Implementering af NIS-direktivet – IXP

Teknisk gennemgang

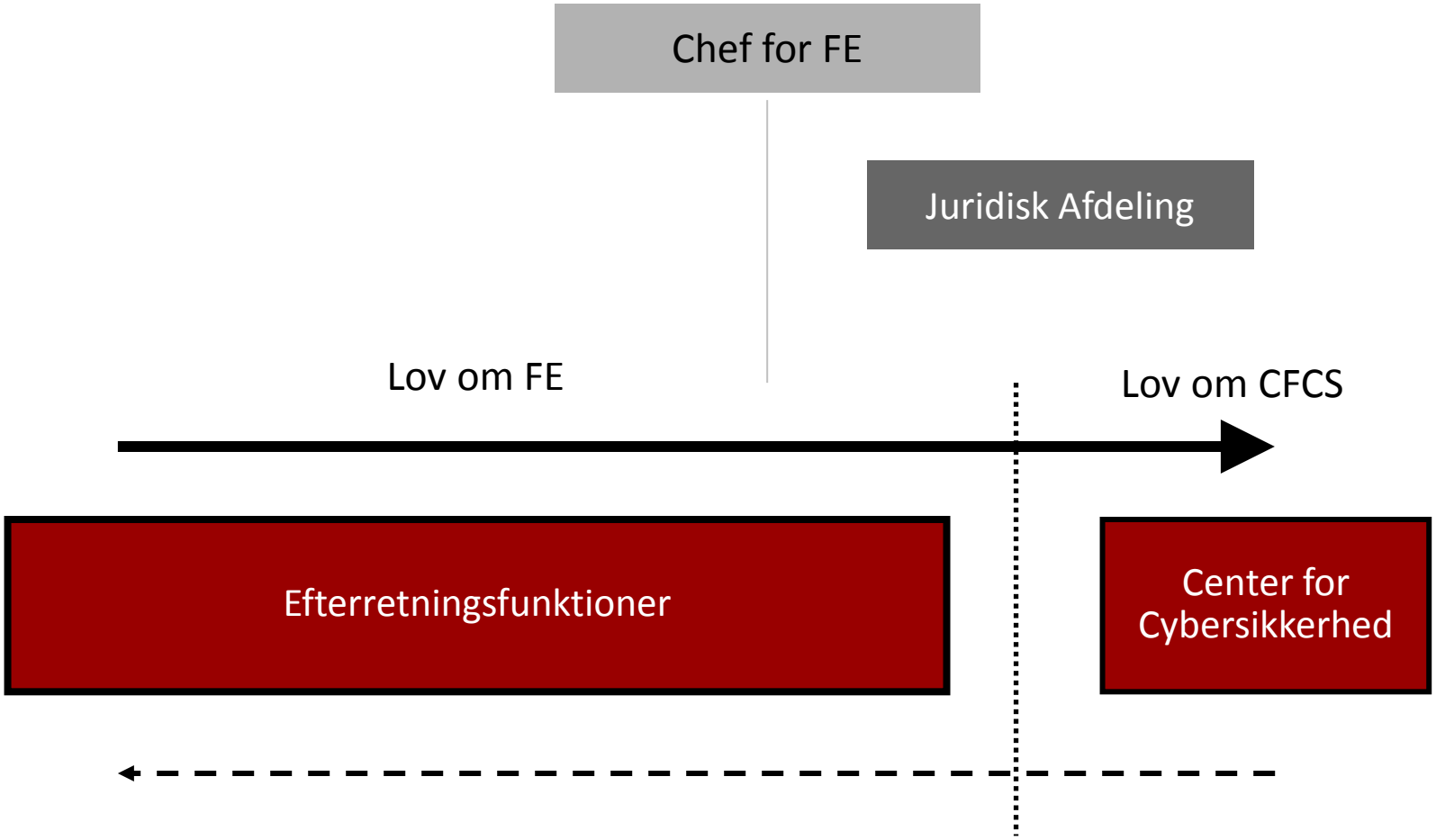
Chef for Center for Cybersikkerhed, FE
Thomas Lund-Sørensen

CENTER FOR CYBERSIKKERHED

Forsvarsministeriets ressort: NIS-direktivets regulering af internet-udvekslingspunkter (IXP'ere) og Center for Cybersikkerheds rolle

- Center for Cybersikkerhed i Forsvarets Efterretningstjeneste
  - Lovgrundlag og arbejdsform
  - Begrundelser for organisatorisk placering
- Center for Cybersikkerheds rolle i NIS-direktivet
  - Nationalt centralt kontaktpunkt
  - CSIRT
  - IXP-ansvarlig it-sikkerhedsmyndighed
- Behandling af oplysninger som følge af NIS-direktivet

Lovgrundlag og udveksling af oplysninger



FE er Danmarks udenrigsefterretningstjeneste med fokus på trusler fra udlandet.

- Cybertruslerne kommer fra udlandet
- FE har opbygget særlig viden og kompetencer om cybersikkerhed
- FE alene har adgang til klassificerede oplysninger fra udenlandske partnere
- FE har mangeårig erfaring som it-sikkerhedsmyndighed i Forsvaret
- FE har særlig systemunderstøttelse til håndtering af sensitive oplysninger
- Særlige it-sikkerhedskompetencer samlet på ét sted giver kritisk masse
- Netsikkerhedstjenesten dækker både civile og forsvarets myndigheder – forhindrer dublering af kapacitet og sikrer optimal udnyttelse af knappe ressourcer
- Tilsynet med Efterretningstjenesterne fører tilsyn med både CFCS-loven, FE-loven og Forsvarsministeriets retningslinjer. CFCS' behandling af personoplysninger, som modtages i medfør af reglerne i NIS-direktivet, vil også være omfattet af tilsynets kompetence.

Sektoransvarsprincippet er grundlaget for gennemførelsen af NIS-direktivets bestemmelser

Center for Cybersikkerheds rolle i NIS-direktivets gennemførelse

- Generelt:
  - Nationalt centralt kontaktpunkt for koordination mellem sektorer og EU (24/7/365 – internationalt partnersamarbejde)
  - CSIRT for koordination af hændelse (CFCS er dansk CERT)
- For IXP'erne:
  - Fastsætte minimumsregler for it-sikkerhed
  - Påbyde inddragelse af trusler i processer
  - Føre tilsyn
  - Evt. forestå offentliggørelse af hændelser

CENTER FOR CYBERSIKKERHED

Hver sektoransvarlig myndighed fastsætter egne krav til underretningers indhold om væsentlige hændelser

Center for Cybersikkerhed modtager underretning som nationalt centralt kontaktpunkt og som CSIRT.

- For IXP'ere:
  - Virksomhed og kontaktoplysninger vedr. underretningen?
  - Beskrivelse af hændelsen og konsekvenser af hændelsen?
  - Hændelsens betydning for tjenester i andre EU-lande?
  - Tiltag der er iværksat og tjenester reetableret?
  - Berørte brugere informeret og hvorledes?
  - Andre oplysninger af betydning?
  - Udfærdiget af og udfærdigelsestidspunkt?

Center for Cybersikkerheds udkast til underretningsskema for væsentlige hændelser hos IXP'ere:

1. Virksomhed og kontaktoplysninger vedrørende denne underretning
2. Tidspunkt for og varighed af hændelsen
3. Beskrivelse af hændelsen
4. Beskrivelse af konsekvenserne af hændelsen
5. Vurderes hændelsen at have væsentlige konsekvenser for tjenester i andre EU- eller EØS-lande?
6. Hvilke tiltag er der blevet iværksat?
7. Er de berørte tjenester blevet reetableret? Hvis nej, hvornår forventes dette at ske?
8. Er de berørte brugere (evt. andre) blevet informeret og hvordan?
9. Andre oplysninger af betydning
10. Udfærdiget af og udfærdigelsestidspunkt