Trusselsvurdering

Truslen fra destruktive cyberangreb

1. udgave juni 2021

Indhold

Destruktive cyberangreb 3
Hovedbudskab..... 3
Truslen fra destruktive cyberangreb mod Danmark 4
Stater udvikler kapaciteten til at udføre destruktive cyberangreb..... 5
Motiver bag destruktive cyberangreb 6
Angreb kan medføre fysisk ødelæggelse 6
Destruktive cyberangreb bruges oftest i forbindelse med konflikter..... 7
Stater udfører også omfattende forstyrrende cyberangreb 8
Rådgivning 9
Når sandsynligheden er lav og konsekvensen stor 9
Worst case - konsekvensvurdering..... 9
Beskyt kommunikation og kernesystemer..... 9
Beredskabsplanen skal kunne klare det uforudsete 10
Når skaden er sket.....10
Tiltag ved outsourcede løsninger 10
Det basale skal være på plads.....10
Trusselsniveauer 11

CENTER FOR CYBERSIKKERHED

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

1. udgave juni 2021.

Destruktive cyberangreb

Formålet med denne trusselsvurdering er at øge opmærksomheden hos danske beslutningstagere, myndigheder og virksomheder på truslen fra destruktive cyberangreb. Selvom truslen er **LAV**, vil succesfulde angreb få betydelige konsekvenser. Det er derfor vigtigt, at organisationerne forholder sig til truslen for at kunne imødegå den. Viden om truslen skal bl.a. kunne bruges til at prioritere tiltag hos den enkelte myndighed og virksomhed såvel som for Danmark som helhed.

Hovedbudskab

- Truslen fra destruktive cyberangreb mod Danmark er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder vil blive ramt af destruktive cyberangreb inden for de næste to år. Selvom truslen er lav, er det nødvendigt at forholde sig til den, da et vellykket angreb kan få alvorlige konsekvenser for de ramte.

- Det er sandsynligt, at flere stater udvikler deres kapacitet til at udføre destruktive cyberangreb. Det er dog mindre sandsynligt, at stater aktuelt har til hensigt at udføre destruktive cyberangreb mod Danmark.

- Destruktive cyberangreb udføres med det overordnede formål at skade eller ødelægge data, fysiske objekter eller medvirke til personskade eller død. Der findes dog en række mere specifikke underliggende motiver for brugen af destruktive cyberangreb, herunder sabotage, straffeaktioner, test og politisk signalgivning.

- Destruktive cyberangreb mod industrikontrolsystemer kan afbryde leveringen af samfundsvigtige ydelser og medføre fysisk ødelæggelse.

- CFCS vurderer, at destruktive cyberangreb oftest bliver brugt i forbindelse med konflikter eller geopolitiske spændinger mellem stater. Det betyder bl.a., at truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

- Stater udfører også omfattende forstyrrende cyberangreb, der har betydelige konsekvenser, selvom de ikke er direkte destruktive.

Hvad er destruktive cyberangreb?

CFCS definerer destruktive cyberangreb som cyberangreb, hvor den forventede effekt er:
- Død eller personskade
- Betydelig skade på fysiske objekter
- Ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning

Truslen fra destruktive cyberangreb mod Danmark

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Det betyder, at det er mindre sandsynligt, at danske virksomheder og myndigheder 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 udføre destruktive cyberangreb mod Danmark. Flere stater har dog kapacitet til at udføre destruktive cyberangreb. Tilstedeværelsen af kapacitet betyder, at truslen kan stige, hvis intentionen ændrer sig. Det kan ske i forbindelse med en skærpet konflikt eller geopolitiske spændinger med stater, der har kapacitet til at udføre destruktive cyberangreb.

Succesfulde destruktive cyberangreb kan have meget alvorlige konsekvenser. De kan potentielt lamme organisationers digitale infrastruktur, medføre fysisk skade og afbryde adgang til samfundsvigtige tjenester, såsom strøm eller telenet. Selvom truslen er **LAV,** bør myndigheder og virksomheder følge udviklingen i trusselsbilledet og berede sig på et angreb, netop fordi destruktive cyberangreb kan have så alvorlige konsekvenser.

Destruktive cyberangreb udføres med forskellige angrebsmetoder, og går fra at slette data i administrative systemer til at ødelægge fysiske komponenter i industrikontrolsystemer, hvilket potentielt kan medføre personskade.

Destruktive cyberangreb er fortsat sjældne. Langt de fleste destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data ved at slette eller kryptere dem uden mulighed for at genopretning.

Indtil nu er der ingen kendte tilfælde, hvor danske myndigheder og virksomheder har været udsat for destruktive cyberangreb, der var rettet specifikt mod dem. Dog blev f.eks. A.P. Møller-Mærsk ramt af det omfattende NotPetya-angreb, der ramte Ukraine og ofre verden over i 2017.

Stater udvikler kapaciteten til at udføre destruktive cyberangreb

Det er sandsynligt, at flere stater udvikler deres kapacitet til at udføre destruktive Cyberangreb. Eksempelvis har Rusland, Kina, Iran og Nordkorea kapacitet til at udføre destruktive cyberangreb. Stater bruger bl.a. cyberspionage, som en del af forberedelsen af destruktive cyberangreb.

Det er muligt, at fremmede stater har forsøgt at kompromittere danske samfundsvigtige virksomheder for at kunne udføre destruktive cyberangreb i Danmark på et senere tidspunkt. CFCS ser derfor med alvor på, at der i 2017 var flere målrettede forsøg på at få uautoriseret adgang til organisationer i den danske energisektor.

Forberedelsen af destruktive cyberangreb vil ofte bestå i en kortlægning af organisationer, systemer og netværksenheder, f.eks. industrikontrolsystemer. Ved at opnå viden om organisationer og systemer kan hackere udvikle specialiseret malware til brug for angrebsforsøg. Derudover kan hackere etablere såkaldte bagdøre på kompromitterede systemer, som de kan benytte i eventuelle senere destruktive angreb. Hvis hackere allerede har en bagdør i et system, vil de hurtigere kunne iværksætte et destruktivt angreb mod systemet. Derfor er en bagdør en alvorlig sikkerhedsbrist, selvom den ikke bliver udnyttet nu og her.

Eksempler på cyberangreb, der slettede data

Olympic Destroyer (2018) I februar 2018 blev de olympiske vinterlege i Sydkorea angrebet med wiper-malwaren Olympic Destroyer. Angrebet ramte tusindvis af computere. Hackerne brugte flere måneder på at forberede sig, ved at kompromittere og placere sig på netværk med tilknytning til vinterlegene. Wiper-malwaren blev aktiveret samme dag, som åbningsceremonien fandt sted. Det lykkedes dog lokale myndigheder at erstatte den digitale infrastruktur og kraftigt begrænse effekten af angrebet. Amerikanske myndigheder har anklaget Rusland for at stå bag angrebet.

NotPetya (2017) NotPetya-malwaren ramte i juni 2017 et meget stort antal computere og servere på verdensplan, og gjorde dem ubrugelige. NotPetya-angrebet havde sit udspring hos en kompromitteret ukrainsk softwarevirksomhed, som har udviklet softwaren M.E.Doc. Hackere leverede malware 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.

Strømafbrydelser i Ukraine (2015) I 2015 blev flere elselskaber i det vestlige Ukraine ramt af cyberangreb. Hackerne fik adgang til elselskabernes SCADA-systemer og afbrød strømmen til mere end 225.000 ukrainske kunder. Under angrebet brugte hackerne bl.a. wiper-malwaren Killdisk til at slette logs og filer. Det lykkedes dog, ved hjælp af manuelle back-up systemer, at få strømmen tilbage til de ukrainske kunder indenfor seks timer.

Sony-hacket (2014) Hackere angreb i 2014 filmselskabet Sony Pictures Entertainment, hvor de ødelagde data og systemer og lækkede bl.a. mails og kopier af film, der endnu ikke var udkommet.

Motiver bag destruktive cyberangreb

Formålet med destruktive cyberangreb er at ødelægge og skade, men der er forskellige mere specifikke motiver bag angrebene. Et bagvedliggende motiv for destruktive cyberangreb kan eksempelvis være at udføre sabotage. Sabotage kan bl.a. indebære, at en aktør udfører et angreb for at afbryde eller forhindre en modstanders adgang til et system, en teknologi eller information. Motivet kan også være en straffeaktion i forbindelse med en konflikt, hvor målet med angrebet er, at offeret påføres økonomiske eller andre ressourcemæssige omkostninger. Et motiv med destruktive cyberangreb kan derudover være at sende et signal til offeret samt andre potentielle ofre. Endelig kan et destruktivt cyberangreb blive udført for at teste og potentielt udvikle en kapacitet eller slette spor efter et angreb med et andet formål

Det er ofte vanskeligt at vurdere præcis, hvilken hensigt der ligger bag et destruktivt cyberangreb. Det er desuden sandsynligt, at et angreb kan tjene flere formål.

Et af de mest omfattende destruktive cyberangreb i verden, NotPetya, kan have tjent flere formål. Angrebet startede i Ukraine i 2017 dagen før den ukrainske uafhængighedsdag og spredte sig derefter globalt. Flere lande har tilskrevet angrebet til Rusland. Angrebet kan dels tolkes som en straf af Ukraine, som Rusland var i konflikt med. Men det kan også tolkes som et signal til omverdenen, om at der er risici forbundet med at drive virksomhed i Ukraine.

Angreb kan medføre fysisk ødelæggelse

Destruktive cyberangreb mod industrikontrolsystemer, der understøtter leveringen af samfundsvigtige ydelser, kan få særligt alvorlige samfundsmæssige konsekvenser. Dels kan angreb på den type systemer afbryde leveringen af vitale ydelser såsom strøm og internet, men de kan også medføre ødelæggelse af fysiske objekter og personskade.

Det kan ske, fordi industrikontrolsystemer styrer, overvåger og kontrollerer industriprocesser, f.eks. sikkerhedsmekanismer, der kan skabe farlige situationer, hvis de afbrydes, manipuleres eller standses.

Industrikontrolsystemer

Begrebet industrikontrolsystemer dækker både over SCADA (Supervisory Control and Data Acquisition) og ICS (Industrial Control System).

SCADA og ICS er netværksopkoblede enheder til styring af industrielle systemer. Det er systemer, som anvendes til overvågning og styring af mekaniske systemer, også kaldet OT-systemer. Når SCADA eller ICS benytter IP-netværk og eventuelt er forbundet via internettet, kaldes begrebet Industrial Internet of Things.

Der er dog fortsat kun få eksempler, hvor det er sandsynligt, at destruktive cyberangreb er blevet udført med det formål at skade fysiske objekter.

Det hidtil eneste kendte destruktive cyberangreb, der har medført reel fysisk ødelæggelse, ramte Iran i 2010. Hackerne brugte malwaren Stuxnet mod iranske centrifuger til berigelse af uran. Angrebet ødelagde centrifugerne.

Få andre destruktive cyberangreb kunne havde medført fysisk ødelæggelse, hvis de var lykkedes. Det er bl.a. muligt, at cyberangrebet mod industrikontrolsystemet Triconex i Saudi Arabien i 2017 kunne have skabt fysisk ødelæggelse. Angrebet var rettet mod en petrokemisk industrivirksomhed og systemet Triconex, som den ramte virksomhed brugte. Triconex sørger bl.a. for, at produktionssystemer bliver lukket ned på en kontrolleret og sikker måde, hvis der opstår kritiske fejl eller problemer. Angrebet kunne potentielt have medført fysisk ødelæggelse, men sikkerhedssystemerne lukkede ned på en ufarlig måde. Nedlukningen betød også, at malwaren blev opdaget. Hvis sikkerhedsmekanismerne var blevet slået fra eller manipuleret med, kunne det have øget risikoen for personskade eller død på og omkring virksomheden, som følge af enten udslip af farlige gasser eller eksplosioner.

Det destruktive cyberangreb, der ramte Ukraines elforsyning i 2016, kunne også havde medført fysisk skade på udstyr. It-sikkerhedseksperter har bl.a. vist indikationer på, at angrebet var planlagt til at ramme kontrolswitches og beskyttelsesrelæer med overbelastningsangreb. Hvis det var lykkedes at ramme dem, kunne det havde medført længerevarende strømafbrydelser. Hackerne havde dog ikke succes med den del af angrebet.

Stater retter sandsynligvis destruktive cyberangreb mod kritisk infrastruktur, herunder industrikontrolsystemer hos samfundsvigtige virksomheder, fordi de derved kan ramme deres modstander, hvor det gør mest ondt. Mange virksomheder bruger de samme industrikontrolsystemer, hvilket betyder, at hackere kan opbygge metoder til at ramme mange mål i lignende systemer i fremtidige konflikter.

Destruktive cyberangreb bruges oftest i forbindelse med konflikter

CFCS vurderer, at destruktive cyberangreb oftest bliver udført af stater i forbindelse med konflikter eller geopolitiske spændinger. Truslen kan derfor stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der har evnen til at gennemføre destruktive cyberangreb.

Destruktive cyberangreb mod mål i Mellemøsten

2012
Shamoon 1
Det saudiske nationale olie- og gasselskab, Saudi Aramco, blev i 2012 udsat for et cyberangreb, der ødelagde en stor mængde data tilhørende selskabet. Mere end 30.000 PC blev ødelagt af wiper-malwaren.

2017
Shamoon 2
I 2017 blev en række organisationer på tværs af sektorer, bl.a. energi-, transport- og finanssektoren, i Saudi Arabien ramt af en ny variant af wiper-malwaren Shamoon.

2018
Shamoon 3
I december 2018 blev endnu en variant af Shamoon malwaren brugt i cyberangreb på organisationer inden for olie-, gas- og mineindustri i Saudi Arabien og Forenede Arabiske Emirater.

2019
ZeroClear rammer flere ofre
Wiper-malwaren Zeroclear ramte ofre i energi-, olie- og gassektoren på tværs af Mellemøsten

Angreb mod Bahrains energisektor
Den 29. december 2019 blev Bapco, Bahrains nationale olieselskab, ramt af et wiper-angreb med malwaren DUSTMAN, der var en ny version af ZeroClear.

2020

Israel afværgede angreb på kraftværk (januar)
Hackere forsøgte at lamme et israelsk kraftværk.

Angreb mod vandværker i Israel (april)
Hackere angreb vandværker i Israel og forsøgte bl.a. at ændre indholdet af klor i drikkevandet. Angrebet blev afværget, uden at det gjorde større skade.

Angreb på iransk havn (maj)
Hackere forstyrrede driften i en af Irans største havne, Shahid Rajaee portterminal, hvilket skabte forsinkelser og kaos.

Nye angreb på israelske vandværker (juni)
Israelske myndigheder udtalte offentligt, at de havde afværget angreb på to vandværker.

Angreb mod Irans havnemyndighed (oktober)
Iranske myndigheder udtalte offentligt, at de havde afværget angreb mod Irans havnemyndighed. Formålet var ifølge myndighederne at forstyrre transport af varer.

I konfliktområder, hvor stater bruger destruktive cyberangreb mod civile mål, kan truslen fra destruktive cyberangreb være højere. Danske virksomheder, der arbejder globalt, kan blive ramt af angreb, som ikke er rettet mod Danmark, men mod virksomheder der opererer i konfliktområder.

Truslen fra destruktive cyberangreb kan også blive skærpet for danske virksomheder, som arbejder for virksomheder eller stater, der er mål for destruktive cyberangreb.

Det er muligt, at danske virksomheder og myndigheder, der er til stede i konfliktområder, særligt i Ukraine og Mellemøsten, kan blive ramt af følgevirkninger af destruktive cyberangreb, såsom strømafbrydelser eller afbrudt netværksforbindelse.

I forbindelser med konflikter i udlandet er visse samfundsvigtige sektorer blevet ramt af destruktive cyberangreb. Særligt energi-, tele-, transport- og finanssektoren har været under angreb i kriser. Enkelte angreb mod disse sektorer har været rettet mod industrikontrolsystemer.

Kritisk infrastruktur ramt af destruktive cyberangreb i Ukraine

Ukraine er flere gange blevet udsat for cyberangreb i forbindelse med landets konflikt med Rusland. Udover angreb mod energisektoren i 2015 og 2016 er Ukraines finans- og transportsektor også blevet ramt flere gange. Blandt andet blev Ukraines finansministerium og Centralbank angrebet i 2016. Angrebet medførte bl.a., at 150.000 elektroniske overførsler blev stoppet. I oktober 2020 anklagede amerikanske myndigheder seks navngivne russiske statsborgere for at stå bag angrebet. Ifølge de amerikanske myndigheder arbejdede hackerne for en russisk efterretningstjeneste.

Ukraines transportsektor blev i 2017 også ramt af angreb med BadRabbit-malwaren. Angrebet medførte bl.a. flyforsinkelser i Odessa lufthavn og nedbrud i billetsystemet i Kievs metro. Tidligere i 2017 blev flere virksomheder i Ukraines transportsektor også ramt af NotPetya-angrebet.

Stater udfører også omfattende forstyrrende cyberangreb

Stater udfører også alvorligt forstyrrende cyberangreb, der ikke falder ind under CFCS' definition af destruktive cyberangreb, men alligevel har betydelige konsekvenser. Blandt andet bruger stater angrebsmetoderne overbelastningsangreb, f.eks. DDoS-angreb, og defacement-angreb til at udføre forstyrrende cyberangreb. Angrebsmetoderne er ikke destruktive, idet de ikke ødelægger eller skader data eller objekter. Omfattende forstyrrende angreb er sjældne, men har i få tilfælde i udlandet

resulteret i afbrydelse eller forstyrrelser af adgangen til og driften af mange eller vitale digitale systemer og tjenester.

I efteråret 2019 blev den georgiske web-hostingudbyder Pro Service ramt af et alvorligt forstyrrende angreb. Både amerikanske og britiske myndigheder har offentligt anklaget russiske statsstøttede hackere for at stå bag angrebet. De britiske myndigheder udtalte bl.a., at angrebet blev udført med det formål at skabe ustabilitet og underminere Georgiens suverænitet.

Cyberangrebet mod Pro Service førte til, at over 2.000 georgiske hjemmesider, der bl.a. tilhørte den georgiske regering, præsidentkontoret, civile domstole, lokale byråd, banker, NGO'er samt større virksomheder og nyhedsmedier i Georgien, blev udsat for såkaldte defacement-angreb. Det originale indhold på de mange hjemmesider blev erstattet af et foto af Georgiens tidligere præsident, Mikheil Saakashvili, med teksten "I'll be back". Herefter lukkede hackerne hjemmesiderne ned, de var dog online igen efter 24 timer.

Den amerikanske finanssektor blev mellem december 2011 og september 2012 udsat for en omfattende og langvarig bølge af DDoS-angreb. Angrebene fik alvorlige følger for sektoren, bl.a. blev hjemmesider utilgængelige, kunder mistede adgang til deres onlinekonti, og remediering af angrebene kostede banker flere millioner dollars. Amerikanske myndigheder anklagede i 2016 iranske hackere for at have udført angrebene på vegne den iranske stat.

Rådgivning

Når sandsynligheden er lav og konsekvensen stor

En forudsætning for at en organisation har mulighed for at håndtere destruktive cyberangreb er, at der er en velfungerende sikkerhedsorganisation og at de basale sikringstiltag er på plads.

Worst case - konsekvensvurdering
I det mindre sandsynlige tilfælde, hvor en organisation rammes af et destruktivt cyberangreb, er der tale om en hændelse, der kan have endog meget alvorlige konsekvenser. Hvis en organisation vælger at forberede sig på at kunne håndtere en sådan hændelse, anbefaler Center for Cybersikkerhed, at der gennemføreres en "worst case"- konsekvensvurdering, der stiller skarpt på de hændelser og situationer, der kan have de største destruktive konsekvenser for forretningen og forholder sig aktivt til disse.
Organisationen bør gennemgå de eksisterende forebyggende, opdagende og korrigerende sikringstiltag med henblik på at tilpasse disse – og de anvendte ressourcer - efter, hvad man kan tåle at miste, og hvad der absolut skal kunne beskyttes.

Beskyt kommunikation og kernesystemer
Erfaringerne fra de destruktive cyberangreb viser, at det er vigtigt at kunne genetablere organisationens kommunikationssystemer, som en forudsætning for at kunne håndtere hændelsen på effektiv vis. IP-telefoni og mail bliver ofte ramt som

følge af et destruktivt cyberangreb mod de centrale systemer. Samtidig er det i sådan en situation vigtigt at kunne kommunikere internt og med kunder og partnere.
Det er også kritisk at beskytte de centrale it-systemer, som mange af de øvrige it-systemer er afhængige af. Det kan for eksempel være systemer til identitets- og adgangsstyring, som er en forudsætning for, at både medarbejdere og it-tjenester kan kommunikere indbyrdes. Disse systemer kan være meget omkostningstunge og tidskrævende at gendanne fra grunden uden en pålidelig backup eller en redundant installation.

Beredskabsplanen skal kunne klare det uforudsete
Destruktive cyberangreb kan have konsekvenser, der er svære at forudse. Derfor er det vigtigt at udarbejde beredskabsplaner, der fokuserer på den generelle håndtering af kriser. Det kan være nødvendigt at udarbejde forskellige planer. Én plan kan for eksempel dække over afgrænsede hændelser, der strækker sig over kort tid. En anden plan kan være beregnet til større hændelser, der strækker sig over længere tid. Når en krise strækker sig over længere tid, er der flere praktiske udfordringer, planen skal tage hånd om. Det kan for eksempel være transport lokalt og globalt, forplejning og midlertidig indkvartering af det personale, der arbejder på at gendanne it-systemerne.

Når skaden er sket
Endelig anbefaler Center for Cybersikkerhed, at organisationen gennemgår, tilpasser og tester sit beredskab så beredskabsplaner og krisehåndtering er dimensioneret til at kunne håndtere de mindre sandsynlige, men meget kritiske scenarier, som "worst case"- konsekvensvurderingen har identificeret. Et velfungerende beredskab kan være medvirkende til at konsekvenserne ved en destruktiv sikkerhedshændelse kan begrænses.

Tiltag ved outsourcede løsninger
Er hele eller dele af organisationens it-infrastruktur outsourcet til en ekstern leverandør anbefaler Center for Cybersikkerhed, at leverandøren altid involveres i arbejdet med at sikre imod destruktive angreb. Leverandøren bør involveres i forbindelse med afdækning af trusler, sårbarheder og tekniske konsekvenser. Også i forbindelse med etablering af grundlæggende sikringstiltag, bør leverandører af it-infrastruktur være tæt involveret.

Det basale skal være på plads
Som sagt er forudsætningen for at kunne håndtere destruktive cyberangreb, at organisationen har den basale sikkerhed på plads. Enhver organisation bør som minimum leve op til følgende råd:

- Cybersikkerhed skal forankres i topledelsen
- Organisationen skal selv have eller kunne trække på de rette tekniske kompetencer
- Uddan og træn især ledelse, men også medarbejderne
- Sørg for at have et gennemprøvet beredskab

En konkretisering af rådene kan læses i Center for Cybersikkerheds vejledning "Cyberforsvar der virker" og i anbefalingerne vedrørende leverandørforhold "Informationssikkerhed i leverandørforhold" samt i CFCS' øvrige vejledninger og trusselsvurderinger.

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**

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