Telesektoren

Teracom, Telenor, HI3G, GlobalConnect (inkl. Nianet), STOFA (inkl. SE), TDC (inkl. Dansk Kabel TV), Eniig, Fibia, Waoo, Telia, Dansk Beredskabskommunikation

Cyber- og Informationssikkerhedsstrategi for telesektoren

12 initiativer til en sikrere teleforsyning i Danmark

November 2018

Cyber- og informationssikkerhedsstrategi for telesektoren

Telesektoren
Cyber- og Informationssikkerhedsstrategi
November 2018

Indhold

1 Indledning

I den nationale cyber- og informationssikkerhedsstrategi fra maj 2018[1], er der udpeget seks samfundskritiske sektorer, som har betydning for opretholdelse af et robust og sikkert Danmark. En af disse sektorer er telesektoren. Opretholdelse af samfundets kommunikationsevne, herunder særligt for samfundskritiske beredskabsaktører - under alle forhold - er et vigtigt element i at sikre et velfungerede samfund.

Den danske telesektor har i en årrække arbejdet målrettet for at modernisere teleinfrastrukturen, og der er i dag høj tilgængelighed af mobiltelefoni og bredbånd overalt i Danmark.

Sikring af samfundets adgang til kommunikation er kerneydelsen for telesektoren. Derfor har det været naturligt, at brancheforeningerne Dansk Industri, Dansk Energi, Teleindustrien, IT-Branchen og Dansk Erhverv tog imod invitationen til at medvirke til implementeringen af cyber- og informationsstrategien i telesektoren. Sammen med udbyderne har brancheforeningerne i løbet af 2018 arbejdet målrettet med strategiimplementering, herunder udarbejdelse af nærværende strategi for cyber- og informationssikkerhed i telesektoren.

Modsat de øvrige fem udpegede samfundskritiske sektorer er strategiudvikling på teleområdet drevet af sektoren og ikke af sektormyndigheden. Telesektoren er tilfredse med, at sektorens myndighed Center for Cybersikkerhed har medvirket til, at der i strategiimplementeringen kan lægges tyngde på initiativer, der skaber værdi for sektoren. I det efterfølgende vil betegnelen telesektoren som minimum omfatte ovenstående myndighed, foreninger og udbydere. Telesektoren vil følge op på implementeringen af strategiens initiativer.

Opretholdelse af samfundets robusthed er et fælles ansvar. Der er afhængigheder mellem sektorerne. Eksempelvis kræver opretholdelse af teleforsyningen adgang til energi, og opretholdelse af finanssektoren forudsætter adgang til tele og energi. Telesektoren vil med strategien forsat arbejde med at styrke robustheden i telesektoren, men vil også gå aktivt ind i samarbejdet med de øvrige sektorer for at sikre, at sektorerne har den kommunikationskapacitet og –evne som er nødvendig for varetagelse af deres sektorspecifikke opgaver.

Forsat sikker udvikling og udbygning af teletjenester i Danmark er dog også afhængigt af adgang til - og tilgængelighed af - de rette kompetencer. I takt med cyber- og informationssikkerhed har fået større politisk bevågenhed, er der sket en betydelig stigning i efterspørgslen på cyber- og informationssikkerhedskompetencer i både den offentlige - og den private sektor. Således kæmper telesektoren, myndigheder og øvrige sektorer dagligt med at rekruttere og tiltrække generalister og specialister med cyber- og informationssikkerhedskompetencer.

Telesektoren opfordrer til, at myndighederne samarbejder aktivt med uddannelsesinstitutionerne om at tilvejebringe efteruddannelse for eksisterende medarbejdere, etablere

[1] https://digst.dk/media/16815/national_strategi_for_cyber-_og_informationssikkerhed_pdfa.pdf

dedikerede cyber- og informationssikkerhedsuddannelser på bachelor- og kandidatniveau, samt sikre at cyber- og informationssikkerhed indgår som et delemne på alle niveauer i uddannelserne i Danmark.

Med denne strategi fastlægger telesektoren rammerne for cyber- og informationssikkerhedsarbejdet frem til 2021. Ikke alle behov eller initiativer er kendt på nuværende tidspunkt, hvorfor der vil ske opdatering af strategien undervejs. Trusselsbilledet er dynamisk, og sektoren udarbejder en årlig risiko- og sårbarhedsvurdering som vil dimensionere næste års arbejde med robusthed og sikkerhed i telesektoren.

2 Governance for det fortsatte strategiarbejde

Telesektoren har organiseret arbejdet med udarbejdelsen af strategien omkring et koordinationsforum bestående af de væsentlige erhvervsmæssige udbydere og brancheforeningerne Dansk Industri, Dansk Energi, Teleindustrien, IT-Branchen og Dansk Erhverv. Det er besluttet, at fortsætte dette forum for at sikre den løbende opfølgning på initiativer og strategi i strategiperioden 2018-2023.

Det er endvidere besluttet, at de væsentlige erhvervsmæssige udbydere nedsætter en selvstændig juridisk enhed til styring af opgaven med at drive sektorens decentrale cyber- og informationsikkerhedsenhed (DCIS). Enheden ledes af en bestyrelse, der består af udbydere der opfylder kravene til at være en væsentlig erhvervsmæssig udbyder i reguleringens forstand. Adgang til DCIS er åben for alle erhvervsmæssige udbydere af telenet og teletjenester uanset størrelse. DCIS har bl.a. opgaven med at facilitere den løbende opdatering af telesektorens risiko- og sårbarhedsvurdering. Risiko- og sårbarhedsvurderingen for telesektoren godkendes af bestyrelsen for DCIS.

3 Risiko – og sårbarhedsvurdering for telesektoren

Telesektoren har i efteråret 2018 udarbejdet en risiko- og sårbarhedsvurdering. Den sektorspecifikke risiko- og sårbarhedvurdering har fokus på konsekvenserne af hændelser i telesektoren for samfundet[2] - ikke for det enkelte selskab. Denne risiko- og sårbarhedsvurdering er et øjebliksbillede baseret på de input, der er modtaget fra sektoren i september 2018. Opretholdelse af et retvisende billede kræver mindst én årlig opdatering, således der kan tages høje for nye erfaringer, trusler og nye teknologier. I telesektoren faciliterer DCIS'en opgaven med en årlig opdatering af risiko- og sårbarhedsvurderingen. Det bemærkes, at i forhold til løbende identifikation af kritisk teleinfrastruktur, som er genstand for risiko- og sårbarhedsvurderingen, så er alle væsentlige erhvervsmæssige udbydere i dag forpligtet til at føre og vedligeholde et register over udbyderens kritiske netkomponenter, systemer og værktøjer[3].

Vurderingen viser, at den danske telesektor generelt leverer høj tilgængelighed på de udbudte tjenester. Det er sjældent, at der optræder landsdækkende og langvarige udfald. Når det sker, er det eksempelvis på grund af sektorens afhængigheder til andre sektorer, så som elforsyningen. Uden strøm kan alle teletjenester ikke opretholdes i længere tid. Når det er sagt, skal det også fremhæves, at der generelt også er en høj el-forsyningssikkerhed i Danmark.

Risiko- og sårbarhedsvurderingen viser, at udbyderne vurderer IP-transmission som den mest sårbare tjeneste – langt mere end mobiltelefoni. IP-transmission er den kommunikationsteknologi, der eksempelvis leverer internettjenester, IP-telefoni og transmission af mobildata. IP-transmission er åbenlyst afhængig af strøm, men er også forholdsvis let at udfordre på tilgængelighed ved overbelastningsangreb (såkaldt DDOS) eller forvanskning af afsender- modtagerinformation (såkaldt spoofing), hvor en angriber ændrer kommunikation til at vise, at kommunikationen er til en forfalsket modtager eller kommer fra en forfalsket afsender. I takt med den fortsatte stigning i brugen af internettjenester og lign., vil betydningen af IP-transmissionen kun vokse.

IP-transmission vurderes at være særligt sårbar over for menneskelige fejl eller insiderangreb. Dette betoner behovet for udvekslings af best practice mellem udbydere for at lære af hinanden i sektoren og behovet for at opretholde fokus på imødegåelse af truslen fra insidere. Cyberangreb på underleverandører ses også som en væsentlig risiko for IP-transmission. Transmissionskapacitet lejes og deles løbende mellem udbydere, og vurderingen tyder på, at udveksling af best practice på leverandørstyring med fordel kan styrkes.

Vurderingen viser endvidere, at broadcasttjenester betragtes som næstmest sårbar - særligt overfor menneskelige fejl og insidere, samt varme og fysisk sabotage. Selv om skalsikring af eksempelvis master eller broadcastknudepunkter er en del af udbyderens

[2] https://brs.dk/viden/publikationer/Documents/S%C3%A5rbarhedsudredning_2004.pdf p.50

[3] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20567%20af%201.%20juni%202016%20om%20informationssikkerhed%20og%20beredskab%20i%20net%20og%20tjenester.pdf §11

ansvar viser analysen, at konsekvenserne for tjenesten ved fysisk sabotage er omfattende. Muligheden for myndighedsbeskyttelse af master og broadcastknudepunkter med fysisk magt i tilfælde af kriser bør indgå i en nærmere dialog mellem telesektoren og telemyndigheden.

Initiativer som følger af risiko- og sårbarhedsvurderingen

På baggrund af den udarbejdede risiko- og sårbarhedsvurdering har telesektoren identificeret en række initiativer, der kan bidrage til at styrke sikkerheden.

Initiativ 1: Styrket indsats mod angreb fra insidere
Betjening af telekommunikationsinfrastrukturen er en specialistopgave. Udbyderne har veluddannet personale til varetagelse af disse opgaver. Som i alle andre sektorer kan nøglepersonel med særlige adgange påføre infrastrukturen betydelig skade, såfremt den særlige adgang misbruges. Selv om der er få eksempler på misbrug via insidere i telesektoren, vil telesektoren tage initiativ til, at der gennemføres fælleskursus i sektoren i samarbejde med PET i at styre evnen til opdage og imødegå insidere[4].

Initiativ 2: Styrket leverandørstyring
Som andre sektorer, benytter telesektoren underleverandører til levering af visse teletjenester, herunder også outsourcing mellem udbydere. Det følger af eksisterende regulering, at CFCS skal inddrages ved indkøb af kritiske netkomponenter[5]. Vurderingen viser, at risikoen for cyberangreb på en underleverandør fremdeles ses som en væsentlig risiko. Som supplement til eksisterende regulering vil telesektoren i rollen som underleverandør og på baggrund af en konkret risikovurdering som hovedregel sikre, principperne i ISO2700x følges i forbindelse med sikkerhedsleverancen, og at information om evt. cyberangreb på delt infrastruktur deles med andre udbydere.

Initiativ 3: Undersøge muligheden for sikring mod fysisk sabotage i forbindelse med kriser og lignende
Risiko- og sårbarhedsvurderingen viser, at risikoen for fysisk sabotage vurderes som alvorlig. Teleudbyderne sikrer generelt infrastrukturknudepunkter, fiberbrønde og master til at imødegå fysiske angreb, men aktiv bevogtning af knudepunkter i forbindelse med kriser ligger uden for udbydernes muligheder. På den baggrund vil telesektoren i samarbejde med Center for Cybersikkerhed undersøge muligheden for, at eksempelvis hjemmeværnet kan varetage bevogtning af særligt følsomme infrastrukturknudepunkter i tilfælde af kriser og lign.

[4] https://www.pet.dk/Forebyggende%20Afdeling/Kurser.aspx projekt insider.

[5] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20566%20af%201.%20juni%202016%20om%20oplysnings-%20og%20underretningspligter%20vedr%C3%B8rende%20net-%20og%20informationssikkerhed.pdf §3

Initiativ 4: Styrkelse af samarbejdet mellem el- og telesektoren
Selv om Danmark generelt har en høj energiforsyningssikkerhed, viser vurderingen, at bortfald af strøm vil påvirke teleforsyningen, selv om knudepunkter og telemaster generelt har nødstrømskapacitet. Det skærpe trusselsbillede viser dog, at længerevarende bortfald af strøm i tilfælde af en skærpet geopolitisk konflikt, kan være et sandsynligt scenarie[6]. På den baggrund vil telesektoren i samarbejde med energisektoren undersøge effekten på teleforsyningen af et længerevarende strømudfald, og vurdere mulige initiativer, herunder muligheden for prioritering i strømforsyningen ved opstart efter nedbrud.

Initiativ 5: Undersøge mulighed for styrkelse af evnen til at imødegå cyberangreb
Som led i strategien etablerer branchen en DCIS til at styrke informationsdeling og koordination i forbindelse med hændelser i telesektoren, og udbyderne har selv et beredskab til at opdage og imødegå cyberangreb. De virksomhedskunder som telesektoren betjener i de øvrige kritiske sektorer skal hver især også have et beredskab til at opdage og imødegå cyberangreb, som i sagens natur transmitteres via teleforbindelserne. Samfundsmæssigt vil det være en gevinst, hvis udbyderne via monitorering efter angrebsmønstre og lignende kan forhindre, at visse typer af angreb videretransmitteres til virksomhedskunder i de kritiske sektorer. Denne type ydelse skal leveres på helt frivillig basis og være kommercielt funderet. På den baggrund vil telesektoren undersøge, om Center for Cybersikkerhed vil kunne stille viden og vejledning til rådighed for telesektoren- herunder angrebsindikatorer, således virksomheder i de kritiske sektorer kan nyde en særlig beskyttelse mod visse typer af angreb.

[6] https://fe-ddis.dk/cfcs/publikationer/Documents/Destruktive%20cyberangreb%20kan%20ramme%20danske%20virksomheder.pdf p.2

4 Etablering af DCIS

Det er i den nationale cyber- og informationssikkerhedsstrategi fastlagt, at der i de samfundskritiske sektorer - herunder telesektoren - skal oprettes decentrale cyber- og informations-sikkerhedsenheder (DCIS'er). En DCIS kan bidrage til gennemførelsen af sektorvise trusselsvurderinger, overvågning, beredskabsøvelser, sikkerhedsopbygning, vidensdeling, vejledning mv.

DCIS'ens primære opgave er at formidle, efterspørge, skabe og validere informationer om relevante informationssikkerhedsforhold mellem sektorens aktører og Center for Cybersikkerhed (CFCS), og vil dermed fungere som et udvekslingspunkt for informationssikkerhedsinformationer, både til de enkelte aktører fra CFCS og til CFCS fra aktørerne og andre DCIS'er/myndigheder.

Formålet er, at der kan ske en udveksling og behandling af informationer begge veje så simpelt og gnidningsløst som muligt. Det må forventes, at samarbejdet mellem aktørerne, DCIS'en og CFCS kommer til at gennemgå et udviklingsforløb over de kommende år, baseret på de erfaringer, der løbende opsamles og den stadig stigende modenhed i samarbejdet inden for sektorerne omkring cybersikkerhedsspørgsmål.

Initiativ 6. Etablering af DCIS

De væsentlige erhvervsmæssige udbydere nedsætter en selvstændig juridisk enhed til varetagelse af opgaven med at drive sektorens decentrale cyber- og informationsikkerhedsenhed (DCIS). DCIS for telesektoren etableres i 2018. Det er aftalt, at opbygning af funktionsevnen sker trinvist, således en midlertidig enhed varetager af de basale DCIS-opgaver indtil DCIS for telesektoren er fuldt funktionsdygtig medio 2019.

Ved etablering af DCIS for telesektoren lægger branchen afgørende vægt på, at DCIS etableres som en uafhængig enhed, og at der kan sikres fuld fortrolighed blandt de deltagende parter.

Risiko- og sårbarhedsvurderingen viser, at menneskelige fejl udgør en væsentlig risiko for infrastrukturen. Det skyldes bl.a., at komponenterne i telekommunikationsinfrastrukturen undergår konstante forandringer dels som følge af nye teknologier, men også som følge af tilpasninger og opgraderinger. På den baggrund, vil telesektoren via DCIS'en i egen sektor og med andre kritiske sektorer udveksle og dele f.eks. best practices i forbindelse med hændelser for at reducere sektoren samlede risici for driftsforstyrrelser som følge af menneskelige fejl og lign.

5 Håndtering af beredskabshændelser og øvelser

Teleinfrastrukturen udsættes dagligt for mindre hændelser, der håndteres rutinemæssigt hos udbyderne. Større hændelser sker heldigvis sjældent, men alle erhvervsmæssige udbydere er via eksisterende regulering forpligtet til at have et passende og risikobaseret beredskab til håndtering af større hændelser[7].

Det følger af eksisterende regulering, at væsentlige erhvervsmæssige udbydere har underretningspligt ved brud på informationssikkerheden[8], hvilket sikrer, at tilsynsmyndigheden bliver bekendt med væsentlige hændelser i sektoren.

Der er i eksisterende regulering krav om, at væsentlige erhvervsmæssige udbydere skal afholde interne beredskabsøvelser hver andet år og for, at tilsynsmyndigheden kan påbyde udbydere at deltage i nationale og internationale øvelser[9]. Ud over de interne beredskabsøvelser som gennemføres i dag, har telesektoren tidligere deltaget i den nationale krisestyringsøvelse KRISØV.

Initiativ 7: Styrket øvelsesaktivitet
Det er målet, at udbyderne og DCIS'en - efter invitation fra Center for Cybersikkerhed - også deltager i de internationale cyberøvelser: CyberEurope fra EU, Cyber Coalition og CMX fra NATO.

For at styrke og afprøve DCIS'ens funktionsevne og det konkrete samarbejde mellem udbydere og DCIS gennemfører udbyderne og DCIS i 2019 konkrete og passende øvelsesaktiviteter.

[7] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20567%20af%201.%20juni%202016%20om%20informationssikkerhed%20og%20beredskab%20i%20net%20og%20tjenester.pdf kapitel 5
[8] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20566%20af%201.%20juni%202016%20om%20oplysnings-%20og%20underretningspligter%20vedr%C3%B8rende%20net-%20og%20informationssikkerhed.pdf §7
[9] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20567%20af%201.%20juni%202016%20om%20informationssikkerhed%20og%20beredskab%20i%20net%20og%20tjenester.pdf §§ 35,36 dog således, at hændelser betragtes som en øvelse, når hændelse har et omfang der initierer fx krisestyring.

6 Samarbejde i telesektoren

Telesektoren samarbejder i dag omkring en række sikkerhedsrelaterede emner. Blandt andet har sektoren i en årrække drevet et forum til informationsdeling og kontakt mellem de teknikere, der forestår den praktiske hændelseshåndtering hos udbyderne. Center for Cybersikkerhed vil som sektoransvarlig myndighed endvidere udgive sektorspecifik rådgivning og vejledninger vedrørende telekommunikationsinfrastrukturen. Telesektoren vil via DCIS'en sikre, at kendskabet til Center for Cybersikkerheds rådgivningsydelser udbredes i telesektoren, og DCIS'en vil bistå Center for Cybersikkerhed med sparring i forbindelse med udarbejdelse af de sektorspecifikke vejledninger.

Der er et stigende behov for at videreuddannelse af medarbejderne i sektoren indenfor cyber- og informationssikkerhed og for at styrke det praktiske samarbejde yderligere.

På den baggrund vil telesektoren i strategiperioden:

Initiativ 8: Undersøge muligheden for afvikling af fælles kurser i telesektoren indenfor cyber- og informationssikkerhed
Der er en lang række udbydere af sikkerhedsrelevante kurser og certificeringer, som udbyderne hver især sender medarbejdere på - oftest i udlandet. Telesektoren vil undersøge, om det er muligt at få specifikke cybersikkerhedskurser til Danmark og afvikle kurser for telesektoren og telesektorens DCIS, således at medarbejderne i sektoren får lejlighed til at danne netværk og opbygge gensidig tillid, hvorved informationsdeling i forbindelse med hændelser bliver lettere at gennemføre.

Initiativ 9: Undersøge muligheden for etablering af incident response kapacitet i branchen, der kan bistå udbyderne ved omfattende hændelser
Hver af de væsentlige erhvervsmæssige udbydere har i dag eget beredskab til håndtering af konkrete hændelser. Der kan dog tænkes at opstå situationer, hvor en omfattende hændelse overstiger den enkelte udbyders beredskabskapacitet. På den baggrund vil telesektoren undersøge, om det er muligt på frivillig basis at etablere en incident response kapacitet, hvor medarbejdere fra andre udbydere kan bistå en berørt udbyder. En sådan incident response kapacitet vil naturligvis være efter "best effort" og ikke udgøre en forpligtigelse for den enkelte udbyder. Fordelen vil dog være, at der vil kunne være adgang til specialister, der har indgående kendskab til telesektoren og som lettere vil kunne indsættes til at imødegå en omfattende hændelse.

Sikkerhed omkring telesektorens medarbejdere

Det fremgår af tilsynsmyndighedens krav til telesektorens cyber- og informationssikkerhedsstrategi, at strategien skal indeholde overvejelser omkring sikkerhedsgodkendelse af personale og proces for sikring af lovmedholdelighed i ansættelseskontrakter og it-brugeraftaler. Det følger af eksisterende regulering, at væsentlige erhvervsmæssige

udbydere skal have sikkerhedsgodkendte medarbejdere[10]. Det følger endvidere af eksisterende regulering, at Center for Cybersikkerhed kan påbyde udbydere af væsentlige tjenester, at personale, der har adgang til kritiske netkomponenter, systemer og værktøjer er sikkerhedsgodkendt[11]. På den baggrund ses ikke et behov for yderligere initiativer på dette område.

[10] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20565%20af%201.%20juni%202016%20om%20sikkerhedsgodkendelse%20af%20medarbejdere%20p%C3%A5%20net-%20og%20informationssikkerhedsomr%C3%A5det.pdf
[11] https://fe-ddis.dk/cfcs/omos/Lovgivning/Documents/Bekendtg%C3%B8relse%20nr.%20567%20af%201.%20juni%202016%20om%20informationssikkerhed%20og%20beredskab%20i%20net%20og%20tjenester.pdf §26

7 Samarbejde med myndigheder og andre sektorer

Telesektoren er én blandt seks udpegede kritiske sektorer i den nationale cyber- og informationssikkerhedsstrategi som tilsammen bidrager til opretholdelse af samfundets kernefunktioner. Som følge heraf, er samarbejde mellem sektorerne og de relevante myndigheder afgørende for opretholde et robust og sikkert Danmark. Telesektoren vil via DCIS'en sikre, at informationsdelingen omkring best practices deles med andre sektorer.

Som de øvrige sektorer har telesektoren behov for cyber- og informationssikkerhedskompetencer. Frem for at sektorerne kæmper om de samme ressourcer, er der behov for, at mængden af generalister og specialister med cyber- og informationssikkerhedskompetencer øges. Telesektoren vil derfor:

Initiativ 10: Styrke samarbejdet med andre samfundskritiske sektorer i Danmark for at øge udbuddet af cyber- og informationssikkerhedskompetencer

Samarbejdet vil indledningsvist koncentrere sig om opbygning af kompetencer. Der er allerede i dag mangel på såvel specialister og generalister med de rette sikkerhedskompetencer. Denne mangel bliver kun større i takt med, at flere og flere sektorer øger fokus på cyber- og informationssikkerheden. Der er således behov for, at udbuddet øges. Telesektoren vil arbejde for at efter- og videreuddanne medarbejdere, samt samarbejde og videndele med de øvrige kritiske sektorer om dette. Herudover vil telesektoren sammen med de øvrige kritiske sektorer udarbejde anbefalinger til, hvordan regeringen kan prioritere flere uddannelsesmidler til uddannelse af cyber- og informationssikkerhedskompetencer på forskellige uddannelsesniveauer og inden for forskellige fagområder.

8 Klassificerede kommunikationsmidler

Sikker og hurtig kommunikation omkring hændelser er afgørende for at kunne reagere på mulige angrebsindikatorer. For nuværende har telesektoren alene mulighed for at udveksle ikke-klassificeret information elektronisk mellem DCIS'en, udbyderne og Center for Cybersikkerhed. Det anses for tilstrækkeligt i denne indledende fase. Der kan dog forudses et behov for på sigt, at få etableret egentlig klassificerede kommunikationskanaler. På den baggrund vil telesektoren:

Initiativ 11: Undersøge behovet for klassificerede kommunikationsmidler

Som led i strategien vil telesektoren undersøge behovet for etablering af klassificerede kommunikationsmidler. I første omgang mellem DCIS'en og Center for Cybersikkerhed og efterfølgende mellem DCIS'en og udbyderne.

9 Øget sikkerhed i Internet of Things

Robustheden i telenettet kan i de kommende år blive påvirket af den stadigt stigende tilslutning af IoT-enheder. Mange producenter tænker først og fremmest på funktionalitet ved udvikling af disse enheder, hvorfor IoT-enheder ofte er usikre og lette at angribe, når enhederne kommer på internettet. Det betyder, at IoT-enhederne eksempelvis indlemmes i såkaldte botnets, og anvendes til overbelastningsangreb (DDoS) af andre net- og tjenester på internettet.

Initiativ 12: Forbedret IoT-sikkerhed

Telesektoren vil undersøge muligheden for, at IoT-enheder der tilsluttes net i EU skal efterleve fælles minimumsstandarder for sikkerhed**.** Endvidere vil branchen undersøge muligheden for etablering af en fælles best practice i Danmark mellem udbydere, således at IoT-enheder som udbyderne selv sætter på offentligt tilgængelige net i Danmark telenet har et højt beskyttelsesniveau. Det skal i den forbindelse undersøges, om den kommende frivillige IKT-certificeringsordning[12] kan anvendes til at fremme IoT-sikkerheden. Som en mulig del af en fælles best practice i Danmark, skal det undersøges, om udbyderne kan etablere fælles rammer for håndtering af IoT-enheder på offentligt tilgængelige net.

Telesektoren undersøger endvidere muligheden for politisk stillingtagen til at fremme sikkerhedspraktisk indenfor IoT i EU.

[12] https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/