CENTER FOR CYBERSIKKERHED

Trusselsvurdering: 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 opdateret med ændringer i kapitlerne om cyberaktivisme og cyberterror som følge af ændrede trusselsniveauer i den nationale trusselsvurdering "Cybertruslen mod Danmark" udgivet juni 2020. Ligesom i den nationale vurdering er der tilføjet et trusselsniveau for destruktive cyberangreb.

Dato: November 2019
Opdateret juni 2020

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

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

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 **HØJ**. Det betyder, at det er sandsynligt, at virksomheder eller myndigheder i luftfartssektorens vil blive ramt af forsøg på cyberspionage.

- 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 cyberaktivisme mod den danske luftfartssektor er **LAV**. Det betyder, at det er mindre sandsynligt, at virksomheder eller myndigheder i luftfartssektoren vil blive ramt af forsøg på cyberaktivisme. Truslen kan stige for den enkelte organisation i forbindelse med negativ medieomtale eller lignende.

- Truslen fra cyberterror mod den danske luftfartssektor er **INGEN**. Denne type angreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

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. Ransomwareangreb 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 høj. Statslige aktører har udvist særlig interesse for de personfølsomme oplysninger, som flyselskaber ligger inde med.

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 i høj grad af såkaldt ransomware. Ved et ransomware-angreb bliver data og systemer på offerets compu-

ter 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 e-mail, men ransomware-angreb kan også ske i form af f.eks. sms eller et reklamebanner på en hjemmeside.

Der findes mange varianter af ransomware. Mere målrettede ransomwareangreb forsøger at ramme eksempelvis administrative netværk i specifikke virksomheder og myndigheder.

Ransomwareangreb kan have alvorlige konsekvenser. Eksempelvis medførte et ransomwareangreb mod Clevelands Hopkins Internationale Lufthavn i april 2019 forstyrrelser og nedbrud på lufthavnens informationsskærme, i bagagehåndteringen og i lufthavnens interne mailsystemer.

Læs mere om, hvordan du beskytter din organisation mod ransomware i CFCS-vejledningen 'Reducér risikoen for ransomware' på FE's hjemmeside.

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 cyberkriminelle i stand til automatisk at kryptere filer på ofrets computer, slette originalerne og 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 e-mails på passagerer. De fik også adgang til passagerers kreditkortnumre og de tilhørende udløbsdatoer og 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 data-beskyttelsesforordning.

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. 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 pengeoverførelser. I stedet for at sende e-mails til en stor gruppe tilfældige medarbejdere i en virksomhed, laver hackerne grundig research. Det gør dem i stand til at lave troværdige, målrettede e-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.

CFCS og PET har udarbejdet en trusselsvurdering om cybertruslen fra bevidste og ubevidste insidere, som kan findes FE's hjemmeside. I trusselsvurderingen kan du læse mere om truslen og anbefalinger til mitigerende tiltag.

Cyberspionage

Truslen fra cyberspionage mod luftfartssektoren er **HØJ.** Det generelle niveau for cyberspionage mod Danmark er meget høj, da fremmede stater vedholdende forsøger at stjæle information fra staten og visse sektorer. Truslen er særligt udtalt mod de dele af staten, der beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitik. CFCS har ikke kendskab til et ligeså højt aktivitetsniveau mod den danske luftfartssektor. CFCS har dog kendskab til, at en organisation i sektoren har været kompromitteret af statsstøttede aktører. CFCS kender også til eksempler på statsstøttede aktører har forsøgt at kompromittere civile luftfartsmyndigheder i udlandet. CFCS vurderer, at fremmede stater både har intention og kapacitet til at udføre cyberspionage mod sektoren.

Hvor cyberkriminalitet i høj grad er drevet af grupper med et profitmotiv, er cyberspionage drevet af statsstøttede grupper, som ønsker adgang til viden. I luftfartssektoren har statsstøttede grupper især udvist interesse for teknologi, som kan bruges til at udvikle den pågældende stats egen luftfartssektor. Nogle statsstøttede aktører med betydelige kapaciteter 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 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. Eksempelvis blev FN's luftfartsorganisation ICAO udsat for et cyberangreb i november 2016. Det skete, da en statsstøttet aktør indsatte ondsindet kode i artikler på ICAOs hjemmeside. Formålet med kompromitteringen var sandsynligvis at komme videre ind i andre dele af luftfartsindustrien.

Hvis dokumenterne blev åbnet af en besøgende på hjemmesiden, risikerede deres computer at blive inficeret. Hvis en medarbejder hos en flyproducent eller i et medlemsland tilgik en af artiklerne, var der således risiko for, at aktøren fik adgang til organisationens netværk. Denne metode kaldes et vandhulsangreb.

Et vandhulsangreb dækker over en angrebsteknik, hvor en ellers legitim hjemmeside, f.eks. en webshop, inficeres med malware.

Brugere, der normalt benytter hjemmesiden uden problemer, risikerer at blive inficeret med malware. Ved et vandhulsangreb er hjemmesiden udvalgt for at ramme en specifik målgruppe, som benytter den regelmæssigt.

Statsstøttede grupper har ligeledes udvist interesse for persondata, sandsynligvis med henblik på at kortlægge bestemte personers og organisationers rejsemønstre.

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 luftfartssektor 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.

Cyberaktivisme

Truslen fra cyberaktivisme mod luftfartssektoren er **LAV.** Det betyder, at det er mindre sandsynligt, at luftfartssektoren 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 fra cyberaktivisme er ofte motiveret af en-

keltsager, og truslen mod sektoren kan derfor stige uden eller med kort varsel.

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. Verden over har der de seneste år været en række cyberaktivistiske angreb, f.eks. defacementangreb, rettet mod lufthavne og flyselskabers hjemmesider. CFCS har dog ikke kendskab til danske ofre for cyberaktivisme i luftfartssektoren.

Cyberaktivister angriber myndigheder og virksomheder, som hackerne betragter som symbolske mål. Det gør de, selvom de 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.

Cyberaktivister kan 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.

Luftfartssektoren udgør 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.

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.

Denne type alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

DDoS-angreb

Aktører benytter sig også af 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 tilgængeligt for legitim trafik, mens angrebet står på.

Luftfartssektoren bliver ramt af DDoS-angreb. I 2015 blev LOT Polish Airlines base i Warsawa Lufthavn f.eks. ramt af et DDoS-angreb, hvilket medførte, at ca. 1.400 passagerer midlertidigt strandede.

Læs mere om, hvordan du beskytter din organisation mod DDoS-angreb i CFCS vejledningen 'Sådan kan du imødegå DDoS-angreb' på FE'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

Usandsynligt | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**