CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Cybertruslen mod Grønland

April 2024

Indhold

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

April 2024

Cybertruslen mod Grønland

Trusselsvurderingen har til formål at informere beslutningstagere om cybertruslen mod myndigheder og virksomheder i Grønland. Vurderingen kan også tjene som input til grønlandske myndigheders og virksomheders risikovurderinger på cybersikkerhedsområdet.

Trusselsvurderingen erstatter "Cybertruslen mod Grønland", der udkom i marts 2023.

Hovedvurdering

- Truslen fra cyberspionage mod Grønland er **MEGET HØJ**. Særligt Grønlands centrale placering i Arktis bidrager til truslen, da både Rusland og Kina har store interesser i regionen. Stater kan potentielt misbruge den viden, de får via cyberspionage, på bekostning af Grønlands interesser.

- Truslen fra cyberkriminalitet mod Grønland er **MEGET HØJ**. Især ransomware-angreb kan have omfattende konsekvenser for den enkelte organisation, der bliver ramt, men også for hele Grønland, såfremt samfundsvigtige funktioner påvirkes.

- Truslen fra destruktive cyberangreb mod Grønland er **LAV**. Bliver Grønland alligevel ramt af et destruktivt cyberangreb, kan angrebet få meget alvorlige konsekvenser, hvis det påvirker samfundsvigtige funktioner.

- Truslen fra cyberaktivisme mod Grønland er **LAV**. Truslen kan dog stige med kort eller intet varsel, hvis aktivistiske hackere får intention om at rette deres angreb mod mål i Grønland.

- Truslen fra cyberterror mod Grønland er **INGEN**.

Indledning

Grønland står fortsat over for en betydelig cybertrussel. Truslen understreges af, at Grønland også blev ramt af cyberangreb i 2023.

Samfund i Arktis, herunder det grønlandske, kan pga. deres beliggenhed og geografi være særligt afhængige af velfungerende forsyningslinjer for bl.a. fødevarer, el og varme. Derfor kan cyberangreb mod Grønland få særligt alvorlige konsekvenser, hvis de påvirker samfundsvigtige funktioner.

Cybertruslen mod Grønland kommer især fra fremmede stater og kriminelle hackere, der begge udgør en vedvarende trussel. Det skyldes, at både statslige og kriminelle hackere har væsentlige ressourcer, som de løbende bruger til at udføre cyberangreb mod mål verden over. Derfor tager trusselsvurderingen ikke kun afsæt i tidligere cyberangreb mod Grønland, men også den generelle udvikling i cybertruslen mod Danmark og andre lande i Grønlands og Danmarks nærområde.

Samtidig tager trusselsvurderingen også højde for udenrigs- og sikkerhedspolitiske forhold, der kan påvirke fremmede staters interesse i Grønland og Arktis og dermed også cybertruslen. Det gælder eksempelvis de sikkerhedspolitiske spændinger mellem Rusland og Vesten samt Kina's langsigtede interesser i at sikre adgang til og indflydelse i Arktis.

Selvom cyberangreb, der har til formål at udføre spionage eller begå kriminalitet, aktuelt udgør de største trusler mod Grønland, er de ikke de eneste cybertrusler. Trusselsvurderingen beskriver derfor også truslerne fra cyberaktivisme, destruktive cyberangreb og cyberterror.

Cyberangreb lammede KNR's TV- og radiosignal
Kalaallit Nunaata Radioa (KNR), eller Grønlands Radio, blev den 8. december 2023 ramt af et cyberangreb. Angrebet havde omfattende konsekvenser, da KNR måtte lukke deres netværk indtil den 10. december for at afværge angrebet. Nedlukningen betød blandt andet, at KNR's TV- og radiosignal ikke kunne udsendes eller livestreames på KNR's hjemmeside, samt at radioavisen måtte aflyses mellem den 13. til den 15. december. KNR's TV- og radioudsendelser kunne dog fortsat tilgås on demand via hjemmesiden.

Cyberspionage

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

Det er meget sandsynligt, at myndigheder og virksomheder i Grønland vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Fremmede stater forsøger løbende at udføre cyberspionage mod mål verden over, herunder myndigheder og virksomheder i Grønland. Cyberspionagen har generelt til formål at få adgang til sensitiv og værdifuld viden og kan både være politisk og økonomisk motiveret.

Stater som Rusland og Kina har bl.a. en særlig interesse for viden om udenrigs-, sikkerheds- og forsvarspolitik og kan f.eks. være interesserede i at få adgang til viden om Grønlands relationer til rigsfællesskabet og andre stater. Truslen fra cyberspionage retter sig derfor særligt mod organisationer med viden af den karakter.

Cyberspionage kan dog også ramme andre dele af det grønlandske samfund. Det skyldes, at fremmede stater også er interesserede i at få adgang til andre typer viden. For eksempel kan fremmede stater være interesserede i at få viden om råstoffer, naturressourcer, kommercielle forhold, samfundsvigtige sektorer og intellektuel ejendom i Grønland.

Arktis står højt på Rusland og Kinas prioriteringslister
Særligt Grønlands centrale placering i Arktis bidrager til truslen fra cyberspionage mod Grønland. Det skyldes, at både Rusland og Kina har stor interesse i regionen.

Rusland ser sig selv som den førende stat i Arktis med en historisk ret til at spille en hovedrolle i regionen. Ruslands politik i Arktisk har overordnet set to højt prioriterede mål. Ruslands første mål er at beskytte sig mod en, efter russisk opfattelse, stigende trussel nordfra fra USA og NATO. Det andet mål er at udnytte naturressourcerne og det øvrige økonomiske potentiale i Arktis. Ruslands bestræbelser på at nå disse mål udgør de væsentligste drivkræfter for den sikkerhedspolitiske udvikling i regionen.

For Kina har Arktis også et stort strategisk potentiale. Kommercielt ønsker Kina at sikre fremtidig adgang til søtransportruter, der kan afhjælpe Kinas afhængighed af Suezkanalen og Malaccastrædet og forkorte vejen for varetransport mellem Kina og Europa. På længere sigt ønsker Kina også at kunne operere militært i Arktis. Kinas aktiviteter i Arktis er dog endnu ret begrænsede, og landet er generelt afhængige af samarbejde med kyststaterne, herunder særligt Rusland, når det kommer til adgang til regionen. Efter invasionen af Ukraine er Rusland i stigende grad blevet afhængig af samarbejde med Kina, hvilket betyder større russisk velvilje i forhold til at give Kina adgang til den russiske del af Arktis.

Fremmede stater, herunder Rusland og Kina, kan potentielt misbruge viden indsamlet via cyberspionage til at fremme deres handlemuligheder og interesser i Arktis på bekostning af grønlandske interesser.

Grønland er udsat for en delt trussel med Danmark
De tætte relationer mellem Grønland og Danmark betyder, at grønlandske organisationer er udsat for en delt trussel med de danske myndigheder og virksomheder, som har tilknytning til eller betydning for Grønland. Det gælder bl.a. grønlandske myndigheder og virksomheder med forbindelser til danske myndigheder, der indgår i udenrigs- og sikkerhedspolitiske sammenhænge, herunder EU og NATO.

Derudover har der de seneste år været en meget høj trussel fra cyberspionage rettet mod både transportsektoren og forskningssektoren i Danmark. Særligt luft- og søfartssektoren har også stor betydning i Grønland, og danske og grønlandske forskningsinstitutioner har ligeledes et tæt samarbejde. CFCS vurderer, at truslen mod sektorerne i Danmark også gælder for transportsektoren og forskningssektoren i Grønland.

Opportunistisk cyberspionage truer alle dele af samfundet
Cyberspionage rammer også mere vilkårlige ofre på tværs af sektorer og lande. Det skyldes, at stater også udfører opportunistiske cyberangreb. For eksempel forsøger nogle statslige hackere at kompromittere mange organisationer på kort tid ved at udnytte specifikke sårbarheder eller gennem supply-chain angreb mod eksempelvis it-leverandører. Derefter kan hackerne tage stilling til, hvilke adgange, data eller konti der er interessante at arbejde videre med.

Cyberspionage kan også føre til andre trusler
Fremmede stater kan potentielt også bruge den viden, de får gennem cyberspionage, til at understøtte andre former for angreb og aktiviteter mod Grønland.

Fremmede stater kan f.eks. misbruge den viden, der indsamles via cyberspionage, til at understøtte påvirkningskampagner. Det kan de bl.a. gøre ved at stjæle sensitive oplysninger og derefter lække dem med et specifikt budskab. Det kan eksempelvis ske i forbindelse med en eventuel fremtidig interessekonflikt i Arktis, hvor Grønland vil kunne få en fremtrædende rolle i en konflikt med Rusland eller Kina.

Derudover kan fremmede stater f.eks. også bruge cyberspionage til at forberede destruktive cyberangreb. Statslige hackere kan bl.a. bruge cyberspionage til at opbygge viden om og etablere adgange til organisationers systemer og netværk. På den måde bliver det muligt for staterne at udføre destruktive cyberangreb med kort eller uden varsel, såfremt de skulle få intention herom. Dette kan f.eks. ske, hvis den aktuelle sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ**.

Det er meget sandsynligt, at myndigheder og virksomheder i Grønland vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

CFCS bruger begrebet cyberkriminalitet som en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse. Cyberangreb kan anvendes til mange typer kriminalitet, men bruges oftest i forbindelse med forskellige former for tyveri, bedrageri og afpresning.

Cyberkriminalitet rammer bredt på tværs af landegrænser og udgør derfor også en vedvarende trussel mod myndigheder, virksomheder og borgere i Grønland. Det skyldes, at kriminelle hackere ofte går opportunistisk til værks og forsøger at ramme så mange ofre som muligt. Det kan de f.eks. gøre ved at udsende phishing-mails til et meget stort antal modtagere i håb om, at et uopmærksomt offer klikker på et link eller åbner en fil.

Der findes dog også kriminelle hackere, som udfører mere målrettede angreb. Disse hackere har generelt mere veludviklede angrebsteknikker og -metoder og retter i højere grad deres angreb mod organisationer, som forventes at kunne bedrages eller afpresses for store beløb. Cyberangreb fra disse hackere har derfor ofte alvorlige konsekvenser, og tabet for det enkelte offer kan løbe op i millioner af kroner.

Phishing er et forsøg på at narre mail modtagere til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til bl.a. it-systemer. Ofte vil angriberen ved hjælp af simpel social engineering forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer. Phishing-mails sendes ofte bredt ud til mange tilfældige modtagere uden at være tilpasset den enkelte modtager.

Spear phishing adskiller sig fra almindelig phishing ved, at ofrene ikke er tilfældige, men udvalgte. Ved spear phishing anvendes ofte avanceret social engineering for at målrette indholdet det enkelte offer. Kommunikationen er typisk udformet, så den virker særligt relevant, overbevisende og troværdig for modtageren ved f.eks. at anvende modtagerens navn eller andre oplysninger, som er fundet ved forudgående rekognoscering.

Ransomware-angreb er den alvorligste trussel fra kriminelle

Ransomware-angreb udgør aktuelt den mest alvorlige trussel fra cyberkriminalitet mod Grønland. Ved denne type angreb forsøger kriminelle at afpresse myndigheder og virksomheder ved at gøre deres data og systemer utilgængelige, ofte ved at kryptere data. De kriminelle hackere kræver derefter en løsesum, typisk i form af kryptovaluta, for at gøre data og systemer tilgængelige igen. Ofte truer de også med at offentliggøre informationer, der kan være stjålet i angrebet, hvis ikke ofrene betaler.

Ransomware-angreb kan have omfattende konsekvenser. Det gælder både for de myndigheder og virksomheder, som ransomware-angrebet er rettet mod, men også for samfundet som helhed, hvis samfundsvigtige funktioner påvirkes.

I december 2023 blev tre tyske hospitaler for eksempel udsat for et ransomware-angreb. Angrebet påvirkede flere af hospitalets systemer, herunder akutmodtagelsen. Ifølge Katholische Hospitalvereinigung Ostwestfalen, der administrerer hospitalerne, var det muligvis den kriminelle hackergruppe kendt som Lockbit, der stod bag angrebet. Samme hackergruppe har selv hævdet at stå bag et ransomware-angreb mod amerikanske hospitaler i november 2023. Angrebet mod de tyske hospitaler viser, hvordan ransomware-angreb kan true samfundsvigtige funktioner.

Mens afpresning og tyveri er meget udbredte måder at berige sig på, er der fortsat også kriminelle hackere, der specialiserer sig i at bruge cyberangreb i forbindelse med bedrageri. Blandt andet i form af såkaldte Business Email Compromise (BEC), hvor kriminelle udgiver sig for at være en ledende medarbejder og beder om overførsler af penge til hackernes egne konti.

Robusthed kan både modvirke ransomware og cyberspionage
Angrebsmetoderne, der bliver brugt i de indledende faser af ransomware- og cyberspionage-angreb, har ofte mange ligheder. I begge typer angreb forsøger hackere typisk at få adgang til forretningskritiske it-systemer som f.eks. mailservere gennem brug af bl.a. phishing og kendte sårbarheder.

Grønlandske myndigheder og virksomheder, der styrker deres robusthed for at forebygge forsøg på ransomware-angreb, kan derfor også forvente at få en styrket robusthed mod cyberspionage og omvendt.

Selvom formålet med og aktørerne bag de to trusler er forskellige, kan myndigheder og virksomheder således benytte nogle af de samme tiltag til at beskytte sig mod truslerne.

Destruktive cyberangreb

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

Flere fremmede stater har kapacitet til at udføre destruktive cyberangreb, men det er mindre sandsynligt, at disse aktuelt har intention om at udføre destruktive cyberangreb mod virksomheder og myndigheder i Grønland inden for de næste to år.

Hvad er destruktive cyberangreb?
Destruktive cyberangreb er cyberangreb, hvor den forventede effekt er:

- Ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.
- Betydelig skade på fysiske objekter.
- Død eller personskade.

Truslen fra destruktive cyberangreb mod Grønland kan dog stige med kort eller uden varsel, hvis staternes intentioner ændrer sig. Det kunne f.eks. ske, hvis krigen mellem Rusland og Ukraine medfører, at den sikkerhedspolitiske situation eskaleres i retning af en militær konfrontation mellem Rusland og NATO. Det gælder især, hvis konflikten får fokus på Grønland eller Arktis.

Fremmede stater udvikler løbende deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel. Staterne anvender dog hovedsageligt kapaciteterne i forbindelse med konflikter, hvilket krigen i Ukraine er et eksempel på.

Mindre sandsynligt, men alvorlige konsekvenser
Selvom truslen fra destruktive cyberangreb aktuelt er **LAV**, er det en reel mulighed, at Grønland bliver ramt af et destruktivt cyberangreb.

Et sådant angreb kan potentielt få meget alvorlige konsekvenser, hvis eksempelvis adgangen til samfundsvigtige funktioner og ydelser såsom strøm, transport eller internet bliver afbrudt eller forstyrres.

Det er samtidig muligt, at destruktive cyberangreb rettet mod andre lande kan påvirke Grønland. Det kan eksempelvis ske, hvis udenlandske leverandører til samfundsvigtige funktioner i Grønland bliver ramt af destruktive cyberangreb.

I februar 2022 blev Viasat, en amerikansk udbyder af satellitkommunikation, eksempelvis udsat for et destruktivt cyberangreb. Selvom målet for angrebet sandsynligvis var ukrainsk militær kommunikation, fik det følgevirkninger langt ud over dette og påvirkede organisationer i en række lande.

Cyberaktivisme

Truslen fra cyberaktivisme mod Grønland er **LAV.**

Mange aktivistiske hackere har kapacitet til at udføre cyberangreb mod myndigheder og virksomheder i Grønland, men CFCS vurderer, at hackernes intention om angreb mod Grønland aktuelt er begrænset. Det er derfor mindre sandsynligt, at organisationer i Grønland vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

Truslen fra cyberaktivisme kan dog stige med kort eller intet varsel, hvis aktivistiske hackere får intention om at udføre cyberangreb mod organisationer Grønland. Det gælder særligt truslen fra DDoS-angreb, der generelt kan udføres af cyberaktivister uden væsentlig forberedelse.

Samtidig kan Grønland også blive påvirket af følgevirkninger fra cyberaktivistiske angreb rettet mod danske organisationer med betydning for Grønland.

DDoS-angreb
DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Ved DDoS-angreb udnytter hackere kompromitterede computere og enheder 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.

Cyberaktivister anvender oftest DDoS-angreb
DDoS-angreb er den hyppigste form for angreb udført af cyberaktivister og rettes mod internetvendte hjemmesider og systemer. Angrebene kan virke forstyrrende, men har generelt ikke varige eller destruktive konsekvenser.

Særligt pro-russiske cyberaktivister udfører løbende DDoS-angreb mod mål i Danmark og andre NATO-lande som følge af spændingerne mellem Rusland og Vesten. Foreløbigt er der dog ikke tegn på, at de pro-russiske cyberaktivister anser Grønland for at være et mål på linje med Danmark og øvrige NATO-lande.

Cyberterror

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

Det er usandsynligt, at grønlandske myndigheder og virksomheder vil blive udsat for forsøg på cyberterror inden for de næste to år.

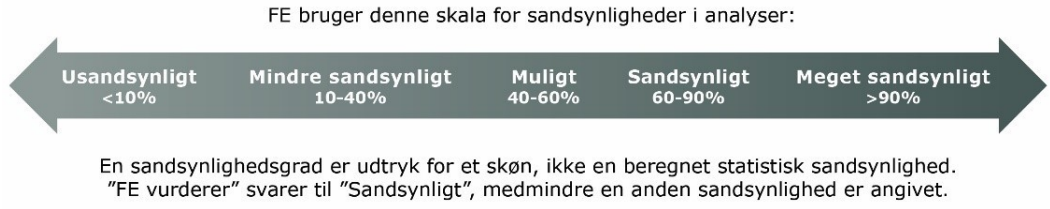
CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

CFCS vurderer, at militante ekstremister kun har begrænset hensigt til at udføre cyberangreb, der har samme effekt som konventionel terror, samt at de ikke har den fornødne kapacitet.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.



Andre relevante publikationer

Center for Cybersikkerhed udgiver løbende trusselsvurderinger og vejledninger på cyberområdet. Derudover udgiver Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste en række årlige publikationer, der beskriver truslerne mod Danmark. Nedenfor er fremhævet en række af de publikationer, som kan være relevante for myndigheder og virksomheder i Grønland. Alle publikationer kan tilgås på myndighedernes hjemmesider.

Publikationer fra efterretningstjenesterne:

UDSYN
Forsvarets Efterretningstjeneste beskriver i denne årlige efterretningsmæssige risikovurdering de ydre vilkår for Danmarks sikkerhed og danske interesser

Vurdering af spionagetruslen mod Danmark, Færøerne og Grønland
Denne trusselsvurdering udgives af Politiets Efterretningstjeneste og beskriver fremmede staters efterretningsvirksomhed mod Rigsfællesskabet, dvs. især spionage, påvirkning og forsøg på ulovligt at anskaffe teknologi og viden.

Vurdering af terrortruslen mod Danmark
I denne trusselsvurdering fastsætter Center for Terroranalyse (PET) det nationale terrortrusselsniveau og beskriver terrortruslen mod Danmark og danske interesser i udlandet.

Trusselsvurderinger fra Center for Cybersikkerhed:

Cybertruslen mod Danmark
I denne årlige trusselsvurdering beskriver Center for Cybersikkerhed den generelle cybertrussel for hhv. cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror mod Danmark.

Cybertruslen mod danske havne og logistikvirksomheder
Trusselsvurderingen beskriver cybertruslen mod danske erhvervshavne og logistikvirksomheder. Vurderingen tager afsæt i analyser af danske havne og internationale eksempler på cyberangreb mod havne og logistikvirksomheder.

Cybertruslen mod dansk luftfart
Trusselsvurderingen redegør for cybertruslen mod den danske luftfartssektor, herunder bl.a. lufttrafikstyrings- og luftfartsmyndigheder, lufthavne, flyselskaber, og underleverandører til flyproducenter.

Ransomware-truslen mod produktionsvirksomheder
Trusselsvurderingen beskriver truslen fra ransomware-angreb fra kriminelle hackere mod danske produktionsvirksomheder.

Cybertruslen mod IoT-enheder
Denne trusselsvurdering informerer om cybertruslen mod IoT-enheder, der ligesom almindelige it-systemer rammes af cyberangreb. I tillæg til trusselsvurderingen er der også udgivet en vejledning med anbefalinger til, hvordan organisationer kan deres IoT-enheder.

Vejledninger fra Center for Cybersikkerhed:

Cyberforsvar der virker
Denne vejledning er Center for Cybersikkerheds grundlæggende vejledning, som gennem seks trin guider myndigheder og virksomheder i at opbygge et cyberforsvar og håndtere cyberangreb. Implementeres vejledningen, vil det være muligt for myndigheder og virksomheder at forhindre en markant del af de cyberangreb, de udsættes for, og styrke deres håndtering af de angreb, der lykkes.

Reducér risikoen for Ransomware
Denne vejledning 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 ransomware-angreb kan håndteres, når skaden er sket.

Cybersikkerhed i leverandørforhold
Denne vejledning giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.

Beskyt din organisationen mod phishingangreb
Vejledningen forklarer begrebet phishing og indeholder beskrivelser af sikkerhedstiltag, der er målrettet henholdsvis modtagelsen af og udsendelse af e-mails. Vejledningen gennemgår også en række sikkerhedstiltag, der bidrager til at begrænse de konsekvenser, et vellykket phishing-angreb kan have for organisationen.