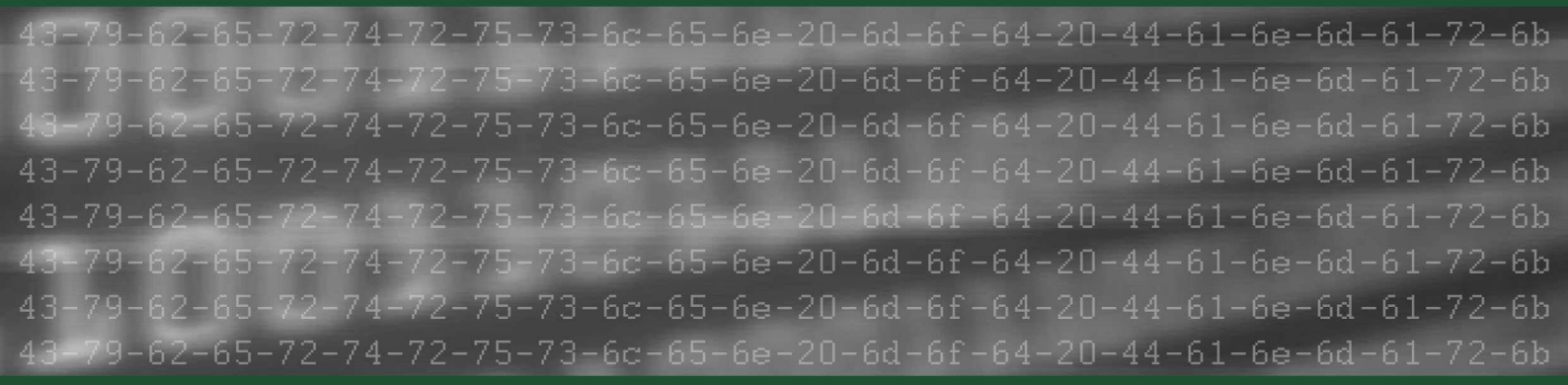
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Januar 2016

CENTER FOR CYBERSIKKERHED

Cybertruslen mod Danmark

Vurderingen redegør for det trusselsbillede, der møder danske myndigheder og private virksomheder på internettet.

Vurderingen er skrevet af Center for Cybersikkerheds Trusselsvurderingsenhed, som har til formål at sætte myndighederne og virksomhederne i særligt kritiske og samfundsvigtige sektorer bedre i stand til at imødegå cybertrusler ved at supplere de varslinger, myndighederne og virksomhederne kan få fra anden side.

Hovedvurdering

Spionage mod offentlige myndigheder og private virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske interesser. Spionagen udføres primært af statslige og statsstøttede grupper. Gennem de seneste år er omfanget af cyberspionage mod Danmark steget betydeligt, og gruppernes metoder og teknikker er blevet mere avancerede.

Truslen fra cyberspionage mod danske myndigheder og private virksomheder er **MEGET HØJ**.

Samlet set er cyberkriminalitet stigende i omfang og kompleksitet, og det rammer både myndigheder og alle typer private virksomheder. Særligt mindre virksomheder, som også er økonomisk sårbare, kan blive truet på sin eksistens af cyberkriminalitet. Der er konstant opdaterede teknologiske værktøjer tilgængelige og stor villighed til at anvende dem i kriminelle miljøer.

Truslen fra cyberkriminalitet mod danske myndigheder og private virksomheder er **MEGET HØJ**.

Uagtet den nemme adgang til værktøjer og dermed kapacitet på internettet ses der ikke mange alvorlige eksempler på Cyberaktivisme mod danske myndigheder og private virksomheder. Der er dog både kapacitet og en generel hensigt om at angribe myndigheder og virksomheder, der opfattes som modstandere. Hvis en myndighed eller virksomhed påkalder sig hacktivisters opmærksomhed, kan truslen uden varsel stige til høj eller meget høj.

Truslen fra cyberaktivisme mod danske myndigheder og private virksomheder er **MIDDEL**.

I yderste konsekvens kan cyberterror medføre tab af liv og ødelæggelse af ejendom eller omfattende finansielle tab, som kan få samfundsmæssige konsekvenser for Danmark.

Trusselsvurderingsenheden vurderer, at særligt militante, islamistiske grupper som ISIL over tid vil tilegne sig cyberkapaciteter med henblik på at kunne gennemføre skadevoldende angreb, men at de aktuelt kun har ringe kapacitet til at gennemføre deciderede terrorangreb gennem internettet.

Truslen fra cyberterror mod myndigheder og private virksomheder er **LAV**.

Trussel	Niveau
Truslen fra cyberspionage	Meget høj
Truslen fra cyberkriminalitet	Meget høj
Truslen fra cyberaktivisme	Middel
Truslen fra cyberterror	Lav

Indledning

Danmark er et af de mest digitaliserede samfund i verden. Både offentlige og private sektorer er i stigende grad afhængige af internettet. Digitaliseringen skaber muligheder for hurtig udveksling af viden og serviceydelser, men også for ondsindet udnyttelse. Omfanget af cybertrusler stiger fortsat i og mod den vestlige verden og dermed også mod Danmark. Samtidig gør den teknologiske udvikling, at truslerne er i konstant forandring, hvilket stiller store krav til vedholdende sikkerhedsforanstaltninger og beredskab.

Denne trusselsvurdering beskriver og vurderer hovedtyperne af de forskellige cybertrusler, der rammer danske netværk, ud fra en aktørvinkel og anbefaler, hvordan de kan imødegås. Vurderingen er udarbejdet af Center for Cybersikkerheds Trusselsvurderingsenhed, som er oprettet på baggrund af den nationale strategi for cyber- og informationssikkerhed. Af strategien fremgår endvidere, at cybertrusler skal indgå i myndighedernes risikovurderinger og risikoledelse. Med denne trusselsvurdering kan cybertrusler også indgå i virksomhedernes arbejde med cyber- og informationssikkerhed.

Der er store mørketal i viden om omfanget af cybersikkerhedshændelserne i både myndigheder og samfundsvigtige private virksomheder. Af flere årsager ønsker særligt private virksomheder at undgå opmærksomhed om konkrete hændelser, hvilket medfører et mindre klart billede af specifikke tendenser i enkelte sektorer. Trusselsvurderingsenheden har til opgave at samarbejde med myndigheder og private virksomheder, så den fælles viden om og forståelse af truslerne forbedres. Det bemærkes i den forbindelse, at statslige myndigheder siden juli 2014 har haft pligt til at indrapportere alvorlige sikkerhedshændelser til Center for Cybersikkerhed, og at private virksomheder ved samme lejlighed også blev opfordret til at rapportere alvorlige hændelser til centeret.

Trusselsbilledet

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering fokuseres der på, hvilket formål aktøren bag den enkelte trussel har, og hvor alvorlige konsekvenserne af truslerne kan være

for den ramte myndighed eller virksomhed. Vurderingen af trusselsniveauerne sker på baggrund af det aktuelle trusselsbillede, som har en varslingshorisont på 0-2 år. Da trusselsbilledet er dynamisk, kan det på nogle områder ændre sig med kort eller uden varsel både generelt og for den enkelte myndighed og private virksomhed.

Når Center for Cybersikkerhed har konkret viden om trusler eller angreb mod danske myndigheder eller virksomheder, varsler centeret direkte myndigheden eller virksomheden.

Cyberspionage

Formålet med cyberspionage er at indhente informationer, som eksempelvis følsomme eller klassificerede informationer, intellektuel ejendom, forretningsplaner mv. Indhentningen kan være strategisk, politisk og økonomisk motiveret. Cyberspionage søges gennemført skjult, og ofte opdager ofret ikke, at det foregår.

Der er de seneste år sket en betydelig stigning i antallet af forsøg på at udføre cyberspionage mod Danmark og danske interesser. Samtidigt er statsstøttede og statslige grupper blevet mere avancerede i deres metoder, fremgangsmåder og bestræbelser på at skjule deres aktiviteter og identitet. De mere avancerede statsstøttede hackergrupper målretter deres aktivitet mod offentlige myndigheder med strategisk viden og højteknologiske private virksomheder, der bliver forsøgt ramt.

Center for Cybersikkerhed har det seneste år adskillige gange opdaget og afhjulpet cyberspionage mod danske myndigheder og private virksomheder. Som eksempel er der næsten daglige angrebsforsøg mod Udenrigsministeriets netværk, som Center for Cybersikkerhed tilskriver fremmende stater og statsstøttede grupper. Ligeledes er flere ngo'er også blevet angrebet, og Center for Cybersikkerhed samarbejder løbende med danske ofre, der er blevet angrebet. Trusselsvurderingsenheden vurderer, at truslen fra cyberspionage ikke kun er rettet mod de centrale myndigheder og større virksomheder. Hvis en myndighed eller virksomhed besidder viden, andre stater eller virksomheder ønsker indsigt i, kan den blive et mål.

Det kan være særdeles vanskeligt for myndigheder og private virksomheder at opdage cyberspionage eller vurdere konsekvenserne af den, selv når aktiviteterne opdages. Den yderste konsekvens af cyberspionage for en virksomhed er, at den mister sit marked og går konkurs. Der er endnu ikke kendte eksempler på, at danske virksomheder er gået konkurs pga. cyberspionage.

De statsstøttede hackergrupper bruger i højere grad end tidligere organisationer, hvis netværk de allerede har adgang til, som angrebsplatforme til at ramme mål med en større sikkerhedsbevidsthed. Myndigheder og virksomheder, som ikke i sig selv er et mål for et cyberangreb, kan altså blive det som et middel til det egentlige mål for angrebet, hvilket bør medtages i risikostyringen.

Truslen mod danske myndigheder

Truslen fra cyberspionage mod danske myndigheder er MEGET HØJ. Det er meget sandsynligt, at flere danske myndigheder er prioriterede mål for statslige og statsstøttede grupper, og at denne udvikling vil fortsætte. I takt med at hackergrupperne udvikler deres teknikker og kapaciteter, stiller det stadigt stigende krav til myndighedernes sikkerhedsniveau, så der reelt er tale om et konstant cyber-kapløb.

Enkelte fremmede stater går målrettet efter danske myndigheder i forsøg på at indhente informationer om bl.a. danske udenrigs-og sikkerhedspolitiske forhold. Eksempelvis står fremmede stater bag flere kampagner i 2015, der har været målrettet centraladministrationen og andre offentlige myndigheder.

Danske myndigheders deltagelse i internationale forhandlinger og samarbejde giver ofte anledning til forsøg på cyberspionage. I 2014 blev flere medarbejdere ved danske myndigheder forsøgt hacket i forbindelse med internationalt samarbejde om et forskningsprojekt. En udenlandsk efterretningstjeneste stod bag forsøgene.

Truslen mod danske virksomheder

Der er generelt en MEGET HØJ trussel fra cyberspionage mod danske virksomheder. Flere statsstøttede hackergrupper er gået målrettet efter danske virksomheder i de seneste år, og denne udvikling ventes at fortsætte.

Eksempelvis var der i 2014-2015 et alvorligt cyberangreb, hvor en dansk virksomhed og dennes underleverandør var mål for cyberspionage gennem mere end et år. Den statsstøttede hackergruppe bag hændelsen havde fuld adgang til begge virksomheders netværk og kunne hente forretningshemmeligheder fra virksomhedernes computere og servere. Gruppen kunne også optage lyd fra de indbyggede mikrofoner i virksomhedernes computere samt tage skærmbilleder og registrere tastetryk, uden at virksomhederne opdagede det.

Det er meget sandsynligt, at danske virksomheder i fremtiden vil blive udsat for stadig flere avancerede forsøg på cyberspionage. Det gælder særligt større virksomheder inden for forskningstunge sektorer, hvor Danmark er langt fremme udviklingsmæssigt og har en stærk position på det globale marked. Det er meget sandsynligt, at en række danske virksomheder har mistet vigtige forretningshemmeligheder og intellektuel ejendom på grund af cyberspionage de seneste år. Også for virksomhederne er der tale om et cyber-kapløb mellem hackernes tekniske udvikling og kapacitet på den ene side og virksomhedernes sikkerhedstiltag og risikostyring på den anden.

Hidtil har kriminelle grupper ikke været tilstrækkeligt organiserede og teknisk dygtige nok til at gennemføre egentlig cyberspionage på niveau med de statsstøttede og statslige grupper, men den seneste udvikling tyder på, at nogle kriminelle grupper begynder at opnå kapacitet til cyberspionage. Dermed stiger truslen mod virksomheder, hvis konkurrerenter kan opnå konkurrencefordele gennem betalt cyberspionage ved cyberkriminelle.

Spear-phishing
Et spear-phishing-angreb er målrettet enkeltpersoner i en organisation. Formålet kan være at hente fortrolige forretningsoplysninger, bruger-id og adgangskoder til konti mv. ud af organisationen. Disse oplysninger vil så sammen med en mulig infektion af modtagerens computer, tablet eller mobiltelefon kunne anvendes i forbindelse med et decideret cyberangreb mod organisationen.
Kilde: Sikkerhedsanbefaling: Spear-phishing - et voksende problem, Center for Cybersikkerhed

Truslen fra cyberspionage

Spionage mod offentlige myndigheder og private virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske interesser. Spionagen udføres primært af statslige og statsstøttede grupper. Gennem de seneste år er omfanget af cyberspionage mod Danmark steget betydeligt, og gruppernes metoder og teknikker er blevet mere avancerede.

Truslen fra cyberspionage mod danske myndigheder og private virksomheder er **MEGET HØJ**.

Cyberkriminalitet

I denne trusselsvurdering dækker begrebet Cyberkriminalitet handlinger, hvor gerningsmanden bruger it til at begå kriminalitet mod myndigheder og private virksomheder. I denne kontekst er der fokuseret på Cyberkriminalitet mod myndigheder og private virksomheder, hvor formålet er økonomisk vinding.

Cyberkriminalitet, der beror på økonomisk vinding, er typisk bedrageri i forskellige former samt afpresning med ransomware, overbelastningsangreb og uberettiget adgang til data med henblik på afpresning eller videresalg og brud på immaterielle rettigheder. Kriminelle grupperinger har vist stor opfindsomhed og teknisk formåen til økonomisk motiveret cyberkriminalitet.

Den 7. december rapporterede sikkerhedsfirmaet FireEye om en trusselsaktør kaldet FIN1. Gruppen er begyndt at anvende en særligt sofistikeret malware, som eksekveres inden operativsystemet starter. Det gør det meget vanskelligt at detektere, ligesom det ikke fjernes ved en almindelig geninstallering af systemet. Gruppen er kendt for at stjæle kreditkort data fra finansielle institutioner som banker og kreditforeninger. Malwaren giver adgang til ofrets netværk og kan også bruges til cyberspionage.
Kilde: https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

Politiet modtager også anmeldelser om faktureringssvindel. Et eksempel på faktureringssvindel er, at kriminelle beder et firma om at omadressere en betaling ved at bruge en mail, der ligner en eksisterende kundemail. Der er i disse sager set tab på flere hundrede tusinde kroner.

Afpresning med ransomware mod danske virksomheder og myndigheder er voksende i omfang og kompleksitet. De kriminelles muligheder er mange, idet de tekniske ressourcer til at gennemføre en ransomware kampagne kan købes online. Flere af de episoder, der er kommet til politiets kend-

skab i 2015, har vist både opfindsomhed og tekniske kompetencer. Eksempelvis var der i efteråret 2015 en bølge af ransomware-mails, der foregav at komme fra Post Nord og indeholdt information om en pakke til modtageren, som ikke var blevet leveret. Modtageren blev opfordret til at klikke på et link for at få yderligere oplysninger om forsendelsen. Ved klik på linket blev ransomware programmet aktiveret og igangsatte kryptering af data lokalt og på alle tilgængelige netværksdrev. De krypterede data skulle derefter købes tilbage ved de kriminelle bagmænd eller genetableres fra backup eller på anden vis.

Ransomware

Et ransomware-angreb foregår typisk ved, at et it-system inficeres med et stykke malware som følge af, at en person i god tro har åbnet vedhæftede filer eller links i en ondsindet e-mail. Malwaren krypterer herefter alt indholdet på ofrets harddisk og de drev, der er skriveadgang til. Når krypteringen er fuldført, vil ofret få en besked fra angriberne, som lover at dekryptere ofrets data mod betaling af en løsesum – deraf navnet ransomware.

Kilde: SIKKERHEDSBULLETIN 1/2015 fra Center for Cybersikkerhed

De cyberkriminelle bruger i stigende grad social engineering teknikker til at gøre deres mails troværdige, så de dermed kan lokke modtagerne til at aktivere den anvendte malware.

Overbelastningsangreb er, ligesom ransomware, tilgængelige online som en serviceydelse for kriminelle, der ikke selv besidder tilstrækkelige tekniske færdigheder til at gennemføre et angreb. Overbelastningsangreb bruges også til afpresning for økonomisk vinding, og løsesummen opkræves ofte i Bitcoins. De kriminelles kompetence er også stor på dette område.

De økonomiske konsekvenser ved både ransomware og overbelastningsangreb er potentielt meget store i form af eksempelvis tabte data, eller hvis virksomheden i en periode ikke kan sælge via deres hjemmeside. De samfundsmæssige konsekvenser ved den slags angreb på offentlige myndigheder vurderes ligeledes at være potentielt store. Det kan eksempelvis være, hvis udbetalingen af offentlige ydelser og services hindres gennem en længere periode.

Den 3. december 2015 rapporterede Wired.com om en hacker, der kalder sig Hacker Buba. Han hackede en bank i De Forenede Arabiske Emirater og truede banken med at offentliggøre stjålne kundedata, hvis ikke banken betalte løsesum. Da banken nægtede, lagde han data på mere end 500 bankkunder på Twitter.

Truslen fra cyberkriminalitet

Samlet set er cyberkriminalitet stigende i omfang og kompleksitet, og det rammer både myndigheder og alle typer private virksomheder. Særligt mindre virksomheder, som også er økonomisk sårbare, kan blive truet på sin eksistens af cyberkriminalitet. Der er konstant opdaterede teknologiske værktøjer tilgængelige og stor villighed til at anvende dem til digital kriminalitet.

Truslen fra cyberkriminalitet er **MEGET HØJ**.

Cyberaktivisme

Cyberaktivisme eller hacktivisme har til formål at formidle et holdningsmæssigt eller politisk budskab ved at hacke en hjemmeside eller et computernetværk og der efterlade sit budskab. Den person, der udfører handlingen kaldes en hacktivist.

Cyberaktivisme kan sidestilles med en form for civil ulydighed gennem internettet. Cyberaktivisme kan bl.a. omfatte defacement af websider, som er en form for cybervandalisme, hvor hacktivisten ændrer hjemmesidens udseende og evt. efterlader holdningsmæssige budskaber, overbelastningsangreb – Distributed Denial-of-Service angreb (DDoS), omdirigeringer og tyveri af information.

Der har været mindre overbelastningsangreb på offentlige hjemmesider fra enkeltpersoner og mindre grupper af hacktivister. Hacktivisterne søger at skabe offentlig opmærksomhed om et givet emne, og truslen fra hacktivister er derfor primært rettet mod organisationer, som har politisk, geografisk eller anden tilknytning til emnet. De politisk motiverede angreb har medført, at hjemmesider er blevet overtaget og brugt til at sprede propaganda, eller at en kritisk komponent er blevet overbelastet med nedbrud af systemet til følge. Det var tilfældet ved et angreb mod NemID i april 2013. Det er meget sandsynligt, at denne form for politisk aktivisme vil fortsætte og øges.

DDoS mod Island

Fredag den 27. november 2015 gennemførte hacktivister med forbindelse til Anonymous et DDoS angreb mod fem hjemmesider, der tilhører den islandske regering. Angrebet var en del af en kampagne mod hvalfangst. Adgangen til hjemmesiderne var blokeret i 13 timer pga. DDoS-angrebet.
Kilde:
http://icelandmonitor.mbl.is/news/politics_and_society/2015/11/30/iceland_hit_by_whaling_cyber_attack/

Den nemme adgang til værktøjer på internettet til eksempelvis at udføre overbelastningsangreb betyder, at hackerne ikke behøver at have stærke tekniske forudsætninger for at forstyrre danske hjemmesider og servere. Det er endvidere fortsat muligt for teknisk dygtige enkeltpersoner at skaffe sig adgang til selv store offentlige og private organisationer, hvis der her ikke er fokus på sikkerheden.

Klimatopmødet i Paris, COP21

Hackergruppen Anonymous har offentliggjort mere end 1.000 delegeredes login oplysninger, ifølge The Guardian den 3. december 2015. Afsløringerne har begrænset praktisk betydning, men afslører et potentielt tvivlsomt niveau af cybersikkerhed på topmødet

Kilde: http://www.theguardian.com/environment/2015/dec/03/paris-climate-summit-hackers-leak-login-details-of-more-than-1000-officials

Truslen fra cyberaktivisme

Uagtet den nemme adgang til værktøjer og dermed kapacitet på internettet ses der ikke mange eksempler på Cyberaktivisme mod danske myndigheder og private virksomheder. Der er dog både kapacitet og en generel hensigt om at angribe myndigheder og virksomheder, der opfattes som modstandere. Hvis en myndighed eller virksomhed påkalder sig hacktivisters opmærksomhed, kan truslen uden varsel stige til høj eller meget høj.

Truslen fra cyberaktivisme mod danske myndigheder og private virksomheder er generelt **MIDDEL**.

Cyberterror

Cyberterror er politisk motiveret, og formålet er det samme som for terrorhandlinger generelt, at skabe opmærksomhed på terrorgruppens sag gennem voldsomme handlinger, som ofte medfører fysisk destruktion eller drab, der fremkalder frygt i befolkningen. De mere simple cyberangreb, som f.eks. et overbelastningsangreb, anses normalt ikke for cyberterror, medmindre de har et større omfang og rammer mål, så det skaber tilsvarende frygt, som et fysisk terrorangreb. Simple cyberangreb i kombination med fysiske terrorangreb vil kunne forøge virkningen af disse ved f.eks. at sætte centrale myndigheder ude af stand til at handle eller kommunikere.

Danske myndigheder, virksomheder og organisationer kan blive mål for cyberterror, hvis de eller Danmark pådrager sig gruppernes opmærksomhed.

Aktører uden statslig tilknytning, herunder ISIL, har udtrykt interesse for at gennemføre cyberangreb mod eksempelvis samfundsvigtige funktioner. Det er dog usandsynligt, at terrorister på kort til mellemlangt sigt vil være i stand til at udføre sådanne skadelige cyberangreb, da de ikke besidder de nødvendige kapaciteter. Det er sandsynligt, at enkelte militante islamister er i stand til at udføre simple operationer som eksempelvis overbelastningsangreb. Terrorister vil i højere grad bruge internettet til propaganda, eksempelvis ved at fremsætte trusler.

Truslen fra Cyberterror

I yderste konsekvens kan cyberterror medføre tab af liv og ødelæggelse af ejendom eller omfattende finansielle tab, som kan få samfundsmæssige konsekvenser for Danmark.

Trusselsvurderingsenheden vurderer, at særligt militante, islamistiske grupper som ISIL over tid vil tilegne sig cyberkapaciteter med henblik på at kunne gennemføre skadevoldende angreb, men at de aktuelt kun har ringe kapacitet til at gennemføre deciderede terrorangreb gennem internettet.

Truslen fra cyberterror mod myndigheder og private virksomheder er **LAV**.

Anbefalinger

Center for Cybersikkerhed anbefaler både myndigheder og private virksomheder at anvende publikationerne:

- Cyberforsvar der virker
- Spear-phishing - et voksende problem
- Begræns risikoen fra Ransomware samt
- Vejledning i imødegåelse af DDoS-angreb

med henblik på at imødegå cybertruslerne.

Derudover bør myndigheder og private virksomheder kende egen infrastruktur og gennemføre løbende risikoanalyse ud fra dens sårbarheder og derved identificere de mulige konsekvenser af de forskellige typer angreb. På baggrund af det skal der implementere beredskabsplaner, der kan håndtere mulige angreb.

Center for Cybersikkerhed anbefaler både myndigheder og private virksomheder at implementere risikostyring efter ISO27000 standarderne og kan henvise til Digitaliseringsstyrelsens Videnscenter for implementering af ISO27001.

Endelig er det vigtigt at ansætte eller have adgang til personer med de rette kompetencer til at håndtere cybersikkerhed, inden et angreb sker.

Definitioner

For at lette læsning af trusselvurderingen følger her en kort beskrivelse af de særlige formuleringer, som Forsvarets Efterretningstjeneste anvender i efterretningsanalyser.

Det er kun sjældent, at en efterretningstjeneste kan give en vurdering, uden at der er elementer af usikkerhed i den. Derfor forsøger man at gøre det klart for læserne, hvor sikker man er i sin vurdering. Det sker ved, at analytikerne udtrykker sig på en standardiseret måde og bruger de samme vendinger, når de vil give udtryk for den samme grad af sandsynlighed, især ved centrale vurderinger.

FE bruger fem sandsynlighedsgrader og følgende faste formuleringer, som her er anbragt på en skala:

Skalaen måler ikke præcise forskelle. Den fortæller blot, om noget er mere eller mindre sandsynligt end noget andet. Eller sagt på en anden måde: Denne skala viser, om analytikerne vurderer, at deres sikkerhed ligger tættere på f.eks. 25 % end 50 %. På denne måde forsøger de at opnå en bedre overensstemmelse mellem deres formuleringer og læsernes opfattelser.

Selv om formuleringernes sproglige form altid kan diskuteres, er de med til at give læseren en mere præcis information. Definitionerne af de særlige formuleringer, der er anvendt i denne trusselsvurdering, er anført nedenfor.

Sandsynlighedsgrader

”Det er usandsynligt, at ...”:	FE forventer ikke en given udvikling. Det er (næsten) ikke en mulighed.
”Det er mindre sandsynligt, at ...”:	Det er mere sandsynligt, at det ikke sker end det modsatte.
”Det er muligt, at ...”:	Det er en sandsynlig mulighed, men FE har ikke grundlag for at vurdere, om det er mere eller mindre sandsynligt.
”Det er sandsynligt, at ...”:	Det er mere sandsynligt, at det sker end det modsatte.
”Det er meget sandsynligt, at ...”:	FE forventer en given udvikling. Det er (næsten) bekræftet.

Trusselsniveauer

I forbindelse med udsendelse af Trusselsvurderingsenhedens trusselsvurderinger bruges fem betegnelser for trusselsniveauer, dækkende fra **INGEN** til **MEGET HØJ**.

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 ikke sandsynlig.
Middel	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mindre sandsynlig.
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.