel insidertrussel i alle organisationer. Det gælder også i luftfartssektoren. Organisationers sikkerhedsmekanismer beskytter ofte ikke mod insidere, som er i stand til at udføre sine handlinger alene ved at bruge sine legitime it-adgange. Fysisk adgang til systemer kan facilitere kompromitteringer. Det kan være særligt relevant at være opmærksom på i forbindelse med systemer og data, som er isolerede fra internettet.

Cyberspionage

Truslen fra cyberspionage mod luftfartssektoren er **MEGET HØJ.**

CFCS vurderer, at der inden for de seneste år har været øget cyberspionageaktivitet rettet mod luftfartssektoren i udlandet. Fremmede stater har udført angreb mod forskellige typer organisationer inden for luftfarten. Det er meget sandsynligt, at den danske luftfartsektor også vil blive ramt af kompromitteringsforsøg. CFCS vurderer, at fremmede stater bl.a. har en særlig interesse for myndigheder inden for sektoren.

Spionage mod transportsektoren kan være motiveret af sikkerhedspolitiske interesser. Transportsektoren indgår i dansk kritisk infrastruktur, og fremmede stater kan derfor have interesse i at opbygge viden om kapaciteter og sårbarheder i luftfartssektoren, der kan have betydning i forbindelse med eksempelvis en militær konflikt. Indhentning af information om kritisk infrastruktur kan f.eks. benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.

I luftfartssektoren har statsstøttede hackergrupper bl.a. udvist interesse for teknologi, som kan bruges til at udvikle den pågældende stats egen luftfartssektor. Nogle statsstøttede aktører med betydelig kapacitet har udvist særlig interesse i teknologi, som både kan bruges i civil- og militær luftfart samt rumfart. Denne trussel retter sig derfor også i høj grad mod flyproducenter og disses underleverandører.

Det er eksempelvis sandsynligt, at udviklingen af motoren i det kinesiske passagerfly C919 blandt andet er sket på baggrund af målrettet statsstøttet cyberspionage mod flyproducenter og underleverandører i udlandet.

Statsstøttede aktører har også udvist interesse for luftfartsområdet i bredere forstand. FN's luftfartsorganisation ICAO blev f.eks. udsat for et cyberangreb i november 2016. Det skete, da en statsstøttet aktør indsatte ondartet kode i artikler på ICAO's hjemmeside. Formålet med kompromitteringen var sandsynligvis at komme videre ind i andre dele af luftfartsindustrien.

CFCS har kendskab til et ældre eksempel, hvor en dansk organisation i luftfartssektoren har været kompromitteret af statsstøttede aktører.

Truslen fra cyberspionage er også rettet mod luftfartsselskaber. Statsstøttede grupper har bl.a. udvist interesse for persondata, sandsynligvis med henblik på at kortlægge bestemte personer og organisationers rejsemønstre.

Organisationer i den danske luftfartssektor kan også blive ofre for cyberspionage, der bliver udført via leverandører, såsom softwareleverandører. I 2021 blev tusindvis af organisationer ramt i det såkaldte SolarWinds-angreb. Flyselskabet SAS var blandt ofrene i angrebet. SAS havde fået installeret en bagdør på deres systemer, men har ifølge offentlige udtalelser ikke set tegn på, at bagdøren er blevet udnyttet.

Cyberaktivisme

Truslen fra cyberaktivisme mod luftfartsektoren er **MIDDEL**. Det betyder, at det er muligt, at luftfartsektoren vil blive ramt af aktivistiske 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. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, men Ruslands invasion af Ukraine har skabt stor opmærksomhed i dele af det aktivistiske miljø. Hvor cyberaktivistiske angreb indledningsvist fandt sted i direkte forlængelse af krigen og var fokuseret mod Rusland, Ukraine og Belarus, har cyberaktivistiske angreb sidenhen også ramt vestlige NATO-lande. Blandt andet hævder cyberaktivister at have udført DDoS-sangreb mod lufthavne i Tyskland, England og Polen. Det høje aktivitetsniveau blandt de pro-russiske cyberaktivister øger også truslen for cyberaktivistiske angreb mod Danmark, herunder luftfartssektoren.

Når trusselsniveauet for cyberaktivisme er hævet 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.

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag. Aktivisme mod luftfart har en stor synlighed, som kan skabe opmærksomhed om cyberaktivisters budskaber. Cyberaktivister kan f.eks. få stor opmærksomhed på deres sag, hvis det lykkes at angribe lufthavnes hjemmesider, da disse typisk har mange besøgende. Ligeledes har informationsskærme i lufthavne en høj grad af synlighed, og er derfor interessante mål.

Cyberaktivister angriber også myndigheder og virksomheder, som hackerne betragter som symbolske mål. Det gør de, selvom ofrene ikke har været direkte indblandet i den sag, der optager hackerne. Angrebene kan også være tilfældige i den forstand, at hackerne angriber, hvor de kan skaffe sig adgang eller udnytte sårbarheder.

> Defacement af en hjemmeside er et angreb, der ændrer hjemmesidens visuelle udtryk. Eksempelvis kan angriberen indsætte en tekst eller et billede på hjemmesidens forside.

Luftfartssektoren udgør bl.a. et mål for aktivister, som interesserer sig for klimaområdet. Den klimaaktivistiske gruppe 'Heathrow Pause' truede eksempelvis med at forstyrre flytrafikken i London Heathrow Lufthavn i september 2019.

DDoS-angreb
DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængelig for legitim trafik, mens angrebet står på.

Luftfartssektoren bliver ramt af DDoS-angreb, og det er en tilbagevendende trussel, som både er blevet brugt ved ældre angreb og i de nye angreb forbundet med krigen i Ukraine. Eksempelvis blev LOT Polish Airlines base i Warsawa Lufthavn allerede i 2015 ramt af et DDoS-angreb. Angrebet medførte, at ca. 1.400 passagerer strandede midlertidigt.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod luftfartssektoren er **LAV**.

Det betyder, at det er mindre sandsynligt, at luftfartssektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt.

Et eksempel herpå var NATO-øvelsen Trident Juncture i oktober-november 2018. Her blev områder i det nordlige Norge udsat for elektroniske angreb i form af GPS-jamming, hvilket påvirkede den civile luftfart. Selvom GPS-jamming er et elektronisk angreb – og ikke et cyberangreb – vurderes det, at truslen for destruktive cyberangreb kan stige på samme måde i forbindelse med en konflikt.

En række lande har cyberkapaciteter, der kan bruges destruktivt mod samfundsvigtig infrastruktur såsom luftfartssektoren. Destruktive cyberangreb er cyberangreb, hvor den forventede effekt er tab af menneskeliv, personskade og/eller betydelig skade på- eller ødelæggelse af fysiske objekter. Herunder forandring af informationer, data eller software, så objekter ikke kan anvendes uden væsentlig genopretning.

Det er muligt, at den danske transportsektor kan blive påvirket af destruktive cyberangreb i udlandet. I udlandet er luftfartssektoren blevet ramt af destruktive cyberangreb, som i mindre grad forstyrrede sektorens tilgængelighed. I juni 2017 blev flere virksomheder i sektoren i udlandet ramt af NotPetya-angrebet, der var et destruktivt cyberangreb forklædt som ransomware. I Ukraine blev to lufthavne påvirket af angrebet.

Cyberterror

Truslen fra cyberterror mod luftfartssektoren er **INGEN**.

Det betyder, at det er usandsynligt, at luftfartssektoren, 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.

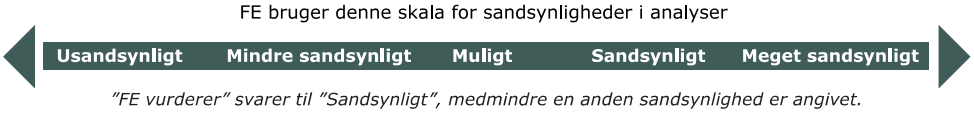
Trusselsniveauer

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.

Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for luftfartsektoren Alle produkterne er tilgængelige på CFCS' hjemmeside.

Truslen fra bevidste og ubevidste insidere
CFCS og PET har udarbejdet trusselsvurderingen 'Cybertruslen fra bevidste og ubevidste insidere'. I trusselsvurderingen kan du læse mere om truslen og anbefalinger til mitigerende tiltag. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/insidertruslen/

Trusselsvurdering om truslen mod leverandører
Trusselsvurderingen "Cyberangreb mod leverandører" beskriver cybertruslen mod leverandører. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/leverandorer/

Vejledning om leverandørstyring
Vejledningen "Informationssikkerhed i leverandørforhold" indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Truslen fra phishing-mails
Trusselsvurderingen "Cybertruslen fra phishing-mails" går i dybden med, hvordan hackere benytter phishing- og spear-phishing-mails i deres forsøg på at kompromittere virksomheder eller franarre dem følsomme oplysninger. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/phishing/

Vejledning til at imødegå phishing
Vejledningen "Phishing: Beskyt organisationen mod phishingangreb" henvender sig til ledelsen og kommer med en række konkrete anbefalinger, der kan bidrage til organisationernes arbejde med at beskytte sig mod phishing-angreb. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/phishing/

Samarbejde mellem cyberkriminelle
Trusselsvurderingen "Drømmer cyberkriminelle om tillidsfulde relationer?" beskriver, hvordan veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/organiseret-cyberkriminalitet/

Truslen fra målrettede ransomware-angreb
Trusselsvurderingen "Digitale gidseltagere på storvildtjagt" beskriver truslen fra såkaldte målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Vejledning om at imødegå ransomware-angreb
Vejledningen 'Reducér risikoen for ransomware' giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-

angreb kan håndteres, når skaden er sket. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/

Hvordan målrettede ransomware-angreb foregår skridt for skridt
Undersøgelsesrapporten 'Anatomien af målrettede ransomware-angreb' går i dybden med, hvordan sådanne angreb foregår. Rapporten indeholder konkrete råd til, hvordan angrebene kan imødegås. Læs rapporten her: https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Cyberangreb mod HR-afdelinger
Trusselsvurderingen "HR-afdelinger rammes også af målrettede cyberangreb" belyser, hvordan hackere forsøger at bruge HR-afdelinger som en nem vej ind i organisationer. Vurderingen indeholder også anbefalinger til, hvordan organisationer kan understøtte deres HR-afdelinger med både tekniske tiltag og awareness. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-hr-afdelinger/