Sikkerhedsstandarden ISO 27001, udbredelse samt relevant anvendelse

Høring om tekniske tiltag til sikring af følsomme personoplysninger

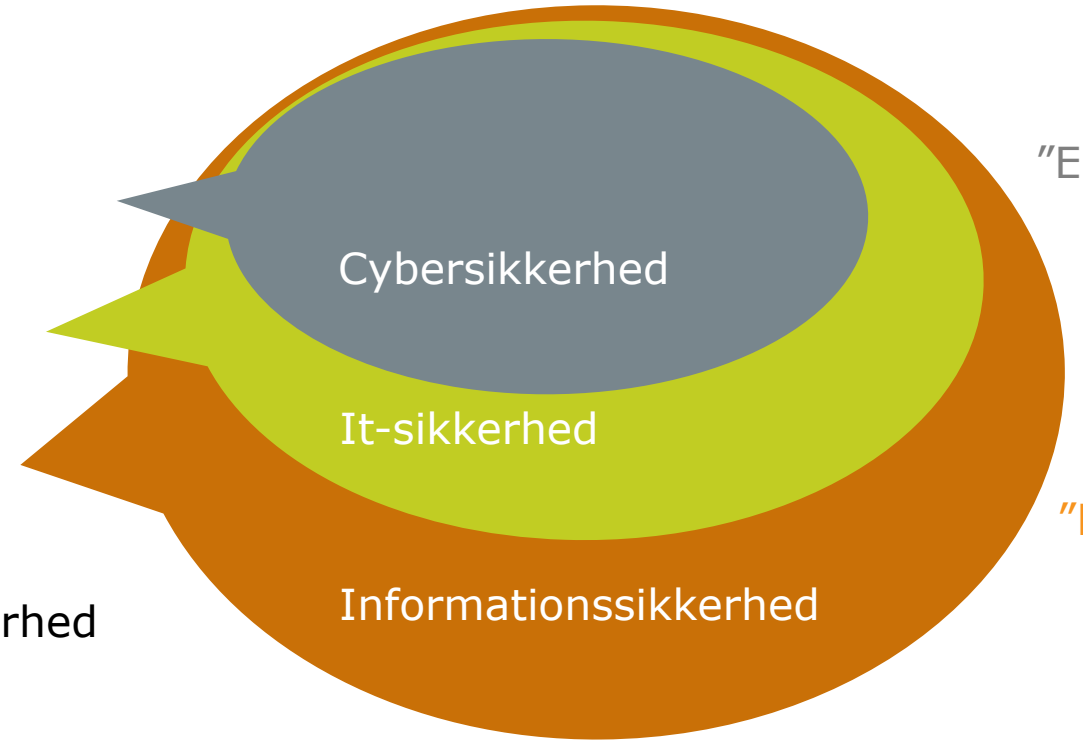
12. november 2014

Niels Madelung, Chefkonsulent
nm@ds.dk - 41218304

DANSK STANDARD

#sikkerhed

Internet
Infrastruktur
+
Teknologi
Databaser
+
Strukturer
Processer
=
Informationssikkerhed



”Energinet.dk”

”Statens Serum”

”Nets/Se & Hør”

ISO/IEC 27001
Ledelsesstandard for Informationssikkerhed

Et ledelsesværktøj til systematisk at opretholde relevant informationssikkerhed, med udgangspunkt i forretningskritiske risici.

DANSK STANDARD

ISO/IEC 27001
Ledelsesstandard for Informationssikkerhed

§ Uafhængig af informationsform (internet, it, nedskrevet, talt etc.).

§ Interessentorienteret (lovgivning, kunder etc.).

§ Harmoni med organisationens størrelse og type.

§ Risikobaseret (reduktion af konsekvens og sandsynlighed).

§ Integreret i organisationens arbejdsrutiner og processer samt partnere.

§ Struktureret og verificerbart (rigsrevisionen, datatilsynet, certificeringsorgan).

§ Kontinuerlig proces.

§ Internationalt anerkendt.

Certificerede organisationer på verdensplan

Opgørelse baseret på frivillig indberetning:

- 25.000 certificerede organisationer
- Antal certificerede organisationer stiger med 15 % årligt.
  - (Gennemsnitlig stigning for tilsvarende ledelsesstandarder er 4 %)
- Europas andel steget fra 18,4 % i 2006 til 35,7 % i 2013.
- Landerepræsentation vokset fra 64 i 2006 til 105 i 2013.
  - (I Europa fra 30 til 44)

Certificerede organisationer i Danmark

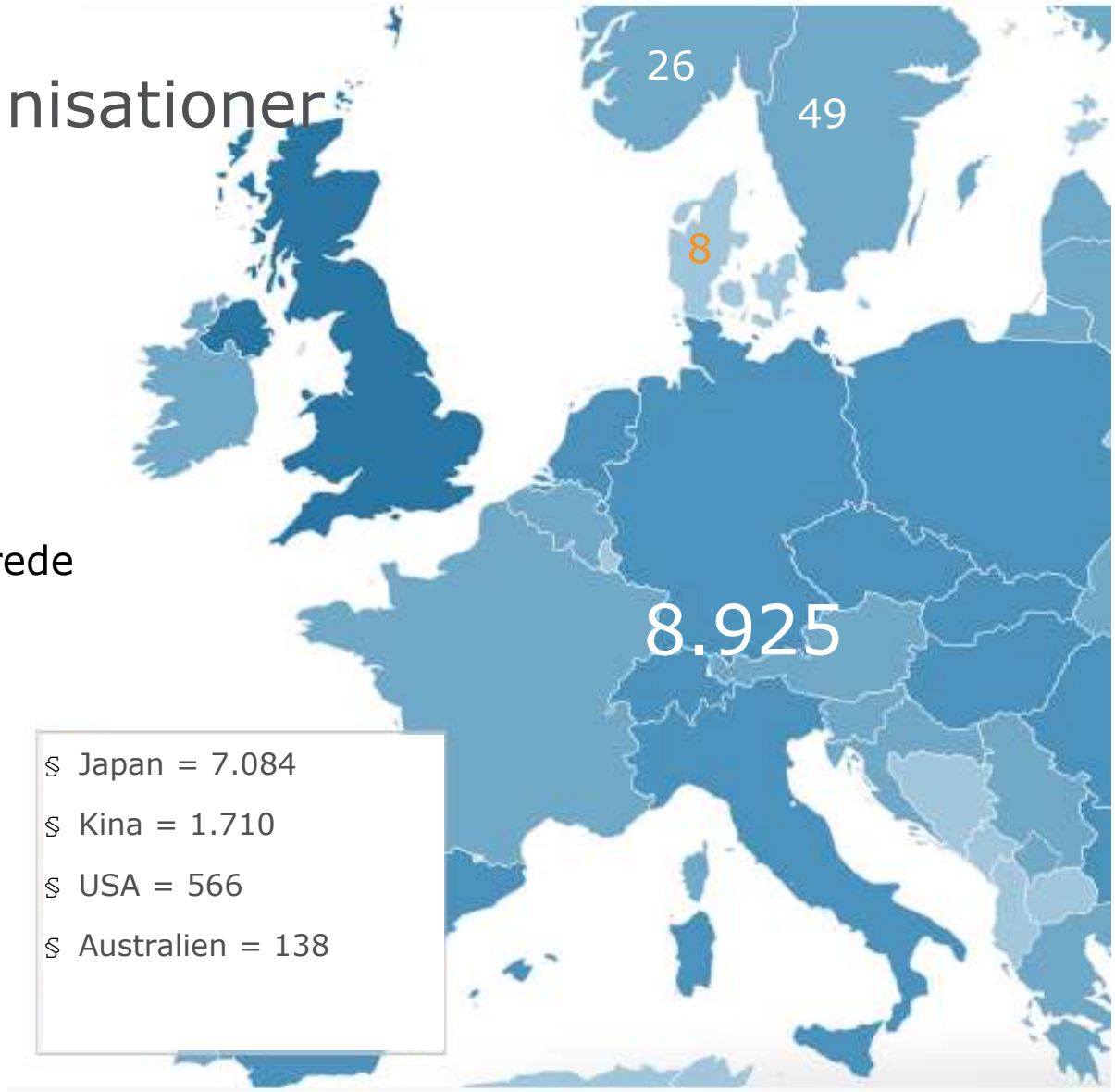
- 8-12 certificerede organisationer
  - KMD 3.000 ansatte, leverandør af bl.a. omsorgssystemer til kommuner
  - AuditData 48 ansatte, leverandør (eksport) af audiologiske patientsystemer

- Anskaffelse af standarden fordobles:
  - 2012: 48 organisationer
  - 2013: 100 organisationer
  - 2014: 219 organisationer
    - I alt siden 2007: ~600 organisationer

- Skønnes efterlevet 99 % af +130 danske organisationer, uden at disse er certificeret.

Certificerede organisationer

Sammenlignet med Sverige burde der være 23 certificerede organisationer i Danmark.



- Japan = 7.084
- Kina = 1.710
- USA = 566
- Australien = 138

ISO/IEC 27001 – løsningen der favner udfordringen

- Mest udbredt og anerkendt løsning internationalt
- Støttes af DI, Forbrugerrådet, Institut for menneskerettigheder og Dansk IT i de afgivne høringssvar
- Inspiration til politisk beslutning:
  - Alle private og offentlig organisationer som opbevarer personhenførbare oplysninger (ud over egne ansatte) samt forsyningsvirksomheder skal:
    - Overholde ISO/IEC 27001*)
    - Certificeres af uvillig part
    - Indberette lækage og nær-ved-hændelser til central myndighed
      - Læring skal indsamles og anvendes til vedvarende forbedringer

*) Statens institutioner har skulle efterleve ISO/IEC 27001 siden 2014.

Spørgsmål?

DANSK STANDARD