Naalakkersuisut Suilittaasuat
Formanden for Naalakkersuisut

NAALAKKERSUISUT
GOVERNMENT OF GREENLAND

Pipaluk Lynge Rasmussen
Medlem af Inatsisartut Inuit Ataqatigit

Svar på § 37 spørgsmål 133/2022 om. Cybersikkerhed

Brevdato: 14. juli 2022

Sagsnr. 2022 - 14013
Akt. nr. 20602172

Postboks 1078
3900 Nuuk
Tel. (+299) 34 50 00

E-mail: digitalisering@nanoq.gl
www.naalakkersuisut.gl

Kære Pipaluk Lynge Rasmussen

Tak for dit spørgsmål vedr. cybersikkerhed som du stiller i henhold til Inatsisartuts forretningsorden. Jeg vil besvare dine spørgsmål herunder.

1. Har Naalakkersuisut en beredskabsplan for cybersikkerhed?
Centraladministrationen skal have mange beredskabsplaner, en beredskabsplan for hvert IT-system. Den vigtigste beredskabsplan er for centraladministrationens server- og netværk. Beredskabsplanen indgår i selve kontrakten med leverandøren. Ansvaret for beredskabsplaner for et konkret IT-system ligger hos den enhed, som har indkøbt et IT-system. Under cyberangrebet var de kritiske systemer ejet af: Digitaliseringsstyrelsen, Økonomi- og Personalestyrelsen, Inussuk IT, Grønlands Fiskerikontrol og Skattestyrelsen.

I efteråret 2021 var et forslag til et cirkulære om IT- og Informationssikkerheds-organisation samt en Informationssikkerhedspolitik i intern høring i centraladministrationen.

Cirkulæret fastsætter de overordnede kompetencer til at træffe afgørelser og handle under et cyberangreb. Ligeledes stiller cirkulæret krav om at alle enheder, der er driftsansvarlige for et IT-system, skal have udpeget en IT-systemejer. IT-systemejeren skal varetage alle forhold omkring den tekniske sikkerhed i forbindelse med et IT-system, herunder også at der er en beredskabsplan for IT-systemet. Informationssikkerhedspolitikken foreslår, at al indkøb, udvikling, drift og vedligeholdelse af IT-systemer skal administreres efter den internationale standard ISO 27001, der er et ledelsessystem for informationssikkerhed. ISO 27001 og IT-systemejer er begge tiltag, der skal mindske risikoen for cyberangreb og minimere skadevirkningen ved et cyberangreb.

Under cyberangrebet i marts 2022 blev den cyber- og informationssikkerhedsorganisering, der er foreslået i cirkulæret anvendt, selv om cirkulæret ikke formelt er godkendt endnu. Cirkulæret er lige nu igen i intern høring, da erfaringerne fra cyberangrebet viste, at der skal yderligere formelle krav til cyber- og informationssikkerheden for at kunne forbygge nye cyberangreb.

a) Hvis ikke, planlægger Naalakkersuisut da at udarbejde en beredskabsplan for cybersikkerhed?
Cyberangrebet har bidraget med nye erfaringer, der skal indarbejdes i eksisterende beredskabsplaner. Der er således igangsat et projekt til at kvalitetstjekke alle IT-

systemejeres beredskabsplaner, og udarbejde beredskabsplaner for de områder som ikke måtte have.

b) Hvordan forestiller Naalakkersuisut sig, at de parter, der varetager samfunds kritiske funktioner, kan blive involveret i udarbejdelsen og udmøntningen af en sådan beredskabsplan?
En del af cybersikkerheden er, at offentlige og andre samfunds kritiske IT-systemer ikke er sammenhængende. Centraladministrations-, Sundhedsvæsenets-, Nukissiorfiits, kommunernes og de selvstyreejede virksomheders IT-systemer skal være adskilte. Dette for at forhindre, at et cyberangreb på et af IT-systemerne kan brede sig til de andre. Hvert enkelt samfundskritisk IT-system skal have deres egne beredskabsplaner, som de enkelte områder har ansvaret for. Dette skyldes, at de samfundskritiske funktioner har meget forskellige forretningsgrundlag, hvilket beredskabsplanerne skal tage højde for.

Digitaliseringsstyrelsen tilbyder bistand i samarbejde med eksterne fagfolk til både offentlige myndigheder og private, for at sikre det bredest mulige kvalitetstjek af beredskabsplaner.

c) Hvilken myndighed i Grønlands Selvstyre ville være ressortansvarlig for en sådan beredskabsplan?
Digitaliseringsstyrelsen har jf. Cirkulære om ressortfordelingen ansvaret for cyber- og informationssikkerhed i centraladministrationen.

2. Har hackerangrebet mod Grønlands Selvstyre, der fandt sted i marts, foranlediget beredskabsmæssige forandringer i Grønlands Selvstyre?
Digitaliseringsstyrelsen har opgraderet eksisterende IT-systemer, der skal overvåge datatrafikken i centraladministrationens IT-systemer. Investeringen har til formål at styrke beskyttelsen mod cyberangreb, men også at forbedre mulighederne til at kunne inddæmme og standse et cyberangreb.

a) Hvilke andre initiativer i Grønlands Selvstyre foranledige hackerangrebet?
I svarene til spørgsmål 1 og 2 er beskrevet en række initiativer, der var iværksat før cyberangrebet og initiativer, der er iværksat som følge af cyberangrebet.

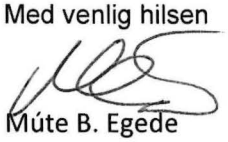
3. Såfremt Naalakkersuisut skal udarbejde en beredskabsplan for cybersikkerhed, der som minimum indtænker de parter, der varetager samfunds kritiske funktioner, hvad vil de økonomiske og administrative konsekvenser være for henholdsvis:
Som beskrevet i 1 b) skal alle samfunds kritiske funktioner have deres egne beredskabsplaner, der klart beskriver, hvordan et cyberangreb håndteres. Ligeledes er adskillelse mellem samfundskritiske funktioner også et vigtigt element.

a) Det offentlige?
Der vil over de næste par år skulle forventes flere omkostninger til indkøb, udvikling, drift og vedligeholdelse af IT-systemer i takt med at eksisterende kontrakter gennemgås, nye kontrakter implementeres og IT-systemerne gennemgår sårbarhedscanninger. IT-systemejeransvaret inkluderer bl.a.; leverandørstyring, systemopgraderinger, vedligehold af beredskabsplaner og andre procedurebeskrivelser.

b) Det private erhvervsliv?
Det private erhvervsliv skal anse øgede omkostninger til beskyttelse mod cyberangreb som en grundomkostning i deres forretningsmodel. Dette vil også gælde for selvstyreejede virksomheder.

c) Borgerne?
I en digital verden må borgerne se i øjnene, at de kan blive hacket eller ufrivilligt kan komme til at medvirke til at andre bliver udsat for et cyberangreb. Det må derfor stærkt anbefales, at alle borgere investerer i virusbeskyttelse til deres computere, tablets, mobiltelefoner og andre smarte ting, som urer, der har adgang til internettet.

Med venlig hilsen



Múte B. Egede