Cyber- og Informationssikkerheds-strategi for telesektoren

12 initiativer til en sikrere teleforsyning i Danmark

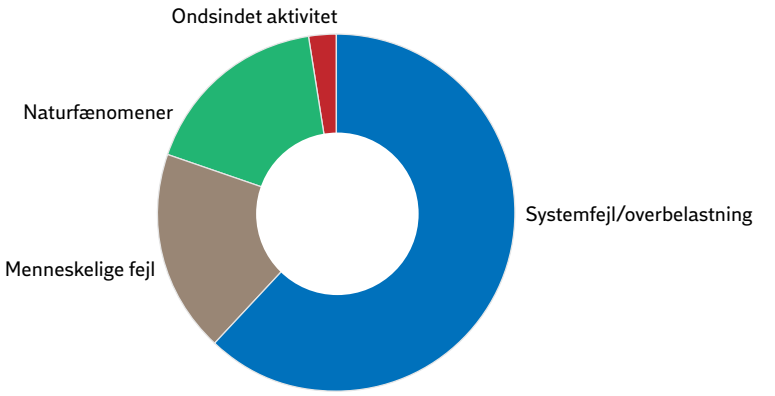
Hvorfor udarbejder telesektoren en Cyber- og Informationssikkerhedsstrategi?

Telesektoren er i regeringens strategi for cyber- og informationssikkerhed udpeget som en af de 6 samfundskritiske infrastrukturer for Danmark og skal derfor udarbejde en særlig cybersikkerhedsstrategi for sektoren. Modsat de 5 øvrige sektorer, udarbejdes del-strategien i telesektoren ikke alene af myndigheder, men fortrinsvist af sektoren selv. Med strategien er der skabt et grundlag for, at telesektoren kan stå sammen og tage ansvar for en samlet forbedret digital sikkerhed for Danmark.

Sikkerhedshændelser i telesektoren

Strategien er udarbejdet på baggrund af en aktuel risiko- og sårbarheds-vurdering af den danske telesektor med fokus på konsekvenserne af hændelser i telesektoren for samfundet – ikke for det enkelte selskab.

Oversigt over betydende sikkerhedshændelser i den europæiske telesektor



Kilde: ENISA; Annual Report Telecom Security Incidents 2017

Hvad gør strategien?

Det mest omfattende initiativ er oprettelse af en såkaldt decentral cyber- og informations-sikkerhedsenhed (DCIS). DCIS'ens primære opgave at være et bindeled mellem teleselskaberne og Center for Cybersikkerhed (CFCS), og vil dermed fungere som et udvekslingspunkt for informationssikkerhedsinformationer i telesektoren og til andre samfundskritiske sektorer og myndigheder.

STRATEGIENS 12 INITIATIVER

- Styrket indsats mod angreb fra insidere
- Styrket underleverandørstyring
- Undersøge muligheden for sikring mod fysisk sabotage i forbindelse med kriser og lignende
- Styrkelse af samarbejdet mellem el- og telesektoren
- Undersøge mulighed for styrkelse af evnen til at imødegå cyberangreb
- Etablering af DCIS
- Styrket øvelsesaktivitet
- Undersøge muligheden for afvikling af fælles kurser i telesektoren indenfor cyber- og informationssikkerhed
- Undersøge muligheden for etablering af incident response kapacitet i branchen, der kan bistå udbyderne ved omfattende hændelser
- Styrke samarbejdet med andre samfundskritiske sektorer i Danmark for at øge udbuddet af cyber- og informationssikkerheds-kompetencer
- Undersøge behovet for klassificerede kommunikationsmidler
- Forbedret IoT-sikkerhed

Digital · DANSK ENERGI · TELE INDUSTRIEN · IT-Branchen · DANSK ERHVERV