Beskriv forslaget:

EU-direktivet for Netværk- og InformationsSikkerhedstjenester (NIS) er blevet opdateret til en version 2 (NIS2). Lovarbejdet er ikke nået at blive færdigt til tiden, så det træder ikke i kraft som planlagt til oktober 2024. NIS2 betyder dog ændringer for en del organisationer i sundhedssektoren.

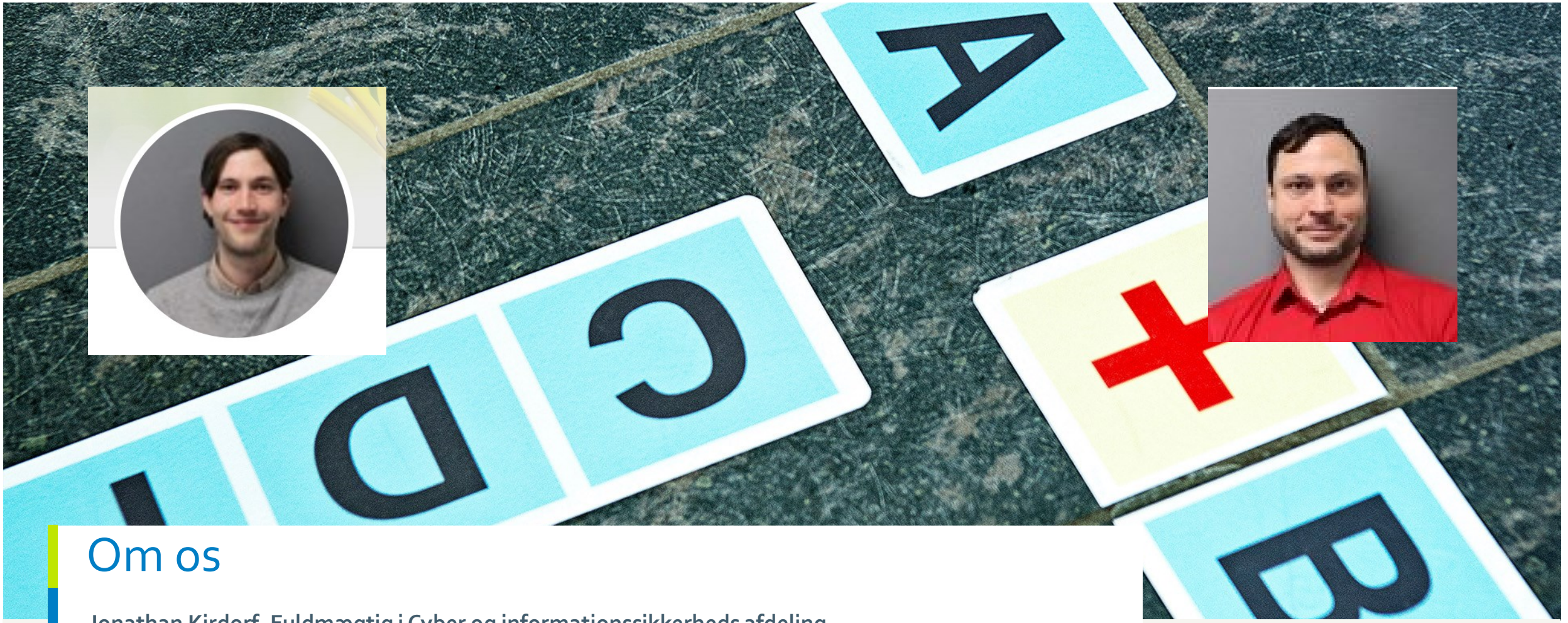
Sundhedsdatastyrelsen er den kompetente myndighed for NIS i sundhedssektoren, og oplægget vil give de nyeste informationer om:

- Hvad er status lige nu?
- Hvad ligger fast?
- Hvem bliver omfattet?
- Hvad kommer der af nye krav?
- Hvem bliver tilsynsmyndighed?
- Hvordan har Sundhedsdatastyrelsen selv implementeret direktivet i sit arbejde?

NIS2 oplæg - E-sundhedsobservatoriet

17 min

SUNDHEDSDATA-
STYRELSEN



Om os

Jonathan Kirdorf, Fuldmægtig i Cyber og informationssikkerheds afdeling

- Udførende på NIS 1 tilsyn i sundhedssektoren og deltagende i NIS2 proces og lovarbejde

Søren Bank Greenfield, chef for Cyber- og Informationssikkerheds afdeling

- 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).

SUNDHEDSDATA-
STYRELSEN

Forbehold for at alt endnu kan ændre sig ☺!

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

NIS2 og alt det der!

SUNDHEDSDATA-
STYRELSEN

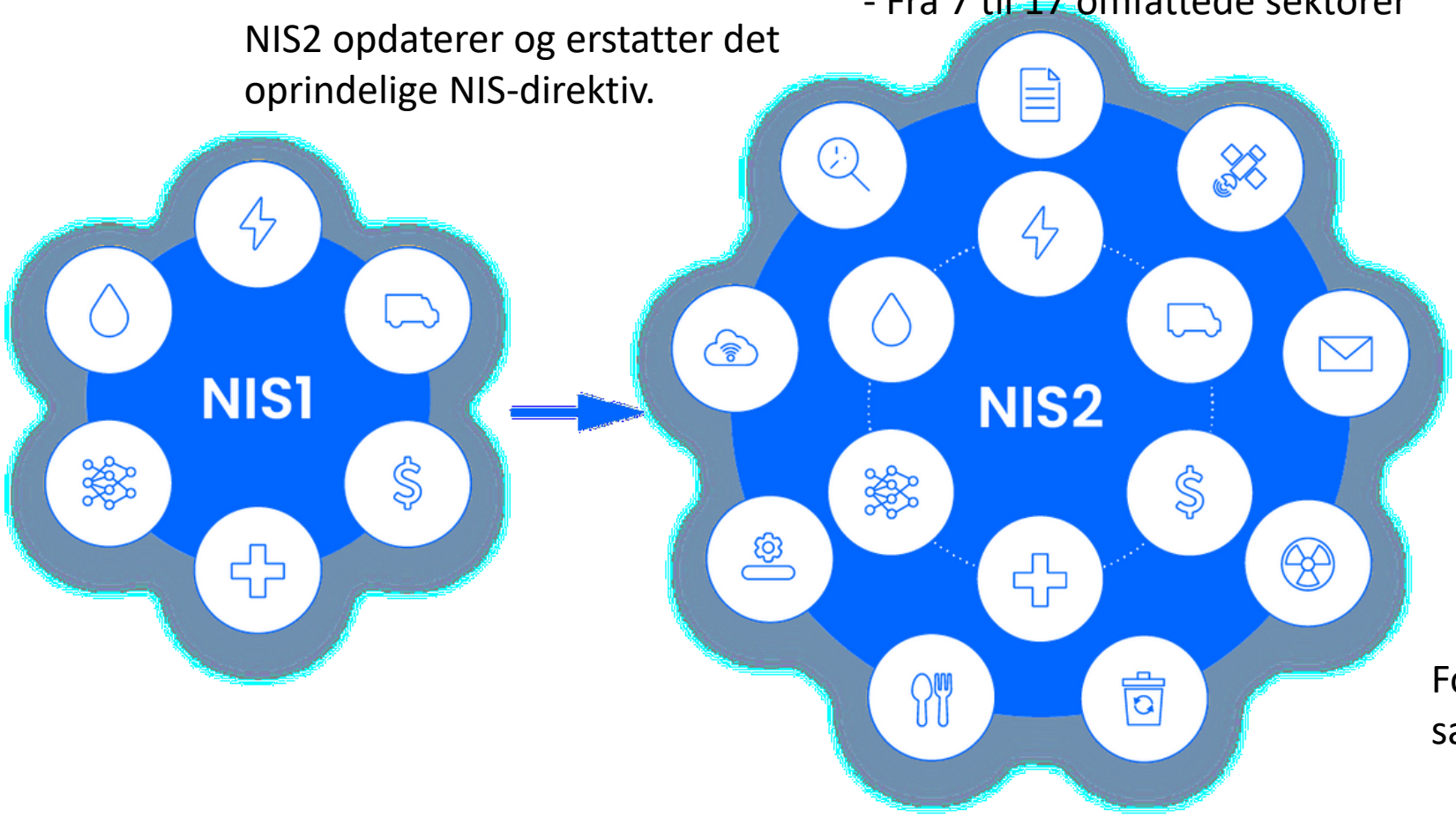
Baggrund

- Direktiv fra EU
- Bygger videre på NIS1 fra 2016, ikrafttrædelse 2018
- Hensigt: at sikre et højt cybersikkerhedsniveau på tværs af medlemslandene gennem bl.a:
  - Nationale CSIRT'er
  - Nationale kompetente myndigheder
  - Krav til omfattede enheder
  - Koordination imellem medlemslandene gennem bl.a. en samarbejdsgruppe
- En del af EU's fokus på det digitale område og sikkerhed, som også tæller:
  - Cyber resilience act (CRA)
  - Critical entities resilience directive (CER)
  - Cybersecurity act
  - Cyber solidarity act

Hv

NIS2 opdaterer og erstatter det oprindelige NIS-direktiv.

Udvider anvendelsesområde og tilføjer en række nye kritiske sektorer.
- Fra 7 til 17 omfattede sektorer



Faste kriterier for at omfattes sizecap reglen

Indfører skærpede krav om hændelsesrapportering (24 timer, 72 timer og 1 måned)

Indfører minimumsikkerheds-foranstaltninger og ledelsesansvar

Fokus på konsekvenser for samfundet

Indfører administrative sanktioner og potentielt bøder

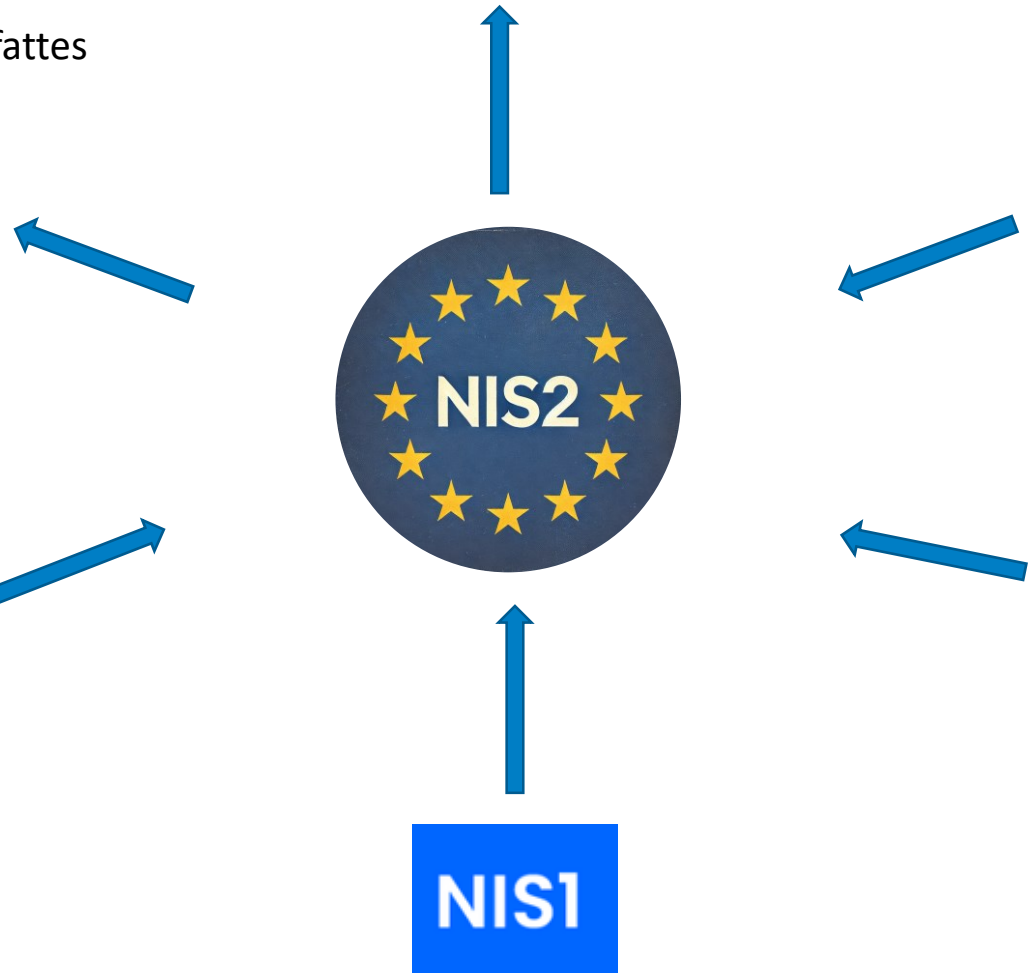
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Hvem er omfattet?

Konsekvens for sundhedssektoren:
Betyder formegentligt en udvidelse fra 9 enheder til mindst 200

Afhængig af NIS tjenesten der leveres kan organisationer omfattes som væsentlige eller vigtige enheder:

- Væsentlige enheder = regelmæssigt tilsyn + hændelsesbaseret tilsyn
- Vigtige enheder = hændelsesbaseret tilsyn



Særligt kritiske enheder kan omfattes, uden at overstige størrelseskriterier.

Organisationer omfattes, hvis de:

- Leverer tjenester inden for de definerede sektorer
- Overstiger 50 medarbejdere og omsætning eller balance på 10 mil euro (sizecap reglen).

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

Eksempler i de forskellige kategorier fra sundhed

Kategori (fra direktivets bilag)	>250 ansatte	50-250 ansatte	<50 ansatte (udpeges)
Sundhedstjenesteydere	Regioner (Hospitaler), ”kommuner”, ”aktører i sundhedsvæsenet der yder sundhed”	Privathospitaler, fertilitetsklinikker, store sundheds- og lægehuse, ambulancetjenester, apoteker	
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 er omfattet – et muligt eksempel

- De aktiviteter der er omfattet af direktivets anvendelsesområde
- F.eks. Sundhedsydelser, men ikke markedsføring for en sundhedstjenesteyder
- Tænk infrastruktur eller processer, som hvis det blev kompromitteret, ville kunne påvirke de aktiviteter der har gjort, at enheden er omfattet
- Kan potentielt være dele af processer og infrastruktur eller hele forretningen
- Vil afhænge af de konkrete tilfælde og setup

Omfattet enhed - sundhedstjenesteyder		
Forretningsprocesser		
Patientbehandling	Lønudbetaling	Markedsføring

Forretningsområde A Omfattet	**Forretningsområde B Ikke omfattet**	**Forretningsområde C Ikke omfattet**
Applikation A	**Applikation B**	**Applikation C**
Service A	**Service B**	**Service C**
System A	**System B**	**System C**
DB1		**DB2**
Grundlæggende delt infrastruktur – Hardware - netværk		

Minimumsforanstaltningerne fra lovudkast

- **Politikker for risikoanalyse og informationssystemsikkerhed**
- **Håndtering af hændelser**
- **Driftskontinuitet**, eksempelvis **backup-styring og reetablering** efter en katastrofe, og krisestyring
- **Forsyningskædesikkerhed**, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere
- **Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse** af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
- Politikker og procedurer til vurdering af **effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici**
- Politikker og procedurer vedrørende brug af **kryptografi** og, hvor det er relevant, **kryptering**
- **Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver**.
- Brug af løsninger med **multifaktorautentificering** eller **kontinuerlig autentificering**, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

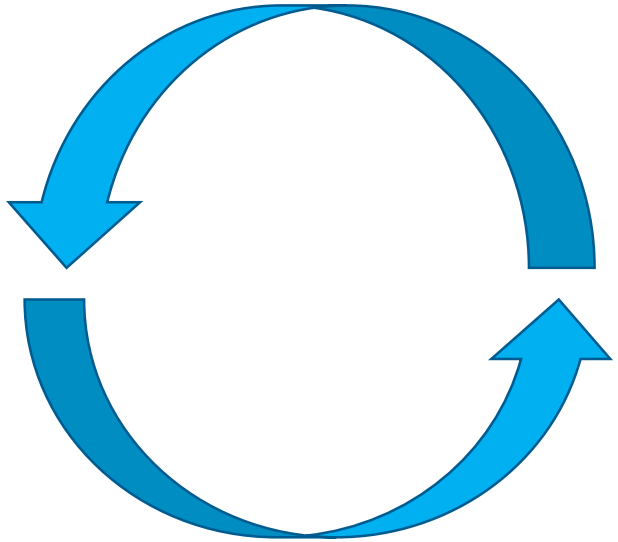
Så hvad skal man gøre?

0. Lav en ”omfattelses-vurdering” med begrundelse

8. Uddannelse af ledelse (og medarbejdere)

7. Udfør tilsyn med leverandører i ”første led”

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



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

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

5. Udarbejd proces og skaf bemanding for hændelseshåndtering:

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

3. For NIS2 infrastruktur
– implementér passende foranstaltninger

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

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk

DCISSund information

https://sundhedsdatastyrelsen.dk/informationssikkerhed