En sikrere teleinfrastruktur i Danmark

Cyber- og informationssikkerhedsstrategi for teleområdet 2022-2024

Indhold

Forside foto: Lars Laursen/Biofoto/Ritzau Scanpix

Indledning

Adgang til sikker og pålidelig kommunikation er en forudsætning for et digitalt samfund som det danske. Derfor indeholder denne cyber- og informations-sikkerhedsstrategi – *En sikrere teleinfrastruktur i Danmark* – en række handlings-orienterede initiativer. Initiativer der både er baseret på kravene i den nationale strategi for cyber- og informationssikkerhed og udbydernes egen interesse i at skabe en mere robust teleinfrastruktur.

Den nationale cyber- og informationssikkerhedsstrategi sætter fokus på, at samfundsvigtige funktioner understøttes af sikker og modstandsdygtig kritisk infrastruktur. Opretholdelse af samfundets robusthed er et fælles ansvar, og der er afhængigheder mellem de samfundsvigtige områder. Eksempelvis kræver opretholdelse af teleforsyningen en stabil energiforsyning, og opretholdelse af finanssektoren forudsætter adgang til både tele og energi.

Den nationale strategi udvides også i både bredden og dybden. Det betyder, at der i denne strategiperiode vil være markant flere snitflader til andre samfundsvigtige områder, funktioner og kritisk infrastruktur. Det betyder, at aktørerne på tele-området, i højere grad end tidligere, skal samarbejde med aktører fra andre områder i samfundet. Det forventes, at denne del-strategi på teleområdet vil bidrage til, at samarbejdet med de øvrige samfundsvigtige områder bliver fokuseret og forløber til gavn for de enkelte områder og Danmark som helhed.

En fortsat udvikling og udbygning af en robust teleinfrastruktur i Danmark er afhængig af adgang til – og tilgængelighed af – de rette kompetencer.

I takt med, at cyber- og informationssikkerhed får større politisk bevågenhed og etableringen af flere decentrale cyber- og informationssikkerhedsenheder (DCIS), er det forventningen, at efterspørgslen efter kompetencer inden for cyber- og informationssikkerhed vil stige.

Det medvirker til, at der på teleområdet fortsat er behov for at styrke de nuværende kompetencer via uddannelse og øget viden og informationsdeling. Det er forvent-ningen, at nogle af initiativerne i denne strategi kan bidrage hertil.

Den nationale strategi for cyber- og informationssikkerhed stiller krav om, at DCIS'er skal have en operativ kapacitet i dagtimerne. I den forbindelse igangsættes der initiativer på teleområdet med henblik på, at en sådan kapacitet bliver løftet senest ved udgangen af 2022.

Denne del-strategi fastlægger rammerne for cyber- og informationssikkerhedsarbejdet på teleområdet frem til og med 2024.

Trusselsbilledet er dynamisk, og DCIS på teleområdet (TeleDCIS) udarbejder en årlig risiko- og sårbarhedsvurdering, som vil bidrage til at prioritere arbejdet med robusthed og sikkerhed på teleområdet et år ad gangen. Således er ikke alle risici, sårbarheder og behov kendt på nuværende tidspunkt, hvorfor der kan ske opdateringer af strategien undervejs strategiperioden.

Brancheforeningerne Dansk Industri, Green Power Denmark, Teleindustrien, IT-Branchen og Dansk Erhverv deltager i udviklingen og implementeringen af strategien med Center for Cybersikkerhed som ansvarlig myndighed. Dermed sikres en bred forankring af strategien hos de væsentlige interessenter på teleområdet.

Fokusområder

Hovedopgaven med denne strategi er at skabe en sikrere teleinfrastruktur, hvilket er udgangspunktet for alle initiativer i strategien. Store dele af teleområdet står på mange områder rigtig stærkt, men området kan komme endnu længere op ad modenhedstrappen, når det handler om eksempelvis videns- og informationsdeling, udvikling af kompetencer og tillid mellem udbydere, der konkurrerer på kommercielle vilkår.

Derfor indeholder strategien fire fokusområder, som den fælles indsats koncentreres om i perioden for 2022 – 2024:

1. Øget robusthed
2. Udvidet videns- og informationsdeling
3. Styrkede kompetencer, uddannelse og tillid
4. Operativ DCIS kapacitet

Hver af de fire fokusområder er konkretiseret med initiativer, der indeholder klare succeskriterier. Det bidrager til, at det bliver nemmere at følge op på, hvorvidt implementering af strategien forløber planmæssigt hen over strategiperioden.

Den nationale strategi for cyber- og informationssikkerhed

Regeringens nationale strategi for cyber- og informationssikkerhed, der udkom i december 2021, indeholder en række initiativer, der skal understøtte at samfundsvigtige funktioner er robuste og modstandsdygtige.

I den forbindelse vil aktørerne på teleområdet sammen med Center for Cybersikkerhed – udover de ovenstående fire fokusområder – også bidrage til, at blandt andet følgende initiativer i den nationale strategi opfyldes:

- Afdækning af kritisk infrastruktur (initiativ 1.11)
- Blokering af ondsindede domæner (initiativ 1.14)
- Alternativ til satellitbaseret tidsstyring (initiativ 1.15)
- Fælles tekniske løsninger (initiativ 1.5.4)

Initiativer og succeskriterier

1. Øget robusthed

Robusthed er nøglen til høj sikkerhed på teleområdet, og der skal løbende arbejdes med robusthed indenfor forskellige områder. Dette fokusområde indeholder tre konkrete initiativer, der skal bidrage til at øge robustheden på teleområdet.

Med det formål at få en endnu højere grad af robusthed i telesektoren går et af initiativerne på at gennemføre beredskabsøvelser. Øvelserne kan gå på tværs af de samfundsvigtige områder og gerne med deltagelse af Center for Cybersikkerhed (CFCS). Initiativ 1.5.4 i den nationale strategi anbefaler én øvelse pr. år, hvori øvelsen for DCIS-medlemmer kan indgå. Ud over de interne beredskabsøvelser, som gennemføres i dag, er der også en forventning om eksempelvis at deltage i den nationale krisestyringsøvelse, KRISØV m.fl.

Den russiske invasion i Ukraine medfører, at der fremover kan forventes en anderledes situation i forhold til cybersikkerheden i Europa. Truslen mod teleinfrastrukturen er indeholdt i trusselsvurderingerne fra CFCS, og en styrket robusthed overfor fremmede magters interesse i at skade nationen og dens teleinfrastruktur er blevet endnu mere aktuelt.

Som andre sektorer benytter telesektoren underleverandører til levering af visse teletjenester, herunder også outsourcing udbyderne imellem.

Derfor fokuserer to andre initiativer på at styrke robustheden ved at fokuserer på afhængigheder på tværs af de forskellige erhvervsmæssige teleudbydere og på bedre leverandørstyring.

1.1 Beredskabsøvelser

Formål

Udbyderne indøver og træner de beredskabsplaner, der løbende tilrettes for at kunne imødegå aktuelle trusler samt de scenarier som den årlige risiko- og sårbarhedsvurdering, der udarbejdes af TeleDCIS, identificerer.

Succeskriterier

- ✓ Væsentlige erhvervsmæssige teleudbydere har afholdt beredskabsøvelser mindst en gang årligt – enten som en individuel øvelse eller i regi af TeleDCIS.
- ✓ Der er afholdt TableTop-øvelser, som er scenarie-baseret efter risiko- og sårbarhedsanalysen, en til to gange årligt. TeleDCIS er ansvarlig for afviklingen af øvelserne blandt sine medlemmer.
- ✓ Alle væsentlige erhvervsmæssige teleudbydere har deltaget i de nationale øvelser, som afholdes af CFCS/andre.

1.2 Afhængigheder

Formål
De erhvervsmæssige teleudbydere identificerer afhængigheder imellem hinandens teleinfrastruktur. Dette sker især med henblik på kabling/fiber, telemaster, centraler/datacenter etc. Derved kan selskaberne i fællesskab styrke mitigerings-arbejdet i forbindelse med trusler og sårbarheder.

Succeskriterier

- ✓ De erhvervsmæssige teleudbydere har udarbejdet en oversigt over de afhængigheder, der er mellem udbyderne.
- ✓ Der er fastsat en proces for vedligeholdelse af denne oversigt med henblik på sikring af kontinuerlig opdatering.

1.3 Leverandørstyring

Formål
Leverandører til teleområdet skal ses som udbydernes forlængede arm og skal minimum have et tilsvarende sikkerhedsniveau som udbyderne selv – såfremt de leverer til kritiske netkomponenter, systemer eller værktøjer.

Succeskriterier

- ✓ Teleselskabernes leverandører lever op til best practice-sikkerhed og er bekendt med ISO27001-krav. Dette vurderes og evaluseres årligt i forbindelse med risiko- og sårbarhedsvurderingen, som udarbejdes af TeleDCIS.
- ✓ Leverandørerne har en beskrevet og opdateret beredskabsplan samt en risiko- og sårbarhedsvurdering. Dette vurderes og evalueres årligt i forbindelse med risiko- og sårbarhedsvurderingen, som udarbejdes af TeleDCIS.

2. Videns- og informationsdeling

De erhvervsmæssige teleudbyderne samarbejder allerede om en række informationssikkerhedsrelaterede emner. Blandt andet har der i en længere årrække været et forum til informationsdeling og kontakt mellem de teknikere, der forestår den praktiske hændelseshåndtering hos nogle af de væsentlige erhvervsmæssige udbydere.

Udbyderne ønsker at styrke deling af viden og information blandt andet gennem deling af såkaldt "threat intel". Det er ambitionen, at det kan blive et fastforankret tværfagligt samarbejde med en fælles platform, metodik og politikker, så der hurtigt og enkelt kan deles informationer mellem udbyderne.

Det er væsentligt, at de erhvervsmæssige teleudbydere gennem vidensdeling kan øge mulighederne for at imødegå de trusler, der retter sig mod teleområdet og at skabe værdi for den enkelte udbyder. Hensigten er at forankre villigheden til at dele information bredt og styrke værdien for fællesskabet.

Da det grundlæggende er de samme trusler, som de enkelte udbydere står overfor, er der en målsætning om at dele information om, hvad ondsindede aktører foretager sig. Deling af threat intel skal ske i anonymiseret form, via TeleDCIS, så interne data om eksempelvis personer, infrastruktur og andet beskyttelsesværdigt ikke fremgår. Samarbejdet vil indledningsvist koncentrere sig om opbygning af vidensdelingsmodeller, platforme og metodikker for, hvordan udbyderne i praksis etablerer en solid vidensdeling.

Ligeledes skal muligheden for, at en tredjepart kan levere threat intel – eventuelt med TeleDCIS som koordinator – undersøges mht. pris og kvalitet.

Teleområdet er ét blandt 18 samfundsvigtige områder. Som følge heraf er samarbejde mellem de 18 respektive områders virksomheder, organisationer og myndigheder afgørende for at opretholde et robust og sikkert Danmark. Aktørerne på teleområdet vil arbejde for, at viden og informationer om best practices mv. deles med relevante aktører i andre samfundsvigtige områder.

CFCS vil som sektoransvarlig myndighed rådgive og vejlede udbyderne om informationssikkerhed, beredskab og leverandørsikkerhed på teleområdet.

TeleDCIS skal via rådgivning og koordination bidrage til at en øget videns- og informationsdeling dels internt mellem udbyderne på teleområdet, dels mellem de øvrige samfundsvigtige områder, herunder ikke mindst til de områder, som teleområdet er mest afhængige af.

2.1 Threat intel

Formål
Der etableres en ramme, hvor udbyderne hurtigt og sikkert kan samarbejde om vidensdeling i forbindelse med cybertrusler. Samarbejdet skal være konstruktivt, fremadrettet og bidrage til en fælles forståelse af truslen, som igen kan bidrage til en sikrere teleinfrastruktur samt indgå CFCS' udarbejdelse af en samlet trusselsvurdering på teleområdet.

Succeskriterier
- ✓ Der er etableret en platform og skabelon til deling af udbydernes threat intel.
- ✓ Der er indgået en aftale om hvilke informationer, der kan deles.
- ✓ Der er valgt en Point-of-Contact (PoC) hos de enkelte udbydere. Formålet med en PoC er at opnå en hurtig og effektiv videns- og informationsdeling.
- ✓ Der er foretaget en analyse og evaluering i forhold til behovet for en ekstern leverandør af threat intel. Såfremt der er et behov for en ekstern leverandør, er der endvidere foretaget en udvælgelse/anbefaling af leverandør(er).

2.2 Vidensdeling

Formål
At styrke vidensdeling mellem de erhvervsmæssige teleudbydere og myndigheder, hvilket er essentielt for at kunne respondere hurtigt i tilfælde af cyberangreb eller -trusler. Det skal sikres, at information fordeles hurtigt samtidig med, at den enkelte udbyder kan bibeholde sin anonymitet.

Succeskriterier
- ✓ Behovet for vidensdeling på teleområdet er afdækket og er bredt understøttet af de erhvervsmæssige teleudbydere. Dette foretages i samarbejde mellem udbyderne og TeleDCIS.
- ✓ Der er etableret en metode for relevant og prioriteret vidensdeling på tværs af samfundsvigtige områder og deres DCIS'er. Dette kan ske gennem DCIS-forum eller lignende tværgående samarbejde.
- ✓ Der er etableret effektive processer for vidensdeling inden for teleområdet og mellem de respektive myndigheder[1] på området.
- ✓ Den operationelle vidensdeling er styrket markant således, at CFCS og aktørerne på teleområdet deler viden og information rettidig for derved at styrke robustheden. Dette evalueres gennem et spørgeskema og interview med udbyderne om, hvorvidt de modtager de relevante oplysninger på det rigtige tidspunkt. TeleDCIS varetager spørgeskemaudsendelse og interviews.
- ✓ Der er oprettet en statistik over omfanget af information fra CFCS, der månedligt er delt med TeleDCIS og de erhvervsmæssige teleudbydere.

[1] CFCS, Styrelsen for Dataforsyning og Infrastruktur samt Erhvervsstyrelsen

3. Kompetencer, udvikling og tillid

Awareness, kvalifikationer og uddannelse er centrale elementer i cyberforsvaret. Der er mangel på såvel specialister som generalister med de rette sikkerhedskompetencer. Denne mangel forventes at stige i takt med, at flere og flere samfundsvigtige områder øger fokus på cyber- og informationssikkerheden. Der er således behov for, at udbuddet øges. Teleindustrien (TI) og TeleDCIS vil derfor arbejde for, at der bliver uddannet medarbejdere i telesektoren samt vidensdele med de øvrige samfundsvigtige områder.

TI og TeleDCIS vil desuden undersøge, om det er muligt at få specifikke cyber-sikkerhedskurser og mulighed for at afvikle kurser for telesektoren og telesektorens DCIS således, at medarbejderne i sektoren samtidig får lejlighed til at danne netværk og opbygge gensidig tillid. Dette skal også bidrage til at informationsdeling i forbindelse med hændelser bliver lettere at gennemføre i praksis.

Desuden er det et mål at opbygge relationer på tværs af de erhvervsmæssige teleudbydere for derved at skabe en tryg ramme, der kan understøtte vidensdeling og andre faglige samarbejder.

3.1 Uddannelse og kompetenceudvikling

Formål

At løbende dygtiggøre og fastholde medarbejderne hos de erhvervsmæssige tele-udbydere for derved at skabe værdi og robusthed for de enkelte udbyderne og på teleområdet som helhed – for derved også at undgå, at medarbejderne skifter væk fra teleområdet.

Succeskriterier

- TI og TeleDCIS har nedsat et koordinationsudvalg med henblik på at afdække muligheden for at oprettet et 'Telecyber Akademi' eller lignende kompetenceudvikling. Afdækningen skal være færdig Q1 2023.
- TI og TeleDCIS har nedsat et koordinationsudvalg, som belyser mulighederne for, at selskaberne kan deltage på cyberkonferencer/-træning i eksempelvis NATO-/EU-regi. Koordinationsudvalget vil søge at etablere et offentligt-privat samarbejde på området. Afdækningen skal være færdig Q1 2023.

3.2 Styrkelse af netværk

Formål
Aktørerne på teleområdet har et ønske om at opbygge loyalitet og personlige relationer på tværs af branchen for derved at skabe den nødvendige tillid i forbindelse med vidensdeling, samt at teleområdet bliver et endnu bedre sted at arbejde.

Succeskriterier

- Der er afholdt gå-hjem-møder/arrangementer med henblik for at udveksle informationer/blive informeret om faglige emner vedrørende cybersikkerhed, samt styrkelse af det sociale netværk minimum hver tredje måned.
- Der er etableret arbejdsgrupper omhandlende cybersikkerhed for at understøtte både faglige og sociale relationer. Dette varetages i regi af TI og TeleDCIS.
- TI og TeleDCIS har skabt en ramme for og afholdt mindst en telecyber-konference inden udgangen af strategiperioden (2024).

4. Operativ DCIS kapacitet

Den nationale strategi for cyber- og informationssikkerhed stiller krav om, at DCIS'er skal have en operativ kapacitet i dagtimerne. I den forbindelse igangsættes der to initiativer på teleområdet med henblik på, at en sådan kapacitet bliver løftet senest ved udgangen af 2022.

Siden den forrige nationale strategi har DCIS-funktion på teleområdet været varetaget af foreningen TeleDCIS, hvor de erhvervsmæssige udbydere på teleområdet har mulighed for at være medlemmer. Denne model har fungeret hensigtsmæssigt og TeleDCIS løfter en række opgaver, herunder udarbejdelse af en samlet risiko- og sårbarhedsvurdering, øvelsesaktiviteter samt vidensdeling udbyderne imellem og mellem udbyderne og CFCS.

Det nuværende samarbejde om de opgaver, som en DCIS er forpligtet til at udføre, ønskes fortsat og udvidet mellem de erhvervsmæssige udbyderne på teleområdet og med CFCS som myndighed på området. For at sikre den operative kapacitet igangsættes der to konkrete initiativer, som fremgår af nedenstående.

1.1 Analyse af opgaver

Formål

Der gennemføres en analyse med udgangspunkt i de nye opgaver til en DCIS, som er fastlagt i medfør af den nationale strategi. Analysen kommer med anbefalinger til fordelingen af opgaver mellem foreningen TeleDCIS og CFCS.

Analysen gennemføres af CFCS, TeleDCIS og TI med CFCS som ansvarlig myndighed.

Succeskriterier

- ✓ Der er udarbejdet en analyserapport med konkrete anbefalinger til organisering og fordeling af opgaver for den operative kapacitet for DCIS'en på teleområdet.
- ✓ Analyserapporten er færdig tidsnok til, at den kan indgå i arbejdet med initiativ 4.2.

1.2 Samarbejdsaftale mellem TeleDCIS og CFCS

Formål

Der indgås en skriftlig samarbejdsaftale mellem foreningen TeleDCIS og CFCS om den operative kapacitet. Samarbejdsaftalen skal i tillæg til den eksisterende samarbejdsaftale af 29. maj 2019 fastlægge rammerne for de nye opgaver, som foreningen TeleDCIS varetager på vegne af CFCS, der er myndighed for informationssikkerhed, beredskab og leverandørsikkerhed. Samarbejdsaftalen skal tage højde for de anbefalinger, som fremgår af den analyserapport, som er udarbejdet i forbindelse med initiativ 4.1.

Succeskriterier

- ✓ Samarbejdsaftalen skal blandt andet indeholde aftaler om, hvordan opgaverne i forbindelse med at drive en DCIS med en operativ kapacitet fordeles mellem foreningen TeleDCIS og CFCS, herunder udarbejdelse af risiko- og sårbarhedsvurderinger, øvelsesaktiviteter og vidensdeling, samt hvornår og hvordan aftalen evalueres.
- ✓ Samarbejdsaftalen underskrives af TeleDCIS og CFCS inden udgangen af 2022 og skal omhandle samarbejdet i indeværende strategiperiode.

Governance

Aktørerne på teleområdet har organiseret udarbejdelsen af strategien i et koordinationsforum bestående af de væsentlige erhvervsmæssige udbydere og brancheforeningerne Dansk Industri, Green Power Denmark, Teleindustrien, IT-Branchen og Dansk Erhverv og med inddragelse af CFCS.

Strategien er forankret i TI og TeleDCIS, som forestår udarbejdelse, løbende opdatering og implementering af strategien med inddragelse af koordinationsforummet og ikke mindst CFCS som myndighed for informationssikkerhed, beredskab og leverandørsikkerhed på teleområdet.

Den decentrale cyber- og informationssikkerhedsenhed på teleområdet

Opgaven som DCIS på teleområdet varetages af en forening. Medlemmer i foreningen er erhvervsmæssige og væsentlige erhvervsmæssige udbydere af net og tjenester.

Foreningens formål er at samle erhvervsmæssige udbydere i et forpligtende samarbejde med henblik på at varetage medlemmernes forpligtelse for opretholdelse af en sektorspecifik DCIS i henhold til det nationale beredskab.

TeleDCIS ledes af en bestyrelse, der består af væsentlige erhvervsmæssige udbydere, som opfylder kravene hertil i reguleringens forstand. TeleDCIS er åben for medlemskab for alle erhvervsmæssige udbydere af telenet og teletjenester uanset størrelse. Jfr. National strategi for cyber- og informationssikkerhed skal TeleDCIS have operativ kapacitet, eksempelvis mellem 8.00 og 16.00.

TeleDCIS har bl.a. opgaven med at facilitere den løbende opdatering/udvikling af:

- Risiko- og sårbarhedsvurdering.
- Beredskabsplanlægning og facilitering af øvelser.
- Vidensdeling mellem aktørerne på teleområdet.
- Koordinering af uddannelse, kompetenceudvikling og netværk.
- Operationel håndtering af sikkerhedshændelser.
- Vidensdeling på teleområdet og på tværs af samfundsvigtige områder.
- Udarbejdelse af en intern trusselsvurdering for telesektoren.
- Udarbejdelse af vejledninger om cybersikkerhed på teleområdet.
- Facilitere det fremadrettede arbejde omkring implementering af NIS2-direktivet.

Referencer

Regeringen (2021): *National strategi for cyber- og informationssikkerhed*

Center for Cybersikkerhed (2022): *Cybertruslen mod telesektoren*