10.15-11.00: NIS2 og ny cybersikkerhedsstrategi v. Søren Bank Greenfield, DCIS Sund

- Status på NIS2
- Robusthed og resiliens i sundhedssektoren
- Cybersikkerhedsstrategien og EU-actionplan

SUNDHEDSDATA-
STYRELSEN

SDN Temadag

Søren Bank Greenfield

23 okt. 2025

Søren Bank Greenfield

Chef for

C yber- og

I nformationssikkerheds

A fdeling

- Faglig baggrund som operationel sikkerhedschef, CISO og med viden indenfor brugervendt infrastruktur, identitetsstyring og cybersikkerhed.
- Har før været i KBH amt, Glostrup hospital og RegionH (CIMT).
- Vildt dårlig humor ☺

https://sundhedsdatastyrelsen.dk/Media/638641645405294664/strategi_cyber_informationssikkerhed_2023_2025.pdf

Agenda

1. NIS2
   - Hvad er baggrunden for NIS?
   - Hvem er omfattet?
   - Hvem fører tilsyn?
   - Hvad betyder det for en omfattet enhed?
   - Hvad er status?
2. NY NCIS, CER, ”EU action plan on the cybersecurity of hospitals and healthcare providers”
3. Robusthedsarbejde

Dette oplæg afholdes under ”Chatham house rules”

> When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

https://www.chathamhouse.org/about-us/chatham-house-rule

NIS2

SUNDHEDSDATA-
STYRELSEN

Baggrund for NIS

Bygger videre på NIS1 direktivet fra 2016

Det er et direktiv fra EU fra 2022

- Implementeret ved lov som blev vedtaget den 26. april 2025
- **Trådte i kraft den 1. juli 2025 i DK**

Formål

- At sikre et højt cybersikkerhedsniveau på tværs af medlemslandene
- At gøre samfundet mere robust

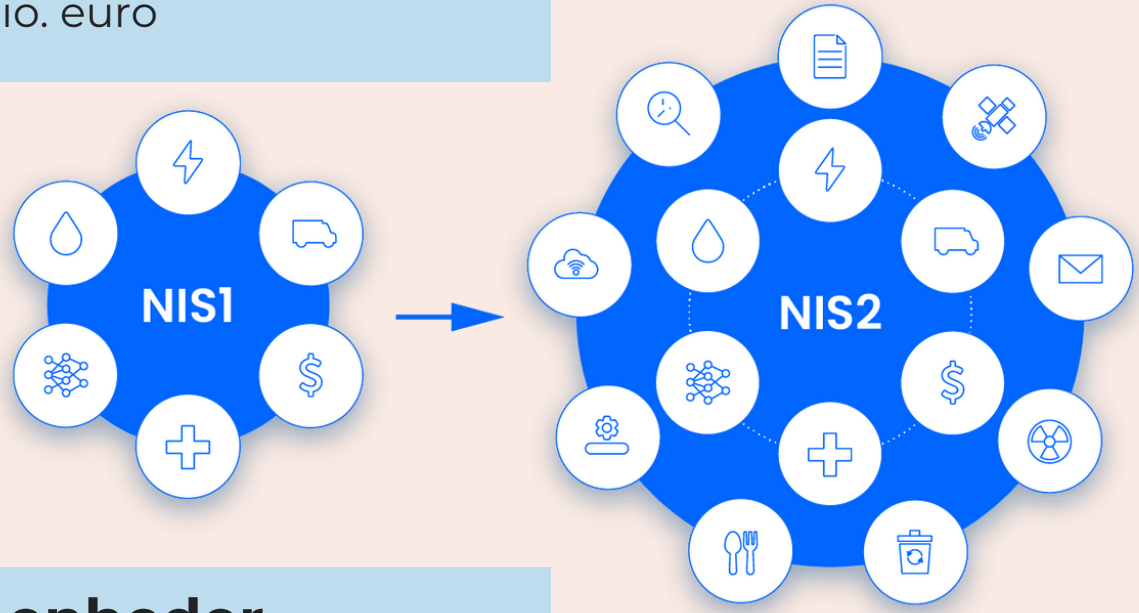
Hedder i dansk lov:
Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2 loven)

Hvad er nyt?

- Udvider anvendelsesområde
  - Nye kritiske sektorer
  - Fra 7 til 17 kritiske sektorer
- Fastlægger nye rammer
  - Indfører minimumsikkerheds-foranstaltninger og ledelsesansvar
  - Indfører skærpede krav om hændelsesrapportering
  - Bødestraf for private
    - Ikke offentlige myndigheder

Væsentlige enheder

- Enheder der beskæftiger 250 personer eller derover
- Enheder med årlig omsætning på 50 mio. euro



Vigtige enheder

- Enheder der beskæftiger 50 personer eller derover
- Enheder der har en årlig omsætning på over 10 mio. euro

Hvem er omfattet i øvrigt?

Væsentlige enheder

- Den centrale forvaltning
- Regioner og kommuner
- Enheder omfattet af CER
- Enheder omfattet af NIS1

Vigtige enheder

- Enheder udpeget som vigtig af tilsynsmyndighed

Eksempler for sundhedsområdet

Kategori	> 250 ansatte	50-250 ansatte	< 50 ansatte
Sundhedstjenesteydere	**Regioner (Hospitaler), Kommuner og andre "aktører i sundhedsvæsenet, der yder sundhed"**	**Privathospitaler, fertilitetsklinikker, store sundheds- og lægehuse, ambulancetjenester**	
EU reference laboratorier	Udpegede EU-reference laboratorier	Udpegede eu-reference laboratorier	
Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler	Medicinalproducenter	Forskningsenheder	
Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater	Medicinalproducenter	Medicinalproducenter; produktion af råvarer, som anvendes i lægemidler	
Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation	Medicoproducenter	Medicoproducenter, mundbinds eller håndsprits producenter	
Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	Medicoproducenter, dentale instrumenter	Medicoproducenter, dentale instrumenter	

Hvad betyder det så for en omfattet enhed (SDS)?

SUNDHEDSDATA-
STYRELSEN

Så hvad skal man gøre?

0. Lav en ”omfattelsesvurdering” med begrundelse for hvilken sektorer man er omfattet af

Registrer organisation på Virk.dk (inden 1. oktober 2025)
Det kan dog nås endnu ☺

1. Konsekvensvurder processer i forhold til ”det man er omfattet på baggrund af” (er det NIS2 tjenester eller aktiviteter?)

2. For ”NIS2 tjenester eller aktiviteter”
– Risikovurdér underliggende NIS infrastruktur ift. autenticitet (+FIT)

3. For NIS2 infrastruktur
– implementér passende foranstaltninger

4. For NIS tjenester og aktiviteter””
– ledelsesrapporter og ansvarstagen for foranstaltninger

8. Cyberspecifikt uddannelse af Ledelse (og medarbejdere)

Certificér i ISO27001?

Fast få NIS2 specifikt revisions erklæringer fra leverandører?

7. Udarbejd proces for og udfør tilsyn med leverandører i ”første led”

6. Lav aftaler med alle leverandører omkring hændelseshåndtering, rapportering og tilsyn

Beslut:
Hvem skal indmelde hændelserne på virk.dk?

5. Udarbejd proces og skaf bemanding for hændelseshåndtering og rapportering:

- Tidlig advarsel **inden for 24 timer.**
- Indberetning om hændelsen **senest efter 72 timer.**
- En endelig rapport senest **én måned med RCA.**

Bemærk: Indmelding for ”de NIS systemer der ***kan*** påvirke enhedens evne til at ***levere*** de ydelser, som gør, at enheden er **omfattet af** NIS2-loven”.

Status på NIS2

- Er trådt i kraft 1. juli og alle skal indmelde hændelser (24/72/1 måned)
- Alle skal have indmeldt sig 1. okt. 2025.
- Myndighederne er ved at gennemgå listerne og ”minder” virksomhederne om det.
- Myndigheder laver vurderinger om der mangler nogen.
- 25 april melder myndigheder til EU – hvem er omfattet i hvert land.

- Hvis man er offentlig myndighed – så er man omfattet der ”først” og så fører SAMSIK tilsyn (herunder kommunerne)
- Undtagen regionerne, der er så meget sundhed at det er SDS der fører tilsyn ☺ (både på offentlig myndighed og sundhed)
- SDS fører tilsyn med SAMSIK

NY NCIS, CER, ”EU Action plan for healthcare”

SUNDHEDSDATA-
STYRELSEN

Hvordan hænger det hele sammen?

CER ”Critical Entities Resilience Directive”

CER-loven implementerer EU’s direktiv om kritiske enheders fysiske modstandsdygtighed.

Loven omfatter enheder i 11 samfundsvigtige sektorer, herunder bl.a. energi-, transport-, fødevare- og sundhedssektoren og pålægger dem at beskytte sig mod en bred vifte af trusler og hændelser.

Formålet med loven er at sikre, at samfundsvigtige funktioner kan opretholdes i bedst muligt omfang – også ved alvorlige hændelser som naturkatastrofer, terror eller tekniske sammenbrud.

https://samsik.dk/tre-nye-love-traeder-i-kraft-nis-2-cer-tele/

NIS2

Formålet med EU’s Net- og Informationssikkerhedsdirektiv (NIS 2) er at yderligere styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder indenfor en lang række sektorer samt for offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet.

https://samsik.dk/nis2/

Ny National cybersikkerhedsstrategi

Strategi for ”det der ikke er omfattet af NIS2”

- Borgere
- Ikke NIS2 sektor enheder
- Samfundsberedskab
- Samarbejde mellem sektorer, NIS, Politi, SAMSIK mv.

https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

Eu actionplan

European Commission

Cybersecurity of hospitals and healthcare providers

January 2025

#DigitalEU #HealthUnion

Digitalisation of health services brings many benefits to patients, including electronic health records, telemedicine, and AI-driven diagnostics. However, **healthcare is one of the most targeted sectors by cyber and ransomware attacks.**

To better protect its healthcare systems and create a safer environment for patients, the EU is launching a **European action plan on the cybersecurity of hospitals and healthcare providers.**

The action plan is based on **4 priorities:**

PREVENT
Strengthen the sector's capacities to prevent cybersecurity incidents.

DETECT
Equip the sector with better detection tools.

RESPOND AND RECOVER
Improve response and recovery to minimise the impact on patient care.

DETER
Deter cyber threat actors from attacking European healthcare systems.

2025

Q1
- Launch **stakeholder consultations**.
- Set up a joint **Health Cybersecurity Advisory Board**.
- Explore options to give support to health sector for **preparedness testing**.
- Develop a **regulatory mapping tool** to help minimise the administrative burden.

Q2
- Begin work to establish a **European Cybersecurity Support Centre** for hospitals and healthcare providers.
- Call on cybersecurity stakeholders to **pledge actions** to address the challenges.

Q3
- Develop **guidance on most critical cybersecurity practices**.
- Create a framework for cybersecurity maturity assessments.
- Set up new procurement guidelines for cybersecurity in healthcare.
- Offer **guidance to help healthcare providers avoid paying ransoms**.

Q4
- Include a **Rapid Response Service** for the healthcare sector in the EU Cybersecurity Reserve.
- Build up a **European known exploited vulnerabilities** catalogue for medical devices, EHRs and ICT providers.
- **Identify key ransomware strains targeting healthcare**.
- Adopt **recommendations to further refine the Action Plan**.
- Launch pilot projects to develop **best practices for cyber hygiene** and security risk assessment.

2025-2026
- Carry out an **annual Health Cyber Maturity Assessment**.
- Create Cybersecurity **Voucher programmes** providing financial assistance to implement cybersecurity measures.
- Boost international cooperation against ransomware actors, notably through the **International Counter Ransomware Initiative** and the **G7** Cybersecurity Working Group.

2026
- Design **training modules and courses** for healthcare professionals.
- Create an **EU-wide early warning subscription service** and a **ransomware recovery subscription service for the health sector**.

https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

Robusthedsarbejde

SUNDHEDSDATA-
STYRELSEN

Hvordan hænger det hele sammen?

Robusthedsarbejde på baggrund af trusselsvurdering og udvikling (SAMSIK + forsvaret)

Alle ministerier analyserer:
- Deres egne sårbarhed
- Potentielle robusthedstiltag

Alle ministerier med sektoransvar analyserer også:
- Sektorens kritiske sårbarheder
- Sektorens potentielle robusthedstiltag

Sundhedssektorens robusthed (ansvar SST)

Overordnet ansvar og specifikt fokus på:

- Akut- og sundhedsberedskabet
- Strukturelle, systemiske eller kritiske sårbarheder hos stat, regioner, kommuner og andre væsentlige enheder
- Sektorens potentielle robusthedstiltag der kan mitigerer for sårbarhederne

Cyber, digitalisering, tele- og IT (SDS)

Specifikt fokus på:

- ”Digitale” kritiske sårbarheder hos stat, regioner, kommuner og andre væsentlige enheder
- Del input til sektorens potentielle robusthedstiltag der kan mitigerer for sårbarhederne

Enheders robusthed

Specifikt fokus på:

- Egne kritiske sårbarheder, herunder både fysiske, sundheds, beredskab, robusthed, cyber, digitale, tele eller IT.
- Egne robusthedstiltag der kan mitigerer for sårbarhederne

Spørgsmål

SUNDHEDSDATA-
STYRELSEN

Krølle: Sundhedstjenesteydere

- »**Sundhedstjenesteyder**« : en fysisk eller juridisk person eller anden enhed, der lovligt leverer sundhedsydelser på en medlemsstats område
- »**Sundhedsydelser**« : sundhedsydelser, der leveres af **sundhedsprofessionelle** til patienter for at vurdere, bevare eller genetablere deres sundhedstilstand, **herunder ordinering, udlevering og levering af lægemidler** og medicinsk udstyr
- »**Sundhedsprofessionel**« : en læge, en sygeplejerske med ansvar for den almene sundheds- og sygepleje, en tandlæge, en jordemoder eller en **farmaceut** som defineret i direktiv 2005/36/EF eller en anden, der udøver en form for erhvervsmæssig virksomhed i sundhedssektoren, der er begrænset til et **lovreguleret erhverv**, jf. artikel 3, stk. 1, litra a), i direktiv 2005/36/EF, eller en person, der anses for at være en **sundhedsprofessionel i henhold til behandlingsmedlemsstatens lovgivning**