Trusselskatalog for Statens IT

Version 16

Nedenstående tabel repræsenterer aktuelle trusler mod Statens It som virksomhed og som serviceleverandør i Staten. Kataloget skal betragtes som et relativt statisk dokument, hvis formål er at fungere som dialogredskab i forbindelse med workshops og interviews ift. udarbejdelse af risikovurderinger. Det skal ikke ses som et redskab til at få et her-og-nu overblik over de væsentligste trusler i Danmark og i Statens It.

Trusselkataloget revideres årligt.

Metadata:

Dato for godkendelse	31-10-2022
Næste planlagte revision	31-10-2023
Dokument ejer	Områdechefen for Informationssikkerhed (CIF)
Dokument ansvarlig	Morten Mertz
Arkivering	Statens It's dokumenthåndteringssystem
Publicering af dokument	Statens It's intranet
Klassifikation	Ingen mærkning

Tabel for trusselsniveauer

Sandsynlighed for at en trussel bliver aktuel	Beskrivelse
Høj	Der er en specifik trussel. En trussel er specifik, når der er kapacitet, foreligger en hensigt og at der foregår planlægning til at gennemføre truslen. Angreb/skadevoldende aktivitet eller hændelse er meget sandsynlig.
Middel	Der er en erkendt trussel. En trussel er erkendt, når det er indset, at der er kapacitet og/eller at der foreligger en hensigt til at gennemføre truslen. Angreb/skadevoldende aktivitet eller hændelse er sandsynlig.
Lav	En trussel er potentiel, når der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet eller hændelse er ikke sandsynlig.

Trusler kategoriseres i henhold til Statens It's vurdering med inspiration fra eksterne kilder som fx de nationale trusselsvurderinger.

Aktuelle udvalgte trusselsniveauer vurderet af CFCS

Cybertruslen mod Danmark (28-06-2022)
CFCS vurderer fortsat at truslen fra cyberspionage og cyberkriminalitet er MEGET HØJ. Truslen fra cyberaktivisme blev hævet d. 18. maj 2022 fra LAV til MIDDEL

CFCS hæver trusselsniveauet for cyberaktivisme på baggrund af aktivistiske cyberangreb udført i forbindelse med krigen i Ukraine. (18-05-2022)
CFCS har hævet trusselsniveauet for cyberaktivisme mod Danmark fra LAV til MIDDEL

Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine (15-03-2022)
Cybertruslen fra cyberkriminalitet og Cyberspironage mod Danmark er fortsat MEGET HØJ.

Fjern adgangen (20-12-2021)
Truslen fra cyberkriminalitet er MEGET HØJ - Hackere specialiseret i at kompromittere og videresælge fjernadgange

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.

Tabel for trusselskategorier

Trusler kategoriseret efter sandsynlighed for at trussel bliver aktuel

Nr.	Sandsynlighed	Trussel	Beskrivelse/eksempler
1	**Høj**	Software- og/eller netværksangreb	- Ransomware - Advanced Persistent Treat (APT). - Distributed denial-of-service (DDoS). - Angreb på hjemmesider, netværk og automatiserede løsninger (scipts, "robotter" mv.) - Øvrigt malware som fx trojanere, vira, orme, mobil kode, rootkits, spyware samt Buffer overflows mv. - Cyberspionage fx udført af fremmede stater og cyberkriminalitet. I begge tilfælde bliver angrebsmetoderne fortsat mere avancerede, og deres kompetencer/evner udvikles løbende. Nedbrudt på brancher vurderer CFCS specifik trusselniveauet som højt inden for energi, sundhed og finans. Udover at forsage nedbrud kan formålet også være tyveri og spionage udført at fremmede stater. Virtuelle mødeplatforme er bl.a. udsatte angrebsflader. - Malware bliver i stigende omfang rettet mod mobile enheder - Manglende fokus på håndtering af sårbarheder/patchning af sårbarheder - Trussels aktør fx En aktør der er motiveret for at udføre en given handling for at opnå et mål, er typisk sat sammen med APT (Advanced Persistent Threat) grupper og fremmede stater - Kompromittering af fjernadgange via fx phishing/malware (information-stealers). -

Nr.	Sandsynlighed	Trussel	Beskrivelse/eksempler
2	**Høj**	Ubevidste og bevidste brugere (interne og eksterne), medarbejderes fejl, forsømmelighed eller bevidste ulovlige eller afvigende handlinger.	- Uheld, medarbejderfejl, social engineering, phishing fx uforsætlig afgivelse af adgangskoder og bruger-id mv. Bevidst eller ubevidst manglende efterlevelse af processer og instruktioner herunder manglende efterlevelse af Statens It's Sikkerhedspjece. - Cyberkriminelle udnytter ubevidste insidere i forbindelse med cyberangreb (se angrebsvektorer under "Software- og/ eller" netværksangreb. - Privat hardware og software - Almindelige personoplysninger behandles/tilgås uautoriseret grundet medarbejderfejl/procesafvigende handlinger - Privilegerede brugere tvinges til udlevering af fortrolig information – herunder adgang til it-miljø/netværk - Betroede samarbejdsparter videregiver organisationens sårbarhed
3	**Høj**	Tredjepart leverandørers manglende leverancer eller manglende fokus på informationssikkerhed	- Afvigelser i kvaliteten (IT drift fra 3. parts leverandør). - Dårlig økonomi, konkurs eller overtagelse af ny ejer. - Malware inficere SIT via hacker udnytter adgang til leverandørs løsninger som springbræt til at ramme SIT. (Manglende sikkerhed hos leverandør) - Databaser/data placeret/behandlet i usikre (tredje)lande, også i forhold til databeskyttelsesretlige risici - Utilstrækkeligt kompetenceniveau - Strømforsyning og WAN forbindelser. - Samarbejdskontrakter som ikke i tilstrækkeligt omfang afdækker, hvordan konflikter og kontraktophør skal håndteres. - Utilstrækkelige databeskyttelsesretlige krav i databehandleraftale med leverandør

Nr.	Sandsynlighed	Trussel	Beskrivelse/eksempler
4	**Høj**	Teknisk svigt eller fejl på software	- Generelle funktionsfejl. - Implementering af AI medfører ikke- forudsete konsekvenser - Fejl i forbindelse med *manglende* opdateringer. - Fejl i forbindelse med implementering af opdateringer. - Fejl i forbindelse med ændringer. - Biometriske løsninger på eksempelvis adgangskontrol, der giver en falsk oplevelse af sikkerhed
5	**Høj**	Teknologisk forældelse og/eller fejl på hardware	- Utidssvarende hardware, software og/eller systemer, overdraget til Statens It fra kunder og 3. part. - Fejl og slitage på udstyr, herunder manglende vedligeholdelse og oprydning. - Utilstrækkelige sikkerhedsforanstaltninger (fx manglende logning eller adgangsbegrænsning) i ældre systemer og tjenester iht. behandlingssikkerhed jf. GDPR
6	**Høj**	Kombinerede cyber- og fysiske angreb	- Samtidige angreb på flere fronter udfordrer samarbejdet/koordination til iværksættelse af modforanstaltninger
7	**Høj**	Ekstern spionage	- Aflytning af udstyr – via mikrofoner eller kameraer
8	**Middel**	Fejl i kode og uafklaret licensforhold i relation til Open Source anvendelse	- Ingen notifikation ved identifikation af sårbarheder i kode - Aktiv Community bag kode er begrænset eller ikke eksisterende eller få brugere (kan man forvente at nogle andre finder og løser sårbarheder) - Brugernes erfaring med kode begrænset (Høj risiko for fejl) - Manglende mulighed for at tilknytte eksterne konsulenter med viden om anvendelse - Licensforhold ikke afdækket - Mangelfuld materialeopgørelse til softwaren (tredjepartskomponenter, licenstype, version, versionens stabilitet og sikkerhed, downloades fra, hvilke biblioteker komponenten selv afhænger af, etc..)

Nr.	Sandsynlighed	Trussel	Beskrivelse/eksempler
9	**Middel**	Fejl i, forældelse af eller ineffektive arbejdsgange/procesdokumentation	- Utidssvarende arbejdsgange - Arbejdsgange som på uhensigtsmæssig måde understøtter forretningsprocessens formål - Manglende beskrivelse af arbejdsgange - Manglende håndtering af identificerede problemstillinger - Manglende eller ikke retvisende KPI'er - Ingen eller mangelfuld systemunder-støttelse - Ny lovgivning / GDPR-krav om indsigt, berigtigelse og sletning.
10	**Middel**	Dårlig økonomi og manglende ressourcer	- Utilstrækkelige økonomiske ressourcer kan føre til manglende menneskelige ressourcer og kompetencer. - Faglige stridigheder der fører til arbejdsnedlæggelser, lockout og medarbejderafgang
11	**Middel**	Øget belastning	- Behov for leverancer er større end kapacitet
12	**Middel**	Naturkræfter	- Fx Skybrud, brand, orkan og lynnedslag. - Øvrige hændelser, der umuliggør adgang til datacenter - f.eks. gasudslip, røgudvikling fra nærliggende brand.
13	**Middel**	Kompromittering af intellektuelle rettigheder	- Piratkopiering, copyright-krænkelse/licenskrænkelse. - Udførelse af ulovlige handlinger med Statens IP-adresse scope som unik identifikation. - Uægte hardware.
14	**Middel**	Intern spionage og tyveri	- Uautoriseret adgang til data og personoplysninger - Ulovlig tilegnelse af data eller udstyr - Se også punktet: Software- og/eller netværksangreb
15	**Middel**	Tyveri af fysiske ting	- Ulovlig tilegnelse af udstyr
16	**Middel**	Implementering af ny teknologi	- Implementering/anvendelse af kunstig intelligens medfører utilsigtede konsekvenser - Manglende stillingstagen og implementering af Privacy-by-design/default i ny teknologi iht. GDPR

Nr.	Sandsynlighed	Trussel	Beskrivelse/eksempler
17	**Middel**	Terror/sabotage/hærværk ud over cybertrusler (pkt. 1)	- Destruktion af informationsaktiver. - Hærværk mod bygninger der beskytter mennesker og/eller data.

Dokumenthistorik

Forfatter	Versions-dato	Hvad er ændret	Godkender	Dato
LT (itst)	1	Udarbejdet	Lone Strøm	2010
MS	1.1	Opdateret	Lone Strøm	2012
BFS	1.2	Opdateret og forenklet	Michael Ørnø	2014
JJA	1.3	Opdateret	Michael Ørnø	2015
JJA	1.4	Opdateret med ransomware	Vibe Vallentin	2015
JJA	1.5	Ransomware fremhævet med egen placering.	Vibe Vallentin	2016
MME	13-03-2018	Opdatering med trusler fra CFCS feb 2018 og tilføjelser af forretningstrusler for at understøtte ISO 20000s fokus på processer	Vibe Vallentin	13-03-2018
MME	03-04-2018	Revisionsdatoen er ændret til 15/9-2018 efter beslutning på Områdemøde den 3/4-2018	Vibe Vallentin	03-04-2018
MME	17-09-2018	Gennemlæst og opdateret med de seneste trusselvurderinger fra CFCS	Vibeke på vegne af Vibe	17-09-2018
MME	18-03-2019	Gennemlæst og vurderet mod CFCS seneste trusselsvurderinger. Trussel fra medarbejdere er præciseret	Henrik Ravn	10-03-2019
VVJ	10-10-2019	Opdateret med trusler fra CFCS og rækkefølge på trusler ændret		
MDA	31-10-2019	Opdateret med GDPR	Henrik Ravn	31-10-2019
MME	02-07-2020	Opdateret med seneste fra CFCS og Open Source trusler	Henrik Ravn	03-07-2020
Rasmus Munch	11-11-2020	Trussel 16 er fjernet (afpresning). Trussel 14 er ændret så den kun indeholder Tyveri af fysiske ting og ikke også læk af interne informationer, som er flyttet til trussel 2	Henrik Ravn	01-12-2020
ADJ	01-12-2020	Dokumentets interne metadata opdateret, fra 01-07-2020 til 01-07-2021, som det var tiltænkt i foregående version.	Henrik Ravn	01-12-2020
ADJ	13-01-2021	Dokumentejer og dokumentansvarlig ændret iht. organisationsændring og ny fordeling. Indhold ellers uændret.	Vibeke Bertelsen	13-01-2021

Rasmus Munch	07-06-21	Gennemlæst og opdateret med de seneste trusselvurderinger fra CFCS	Henrik Ravn	07-06-21
Rasmus Munch	08-06-21	Gennemlæst og opdateret med de seneste trusselvurderinger (2021) fra CFCS	Henrik Ravn	08-06-21
ADJ	13-07-2021	Opdatering af dokumentejer i dokumentets metadata iht. den aktuelle organisation. Dokumentet er ellers uændret ift. foregående version, derfor ingen ændring af godkendelsesdato eller dato for næste planlagte revision.		
ADJ	24-08-2021	Opdatering af dokumentansvarlig i dokumentets metadata iht. den aktuelle opgavefordeling i Informationssikkerhed og procesudvikling. Dokumentet er ellers uændret ift. foregående version, derfor ingen ændring af godkendelsesdato eller dato for næste planlagte revision.		
MDJ	18-01-2022	Gennemlæst og opdateret med kort tekst vedrørende cyberspionage og fjernadgange jf. CFCS' "Vejledning om Råd om sikkerhed på virtuelle mødeplatforme" og "Trusselsvurdering: Fjern adgangen". Ændring af versionsnummer samt dato for næste revision.		
ADJ	19-01-2022	Referencer på forside fjernet. Dokumentet godkendt.	Anders D. Johansen	19-01-2022
MME	12-07-2022	Dokument gennemlæst og opdateret med aktuelle trusselsvurderinger fra CFCS	Nicolai Zachariasen	01-08-2022
MDJ	20-10-2022	Dokument gennemlæst og opdateret med ny trussel: Ekstern spionage. Formålsbeskrivelse præciseret. Frekvens for opdatering ændret fra halvårlig til årligt.	Nicolai Zachariasen	31-10-2022