

A photograph of a rugged, snow-covered mountain peak. The mountain's surface is a mix of dark, jagged rock and patches of white snow. At the very top of the peak, several pieces of communication equipment are visible, including a tall antenna tower and a satellite dish. The background shows a vast, hazy landscape of rolling hills and valleys under a clear blue sky.

**Anbefalinger til at øge
sikkerhedsniveauet på
teleområdet**

Indledning

Naalakkersuisoq for Boliger og Infrastruktur Hans Peter Poulsen nedsatte den 21. februar 2024 arbejdsgruppen for sikkerhed på teleområdet. Formålet med nedsættelse af arbejdsgruppen var følgende:

Arbejdsgruppen skal fremlægge anbefalinger til Naalakkersuisut og Anlægsudvalget om:

- 1) hvordan der kan arbejdes langsigtet og målrettet med at fastholde og udbygge et højt sikkerhedsniveau i teleinfrastrukturen og teletjenesterne, og*
- 2) hvilke tiltag der kan implementeres og hvilke lovgivningsmæssige tiltag er nødvendige, for at øge sikkerheden og forbedre sikkerheden og redundansen i teleinfrastrukturen og for teletjenesterne.*

Sikkerhed på teleområdet omfatter organisatorisk sikkerhed, personrelateret sikkerhed, fysisk sikkerhed og teknologisk sikkerhed. Med andre ord, alt hvad der kan påvirke en teleudbyder og dennes forretning med at levere adgang til teleinfrastruktur og teletjenester.

Hvorfor skal vi have en robust telesektor?

Den fysiske trussel og cybertruslen imod teleinfrastrukturen er nogle af de mest alvorlige trusler og kan have alvorlige konsekvenser for samfundet.

Samfundet er igennem de seneste mange år blevet afhængigt af telekommunikation, fordi det understøtter næsten alle aspekter af det moderne liv og fungerer som en kritisk infrastruktur for borgere, virksomheder og samfundets institutioner.

Der er mange trusler mod telekommunikation, som bl.a. omfatter naturkatastrofer, tekniske fejl, terrorisme og sabotage, cyberangreb og overbelastning af netværk. Disse trusler kan påvirke samfundet alvorligt.

En robust telesektor kan modstå, tilpasse sig og overkomme en uforudsigelig kritisk hændelse, som kan være med til at sikre hurtig genopretning efter kriser, minimere tab og reducere den negative indvirkning på både drift og omdømme.

Hvad er samfundsvigtige funktioner og kritisk infrastruktur?

Samfundsvigtige funktioner er de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed. Kritisk infrastruktur er infrastruktur, herunder systemer, tjenester, processer, netværk, aktiver og serviceydelser, som er nødvendig for at opretholde samfundsvigtige funktioner og drift.

Strømnedbruddet i 2021

Mange borgere kan huske strømnedbruddet i november 2021, da strømmen blev afbrudt i Nuuk på grund af kraftige vindstød, da der opstod problemer med kablerne imellem byen og Buksefjorden. I forbindelse med nedbruddet, virkede Nukissiorfiits nødgeneratorer ikke. Strømnedbruddet medførte, at al telekommunikation var ude af drift i hele landet, da Tusass' egen nødgenerator, heller ikke virkede som planlagt.

Mangel på både el og telekommunikation medførte at særligt Nuuk, men også resten af landet, var i en undtagelsestilstand, hvor de fleste samfundsvigtige funktioner var ude af drift. Alarmtjenesten virkede ikke, hvorfor politi og brandvæsen kørte rundt i lokalsamfundene, hvor borgere blev opfordret at stå ved vejen og vinke i tilfælde af at de havde brug for akut hjælp. Butikkerne måtte lukke, da det ikke var muligt at betale for varerne. Der var ingen el eller varme i lejligheder.

Nedbruddet medførte, at de fleste samfundsvigtige funktioner var utilgængelige i et døgn, efterfulgt af ustabilitet i en uge, hvilket medførte tab for myndigheder, virksomheder og borgere.

Konsekvenserne ved den manglende telekommunikation, som myndigheder, virksomheder og borgere oplevede i forbindelse med nedbruddet, kunne også være indtruffet af andre årsager f.eks. søkabelbrud, cyberangreb, sabotage samt andre naturhændelser.

Hvad er NIS2?

NIS2 er den almindelige betegnelse for EU-direktiv (EU) 2022/2555, som fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU. NIS2-direktivet bygger på EU-direktivet om sikkerhed i net- og informationssystemer (NIS1-direktivet).

Arbejdsgruppen har bestået af repræsentanter fra Telestyrelsen, Departementet for Boliger og Infrastruktur, Digitaliseringsstyrelsen, Tusass A/S samt Center for Cybersikkerhed.

Anbefalinger

1. At Naalakkersuisut og Inatsisartut implementerer lovgivning, som sikrer at Telestyrelsen får et klart mandat til at agere som myndighed på teleområdet, hvor Telestyrelsen bemyndiges til at føre tilsyn med overholdelse af den relevante lovgivning og regler udstedt i medfør af denne.
2. Som er del af denne lovgivning fastsættes regler for teleudbydere, som tager udgangspunkt i de krav, der er fastsat i NIS2-direktivet og landets geografiske, demografiske og teleudbydernes økonomiske forhold, for at sikre teleforsyningen bedst muligt. Der tages udgangspunkt i følgende områder, men er ikke begrænset til disse:
 - a) krav om risikostyring for alle teleudbydere i forbindelse med risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i teleinfrastrukturen og teletjenesterne,
 - b) krav om at teleudbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger, for i videst muligt omfang at sikre udbuddet af net og tjenester i beredskabssituationer og andre ekstraordinære situationer,
 - c) at alle teleudbydere pålægges en underretningspligt i forbindelse med hændelser ved væsentlig indvirkning på driften af net eller tjenester, og at disse oplysninger er undtaget reglerne for aktindsigt,
 - d) at der stilles krav om sikkerhedsgodkendelse for særligt udvalgte medarbejdere hos væsentlige teleudbydere, når de pågældende, som led i deres konkrete opgaveløsning for udbyderen, skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i net og tjenester eller beredskab, og
 - e) at teleudbydere pålægges en oplysningspligt i forbindelse med anskaffelser af kritiske netkomponenter, og at disse oplysninger er undtaget reglerne for aktindsigt.

De enkelte anbefalinger uddybes herunder:

1. At Naalakkersuisut og Inatsisartut implementerer lovgivning, som sikrer at Telestyrelsen får et klart mandat til at agere som myndighed på teleområdet, hvor Telestyrelsen bemyndiges til at føre tilsyn med overholdelse af den relevante lovgivning og regler udstedt i medfør af denne

Sektoransvarsprincippet tilsiger, at den myndighed, som har ansvaret til hverdag, også er ansvarlig for beredskabet, kontinuitetsplanlægning og krisestyring under ekstraordinære forhold såsom katastrofer, kriser eller krig. Sektoransvaret ligger hos Naalakkersuisoq for Boliger og Infrastruktur jf. Cirkulære om fordeling af anliggender (ressortfordelingen).

Det anbefales, at Telestyrelsen får et klart mandat fra Naalakkersuisut og Inatsisartut til at agere som myndighed for sikkerhed på teleområdet. Dette begrundes med den gældende struktur på indretningen af teleområdet, samt den viden om televirksomhederne som allerede er opbygget i Telestyrelsen.

Det vil kræve opbygning af kompetencer i Telestyrelsen for løse disse kommende myndighedsopgaver, men det er nødvendigt at den kommende myndighed har kendskab til televirksomhederne, når der skal vurderes om disse lever op til de anbefalede krav vedrørende sikkerhed. Herudover vurderes det, at der er en synergieffekt mellem de kommende myndighedsopgaver for sikkerhed i forhold til de øvrige myndighedsopgaver på teleområdet.

2.a. Krav om risikostyring for alle teleudbydere i forbindelse med risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i teleinfrastrukturen og teletjenesterne

Det anbefales, at der fastsættes krav til alle teleudbydere om risikostyring, herunder at gennemføre en risikovurdering, der skal tage stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de net og tjenester, der udbydes.

En risikobaseret tilgang indebærer, at der skal arbejdes med at minimere risikoen for tab af tilgængeligheden, autenticiteten, integriteten og fortroligheden, hvor krav til sikkerheden skal opstilles på forhånd, for at skabe en robust teleinfrastruktur.

Tilgængelighed omfatter at telekommunikation, data og informationssystemer er tilgængelige, når der er behov for disse. **Autenticitet** vedrører pålidelighed og ægtheden for enheder, data eller personer. **Integritet** omhandler informationsaktivernes nøjagtighed, fuldstændighed og beskyttelse imod ændringer. **Fortrolighed** sikrer, at informationer ikke gøres tilgængelige eller deles med uautoriserede personer eller systemer.

For at opnå kravene i anbefalingerne, anbefales det at teleudbydere skal styre sikkerheden i infrastrukturen og tjenester igennem et ledelsessystem efter en anerkendt international standard, eksempelvis ISO/IEC 27001 eller tilsvarende. ISO/IEC 27001 giver teleudbyderne en struktureret tilgang til arbejdet med sikkerhed.

2.b. Krav om at teleudbyderne skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger, for i videst muligt omfang at sikre udbuddet af net og tjenester i beredskabssituationer og andre ekstraordinære situationer

Det anbefales at teleudbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for at sikre at organisationen kan håndtere beredskabssituationer og andre ekstraordinære situationer. Dette omfatter bl.a. udarbejdelse af en politik for håndtering af beredskabssituationer og andre ekstraordinære situationer med henblik på at sikre, at net og tjenester i videst muligt omfang kan opretholdes.

Beredskabssituationer og andre ekstraordinære situationer kan fx være større ulykker, katastrofer eller hændelser, hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner.

Teleudbydere skal som en del af fastlæggelsen af risikovilligheden i risikostyringsprocessen i ledelsessystemet fx ISO/IEC 27001, i videst muligt omfang tage højde for opretholdelsen af udbuddet i beredskabssituationer og andre ekstraordinære situationer, for at sikre samfundets teleforsyning.

2.c. At alle teleudbydere pålægges en underretningspligt i forbindelse med væsentlige sikkerhedsbrud og hændelser i infrastruktur eller tjenester, og at disse oplysninger er undtaget reglerne for aktindsigt

Det anbefales, at alle teleudbydere pålægges en underretningspligt, som sikrer at Telestyrelsen orienteres om væsentlige sikkerhedsbrud og hændelser vedrørende fortrolighed, integritet, autenticitet og tilgængelighed.

Definition af hvilke væsentlige sikkerhedsbrud og hændelser skal underrettes, bør fastsættes i lovgivningen på baggrund af landets geografiske og demografiske forhold.

Underretningspligten vil give Telestyrelsen et bedre overblik over de sikkerhedsmæssige udfordringer, som findes i infrastrukturen og tjenester for slutbrugerne over hele landet.

Det anbefales herudover, at disse underretninger er undtaget reglerne om aktindsigt, da det kan have negativ påvirkning af samfundets samlede sikkerhed og for teleudbyderen, hvis informationer om sårbarheder i infrastrukturen og i tjenesterne gives videre til tredje part.

2.d. at der stilles krav om sikkerhedsgodkendelse for særligt udvalgte medarbejdere hos væsentlige teleudbydere, når de pågældende, som led i deres konkrete opgaveløsning for udbyderen, skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i infrastruktur og tjenester eller beredskab

Det anbefales, at Telestyrelsen, i samarbejde med teleudbyderne, kan stille krav om at særlige nøglepersoner hos teleudbyderne skal sikkerhedsgodkendes. Dette for at orientere f.eks. den øverste ledelse hos teleudbyderen om en mulig kendt risiko eller om baggrunden for nødvendigheden af at prioritere kapaciteten eller eventuelt nedlægge adgangen for at afværge en endnu større risiko i forbindelse med beredskabssituationer eller ekstraordinære situationer.

2.e. At teleudbydere pålægges en oplysningspligt i forbindelse med anskaffelser af kritiske netkomponenter, og at disse oplysninger er undtaget reglerne for aktindsigt

Det anbefales, at teleudbydere pålægges at underrette Telestyrelsen forud for indgåelse af aftaler med leverandører om køb af udstyr eller tjenester af væsentlig betydning.

Telestyrelsen kan dermed opbygge en større viden om de enkelte teleudbydere, samt indgå i en dialog med teleudbyderne og evt. tredjepart udpeget af Telestyrelsen, om sikkerhedsmæssige aspekter vedrørende de påtænkte aftaler.

Teleudbydere bør arbejde proaktivt med sikkerhed, hvor der i stedet for at reagere på sikkerhedsproblemer, f.eks. efter et køb af udstyr er foretaget, tilsikrer at teleudbydere evaluerer leverandører, udfører risikovurderinger og stiller krav til sikkerheden, før kontrakter indgås. Dette med henblik på at minimere risikoen for at erhverve usikre eller sårbare enheder.

Teleudbydere er afhængige af en bred vifte af leverandører, der leverer udstyr og tjenester. Derfor skal teleudbydere sætte krav til sikkerheden i hele deres leverandørkæde, herunder for kritiske enheder, såsom netværksudstyr, servere og software. Teleudbydere bør kunne pålægges at tilsikre, at leverandører følger bestemte sikkerhedsstandarder og praksisser med henblik på at minimere risikoen for sårbarheder og angreb.

Teleudbyderes anvendelse af leverandører skal herudover indgå i risikovurderingen, som tager stilling til risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de net og tjenester, der udbydes.

Det anbefales ligeledes, at oplysninger som gives i forbindelse med oplysningspligten, vil være undtaget reglerne om aktindsigt. Undtagelsen begrundes i, at det kan have negativ påvirkning af samfundets samlede sikkerhed og teleudbyderne, hvis forretningshemmeligheder og informationer om anskaffelser og sårbarheder i net og tjenester gives videre til tredje part.