Uddannelses- og Forskningsministeriet

Fremtidens sektor

DeiC-konference d. 3. november 2021

Chefkonsulent Gunvor Faber-Madsen
Uddannelses- og Forskningsstyrelsen

Dagsorden

1. National strategi for cyber og informationssikkerhed (2018-2021 + 2022-2024).

2. Uddannelses- og Forskningsstyrelsens myndighedsrolle – tilsyn med universiteternes arbejde med informationssikkerhed

3. Tid til spørgsmål

1. National strategi for cyber- og informationssikkerhed

Ny strategi 2022-2024 - 1

- Udgangspunkt
  - Samfund med høj grad af digitalisering
  - Trusselsbillede
  - Nuværende strategi 2018-2021:
    - 6 samfundskritiske sektorer: sundhed, energi, tele, finans, transport og søfart.
    - sektorstrategi
    - decentral cyber- og informationssikkerhedsenhed (DCIS).
  - 25 initiativer inden for 3 pejlemærker:
    - tryg hverdag
    - kompetencer
    - fælles indsats.

Ny strategi 2022-2024 - 2

- Fokus:
  - udvide i bredden:
    - yderligere sektorer udvikler sektorstrategier og etablerer en decentral cyber- og informationssikkerhedsenhed.
  - udvide i dybden:
    - Øge ambitionsniveau ift. nuværende krav inden for den enkelte sektor og tværgående indsatser.
  - 4 hovedtemaer:
    1. Ledelsesforankring og kompetenceopbygning
    2. Robust og modstandsdygtig (samfund og systemer)
    3. Samarbejde og organisering
    4. International indsats og bidrag

Ny strategi 2022-2024 - 3

- Hvor står universiteterne og ministeriet?

- Udvidelse?

- Kompetenceopbygning

2. Uddannelses- og Forskningsstyrelsens myndighedsrolle – tilsyn med universiteternes arbejde med informationssikkerhed

Myndighed og universiteter

- Rigsrevisionens beretning 08/2018 om universiteternes beskyttelse af forskningsdata:
  - *De 5 store universiteter beskytter ikke forskningsdata i tilstrækkelig grad mod ukendt it-udstyr.*
  - *Konsekvensen kan være, at fremmede aktører relativt let får uautoriseret adgang til forskningsdata på universiteterne.*
  - *Dette finder Rigsrevisionen ikke tilfredsstillende.*

- Myndighedsopgave: sektortilsyn/ulovbestemt tilsyn

- Åbenhed - sårbarhed

Fra vejledning til tilsyn og dialog

- Implementering af ISO27001-standarden fra hvert universitet.
- Opdateret tværgående trussels- og risikovurdering for hele universitetssektoren.
- Få identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.

Status

- ISO-27001
  - 2019/2021 √

- Trusselsbillede og risikovurdering.
  - 2020 √ / 2021 netop opdateret

- Sikkerhedsmæssige tiltag:
  - administratorrettigheder
  - opkobling af ukendt it-udstyr
  - installation af software
  - centralt ansvar for informationssikkerhed.
  - 2020 √ / 2021 netop opdateret

- Rigsrevisionens 3-årsopfølgning

Hvad nu?

1. Strategi er på trapperne.
2. Trusselsbillede: fortsat mere fokus på både universiteternes og ministeriets arbejde med cyber- og informationssikkerhed.
3. Stigende efterspørgsel efter kompetencer
4. Behov for fortsat styrket dialog.

3. Tid til spørgsmål