CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Cybertruslen mod Grønland

1. udgave marts 2023

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave marts 2023.

Trusselsvurdering: Cybertruslen mod Grønland

Trusselsvurderingen har til formål at informere grønlandske myndigheder og beslutningstagere om cybertruslen mod Grønland. Trusselsvurderingen kan bl.a. bruges i grønlandske virksomheder og myndigheders arbejde med risikovurderinger på cybersikkerhedsområdet.

Hovedvurdering

- Fremmede stater og kriminelle hackere udgør en vedvarende cybertrussel mod Grønland.

- Truslen fra cyberspionage mod Grønland er **MEGET HØJ**. Grønlands centrale placering i Arktis medvirker til den alvorlige trussel fra cyberspionage mod Grønland. Viden fra cyberspionage kan blive misbrugt af fremmede stater på bekostning af grønlandske interesser.

- Truslen fra cyberkriminalitet mod Grønland er **MEGET HØJ**. Særligt ransomware-angreb kan ikke kun gøre stor skade på ramte myndigheder og virksomheder, men kan også have alvorlige konsekvenser for samfundsvigtige funktioner i Grønland.

- Truslen fra destruktive cyberangreb mod Grønland er **LAV**. Det er mindre sandsynligt, at fremmede stater har til hensigt at bruge destruktive cyberangreb mod Grønland. Truslen kan dog stige med kort varsel, da flere stater har kapacitet til at udføre destruktive cyberangreb. Det er samtidigt muligt, at destruktive cyberangreb rettet mod andre lande kan påvirke leveringen af samfundsvigtige tjenester i Grønland.

- Truslen fra cyberaktivisme mod Grønland er **LAV**. Truslen fra cyberaktivisme mod Grønland kan stige uden eller med kort varsel, hvis enkeltsager med forbindelse til Grønland får aktivistiske hackeres opmærksomhed.

- Truslen fra cyberterror mod Grønland er **INGEN**. Militante ekstremister har begrænset hensigt til at udføre cyberangreb, der har samme effekt som konventionel terror. De har samtidigt ikke den fornødne kapacitet.

Indledning

Grønland står over for en alvorlig cybertrussel. Truslen kommer hovedsageligt fra fremmede stater og kriminelle hackere. Både fremmede stater og kriminelle hackere har meget væsentlige ressourcer til at udføre cyberangreb og udgør en vedvarende cybertrussel mod Grønland.

Cyberangreb har påvirket samfundsvigtige funktioner i Grønland i forbindelse med hændelser i 2022. Angrebene førte bl.a. til nedetid i borgervendte tjenester i centraladministrationen og i sundhedsvæsenet. Hændelserne afspejler cybertruslens alvor.

Samfund i Arktis, herunder Grønland, kan pga. deres beliggenhed og geografi være særligt afhængige af velfungerende forsyningslinjer for bl.a. fødevarer, el og varme. Cyberangreb mod disse funktioner – begået af statslige eller ikke-statslige aktører – kan derfor have særligt alvorlige konsekvenser.

Cybertruslen er et grænseoverskridende fænomen. Fremmede stater og kriminelle hackere udfører løbende cyberangreb mod lande verden over. Vurderingen af cybertruslen mod Grønland tager derfor ikke kun afsæt i hændelser i Grønland men også i udviklingen i cybertruslen mod Danmark og andre lande i Danmarks og Grønlands nærområde.

Vurderingen har også medtaget udenrigs- og sikkerhedspolitiske forhold, der kan påvirke truslen. Herunder fremmede staters interesse i Grønland og Arktis.

Udover cyberspionage og cyberkriminalitet vurderer CFCS også truslerne fra cyberaktivisme, destruktive cyberangreb og cyberterror.

Cyberangreb påvirkede borgervendte tjenester
Naalakkersuisuts digitaliseringsstyrelse opdagede et sikkerhedsbrud i centraladministrationen 25. marts 2022. Kommunikation ind og ud af landet til administrationens servere blev derfor blokeret. Det gik bl.a. ud over adgangen til hjemmesider ved brug af NemID og forsinkede udbetalingen af sociale ydelser og regninger. Formanden for Naalakkersuisut, Múte B. Egede, udtalte til grønlandske medier, at hændelsen skyldtes et cyberangreb, der havde spionage som formål.

Den 9. maj 2022 meddelte Naalakkersuisut, at sundhedsvæsnet var ramt af systemnedbrud, der bl.a. skabte problemer med hjemmesiden doktor.gl og med mails til sundhedsvæsenet. Naalakkersuisut meddelte den 18. maj 2022, at systemnedbruddet skyldtes et cyberangreb. Genstart af systemerne betød bl.a., at personalet ikke kunne tilgå patienternes journaler.

Cyberspionage

Truslen fra cyberspionage mod Grønland er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at grønlandske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Cyberspionage er politisk og økonomisk motiveret. Stater udfører løbende forsøg på cyberspionage for at få adgang til sensitiv og værdifuld viden, også i Grønland.

Fremmede stater, herunder Rusland og Kina, har en særlig interesse for viden af udenrigs-, sikkerheds- og forsvarspolitisk karakter. Fremmede stater kan eksempelvis være interesserede i viden om Grønlands relationer til rigsfællesskabet og andre stater.

Cyberspionage kan også blive brugt mod andre dele af samfundet i Grønland. Cyberspionage kan eksempelvis blive brugt til at få indblik i viden om råstoffer, naturressourcer, kommercielle forhold, samfundsvigtige sektorer og intellektuel ejendom i Grønland, som har fremmede staters interesse.

Grønlands centrale placering i Arktis medvirker til den alvorlige trussel fra cyberspionage mod Grønland. Både Rusland og Kina har stor interesse i Arktis. Rusland ser sig selv som den førende stat i Arktis med en historisk ret til at spille en hovedrolle i regionen. Kina arbejder samtidigt for større indflydelse på arktiske anliggender for at få adgang til ressourcer og søruter. Cyberspionage kan blive misbrugt af begge lande til at fremme deres handlemuligheder og interesser i Arktis, potentielt på bekostning af grønlandske interesser.

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

Der har i de seneste år været en øget trussel mod både transport og forskning i Danmark. Særligt luft- og søfart har også stor betydning for Grønland, og danske og grønlandske forskningsinstitutioner har et tæt samarbejde. CFCS vurderer, at truslen mod disse sektorer også er gældende i Grønland.

Cyberspionage rammer også mere vilkårlige ofre på tværs af sektorer og landegrænser. Det skyldes, at stater også udfører opportunistiske cyberangreb. Det kan bl.a. ske i forbindelse med offentliggørelsen af sårbarheder eller ved supply-chain angreb via eksempelvis it-leverandører, hvor fremmede stater kompromitterer mange organisationer inden for kort tid. Efter den første kompromittering kan staterne derefter tage stilling til, hvilke adgange, data eller konti der er interessante at arbejde videre med.

Cyberspionage kan føre til andre trusler
Cyberspionage mod Grønland kan føre til andre former for cyberangreb. Viden indsamlet og opbygget gennem cyberspionage kan eksempelvis blive anvendt i forbindelse med eventuelle fremtidige påvirkningskampagner. Det kunne f.eks. ske i en eventuel fremtidig interessekonflikt i Arktis, hvor Grønland vil kunne få en fremtrædende rolle i en konflikt med Rusland eller Kina.

Cyberspionage kan også give fremmede stater viden om eller adgang til it-systemer, der kan blive misbrugt i destruktive cyberangreb i Grønland.

Forsøg på påvirkning mod Rigsfællesskabet
Et eksempel på et påvirkningsforsøg mod Rigsfællesskabet er sagen om et falsk brev fra Grønlands daværende minister for udenrigsanliggender Ane Lone Bagger til den amerikanske senator Tom Cotton i november 2019. Brevet cirkulerede på internettet og omtalte bl.a. grønlandsk-amerikansk samarbejde, en fremtidig afstemning om grønlandsk selvstændighed og en specifik aftale om Grønlands status og amerikansk økonomisk støtte. Det er meget sandsynligt, at formålet var at skabe splid i Rigsfællesskabet og mistillid mellem Danmark og USA vedrørende USA's intentioner i Arktis.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at grønlandske myndigheder og virksomheder 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. Angrebene bliver misbrugt i forskellige typer kriminalitet, der generelt baserer sig på forskellige former for tyveri, bedrageri og afpresning.

Cyberkriminalitet rammer meget bredt på tværs af landegrænser og udgør en vedvarende trussel mod myndigheder, virksomheder og borgere i Grønland. Det skyldes, at nogle typer cyberkriminalitet går efter at ramme så mange ofre som muligt, eksempelvis gennem phishing spredt til tusinder af modtagere i mange lande.

Andre typer cyberkriminalitet går mere målrettet efter myndigheder og virksomheder, hvor tabet for det enkelte offer kan løbe op i millioner af kroner.

Ransomware-angreb er den alvorligste trussel fra kriminelle
Ransomware-angreb er aktuelt den mest alvorlige trussel fra cyberkriminalitet mod Grønland. Her forsøger kriminelle hackere at kompromittere og kryptere data på centrale it-systemer hos myndigheder og virksomheder. De forsøger derefter at afpresse ofrene en løsesum mod at dekryptere data igen. Ofrene bliver også ofte truet med offentliggørelse af stjålet data, hvis løsesummen ikke betales.

Ransomware-angreb kan ikke kun gøre stor skade på ramte myndigheder og virksomheder, men kan også have alvorlige konsekvenser for samfundsvigtige funktioner.

I maj 2021 blev det amerikanske olieselskab Colonial Pipeline eksempelvis udsat for et ransomware-angreb. Angrebet medførte, at Colonial Pipeline i seks dage måtte holde virksomhedens rørledninger lukket. Angrebet illustrerede, hvordan ransomware-angreb kan true kritiske forsyningskæder.

Mens afpresning og tyveri er meget udbredte metoder for kriminelle hackere at berige sig på, er der fortsat også hackere, der specialiserer sig i 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 modvirke cyberspionage og ransomware
Angrebsmetoderne, der bliver brugt i de indledende faser af et cyberspionage- og ransomware-angreb, har mange ligheder. I begge typer angreb forsøger hackere at få adgang til forretningskritiske it-systemer som f.eks. mailservere gennem brug af bl.a. phishing og kendte sårbarheder.

Det betyder, at grønlandske myndigheder og virksomheder, der styrker deres robusthed for at forebygge forsøg på cyberspionage, også får en styrket robusthed mod ransomware-angreb og omvendt.

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

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod Grønland er **LAV**. Det betyder, at det er mindre sandsynligt, at grønlandske myndigheder og virksomheder vil blive udsat for destruktive cyberangreb inden for de næste to år.

Det er mindre sandsynligt, at fremmede stater aktuelt har intentioner om at udføre destruktive cyberangreb mod Grønland.

Destruktive cyberangreb bliver hovedsageligt brugt af stater i forbindelse med konflikter. Flere stater, herunder Rusland, har kapacitet til at udføre den type angreb. Stater udvikler løbende deres kapaciteter til at kunne udføre destruktive cyberangreb med kort varsel.

Det betyder, at truslen mod Grønland kan stige med kort eller uden varsel, hvis den sikkerhedspolitiske situation, eksempelvis som følge af krigen mellem Rusland og Ukraine, eskalerer i retning af en militær konfrontation mellem Rusland og NATO. Truslen kan især stige, hvis konflikten har fokus på Grønland eller Arktis.

Selvom truslen aktuelt er **LAV**, er der tale om en væsentlig trussel mod Grønland, da destruktive cyberangreb kan have meget alvorlige konsekvenser. Konsekvenser af et angreb kan eksempelvis være, at adgangen til samfundsvigtige funktioner og ydelser, såsom strøm, transport eller internet bliver afbrudt eller forstyrret. Et destruktivt cyberangreb kan også medføre omfattende ødelæggelse af data og enheder.

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

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

Cyberaktivisme

Truslen fra cyberaktivisme mod Grønland er **LAV**. Det betyder, at det er mindre sandsynligt, at grønlandske myndigheder og virksomheder bliver udsat for forsøg på cyberaktivisme inden for de næste to år.

Cyberaktivisme kommer oftest til udtryk som overbelastningsangreb, såkaldte DDoS-angreb, og hack og læk af information fra myndigheder og virksomheder.

CFCS vurderer, at selvom der findes cyberaktivister, der har kapacitet til at udføre aktivistiske cyberangreb mod myndigheder og virksomheder i Grønland, er det mindre sandsynligt, at der aktuelt er hackere, der har intentioner om at udføre denne type angreb mod Grønland.

Truslen fra cyberaktivisme mod Grønland kan stige uden eller med kort varsel, hvis enkeltsager med forbindelse til Grønland får aktivistiske hackergruppers opmærksomhed. Da især overbelastningsangreb er lette at udføre uden væsentlig forberedelse, kan truslen fra denne type angreb hurtigt ændre sig.

Cyberangreb mod flere NATO-lande udført af pro-russiske cyberaktivister i kølvandet på konflikten i Ukraine har medført en øget trussel mod Danmark fra cyberaktivisme. Der er dog ikke tegn på, at denne trussel i samme udstrækning også er rettet mod Grønland. Skulle Grønland få en mere aktiv rolle i konflikten i Ukraine, kan truslen stige.

Cyberterror

Truslen fra cyberterror mod Grønland er **INGEN**. Det betyder, at 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 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 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 plan-lægning. 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.