

> **Samarbejde mellem sektorerne:
DKCERT som vært for telesektorens Decentrale Cyber-
og Informationssikkerhedsenhed (DCIS).
Hvorfor gør vi det?**

DeiC Konferencen 31. oktober 2019

DKCERT – en del af DeiC

www.cert.dk/www.deic.dk

Henrik Larsen

Email: henrik.larsen@cert.dk/henrik.larsen@deic.dk

- > **Ny organisering af samfundets cyberberedskab
- ny opgave til DKCERT**

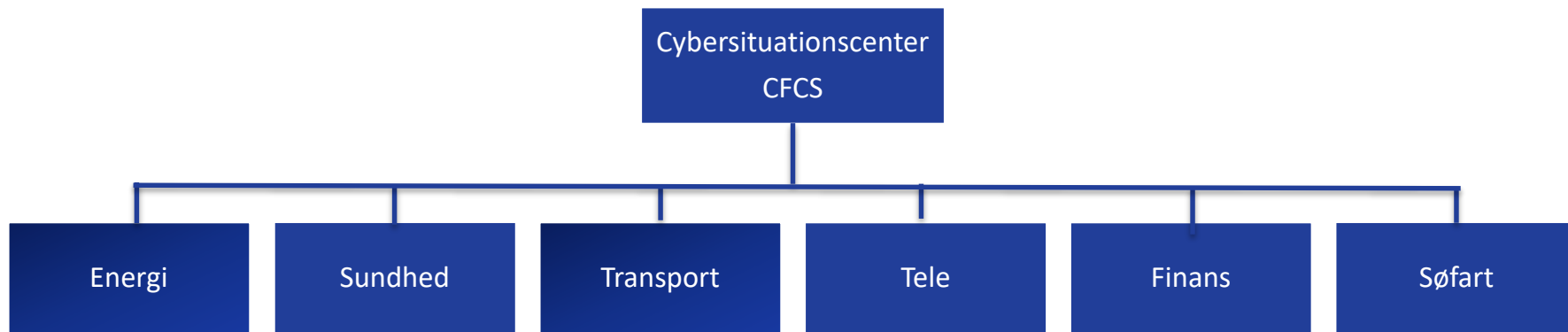


<https://www.fm.dk/publikationer/2018/national-strategi-for-cyber-og-informationssikkerhed>



<https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy>

- > **Sektorvise strategier og decentrale cyber- og informations-sikkerhedsenheder (DCIS) i seks samfundskritiske sektorer (initiativ 3.1)**



> DCIS (Decentral Cyber- og InformationsSikkerhedsenhed)

- > En DCIS bidrager 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)
- > DKCERT har indgået kontrakt med en nydannet forening af teleselskaber om at opstille TeleDCIS pr. 1. juni med 2 ÅV

- > **En “kommerciel DCIS” leveret af en offentlig enhed**
- > DKCERT leverer 'DCIS-as-a-Service' til en sammenslutning af 12 kommercielle telekommunikationsvirksomheder
- > Andre sektors DCIS er typisk del af en styrelse (regulerende myndighed) – finans er undtagelsen
- > CFCS har flere kasketter
- > DKCERT ses som et eksisterende, neutralt fagligt miljø

> **TeleDCIS**

- > TeleDCIS i regi af DKCERT er oprettet 1. juni med en konsulent som midlertidig bemanning
- > Leder af TeleDCIS er ansat pr. 1. august
- > En stilling som medarbejder i teamet er opslået nu
- > Afhængig af fremtidig arbejdsbelastning, senere udvidelse med et yderligere ÅV

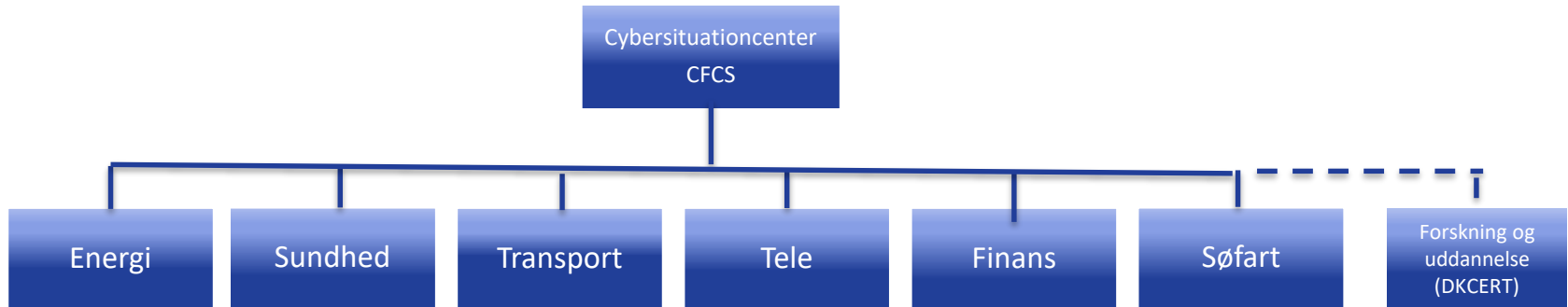
> **Lessons Identified**

- > At indsamle risiko- og sårbarhedsvurderinger fra ISPerne er ikke let
- > Et spørgsmål om at opbygge tillid og netværk
- > Opbygge relationer til de øvrige sektorer
- > Erfarne konsulenter har hjulpet processen på vej
- > Vigtigt at få brancheerfaren teamleder med ”diplomatisk gennemslagskraft”

- > **Hvorfor påtager vi os denne opgave?**
- > En fordel for institutionerne (universiteterne m.fl.)
- > Økonomisk attraktiv, dvs. flere ressourcer til teamet
- > Udbygget samarbejde med CFCS, dvs. adgang til klassificeret information osv.
- > Evnen til at håndtere cyber- og informationssikkerhedshændelser bygger på tillid og deling af viden og operationel information

- > **Forskning og uddannelse som “kritisk infrastruktur”?**
- > Foreslået af CFCS, at F & U-sektoren på frivillig basis kan betragtes på linje med nationens kritiske infrastruktur
- > DKCERT kunne påtage sig rollen som DCIS, hvis universiteterne accepterer at dele flere informationer med CFCS

- > **Cybersituationcenteret bliver gradvist opbygget i 2020, DCIS som sektor CERTs**
 - Foreslået udvidet samarbejde med forsknings- og uddannelsessektoren





Henrik Larsen
+45 9351 1100
henrik.larsen@cert.dk / henrik.larsen@deic.dk
www.cert.dk / www.deic.dk