



14.45-15.15 Strategi for cyber- og Informationssikkerhed 2023—2025 v/ DCIS Sund
Med fokus på initiativer relevante for SDN, herunder:

- Munin
- Sårbarhedsskanning

SDN temadag sept. 2023

Hvis der bliver tid måske noget NIS2 ☺?



SUNDHEDSDATA-
STYRELSEN



Strategi for Cyber- og informationssikkerhed 2023-2025



**SUNDHEDSDATA-
STYRELSEN**

Strategien

Den nationale strategi for cyber- og informationssikkerhed fra maj 2022-2024



<https://digst.dk/strategier/cyber-og-informationssikkerhed/>



Primære fokusområder

- Hver sektor skal lave en strategi
- Oprette en DecentralCyber- og InformationsSikkerhedsenhed



Yderligere fokus

- Mere fokus på operative kapaciteter
- Mere fokus på samarbejde på tværs
- Flere faste krav til cybersikkerheden

Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022



Ny strategi Q3 2023

- Videreføre alt det gode

<https://sundhedsdatastyrelsen.dk/da/strategier-og-projekter/cyberstrategi>

Strategiens initiativer



2.7 Borgernært behandlingsudstyr og cybersikkerhed



EU-forordning om medicinsk udstyr (MDR)

Forordningen om medicinsk udstyr indeholder regler om og krav til medicinsk udstyr og har til formål at øge patientsikkerheden og sikre ensartede standarder for udvikling, produktion og anvendelse af medicinsk udstyr i Europa.

Medicinsk udstyr er blandt andet pacemakere, hjerteklapper, kondomer og graviditetstests, kirurgiske instrumenter, høreapparater, briller, kørestole og hospitalssenge.

Fabrikanterne skal anbringe en CE-mærkning på produktet for at vise, at det medicinske udstyr opfylder kravene i MDR.

Borgernært behandlingsudstyr og cybersikkerhed

Formål

Initiativet skal understøtte sundhedssektorens aktører i deres arbejde med at øge sikkerheden omkring borgernært behandlingsudstyr. Med borgernært behandlingsudstyr menes blandt andet telemedicinsk udstyr, udstyr der kan bæres på kroppen samt behandlingsudstyr hjemme hos borgeren, fx insulinpumper og glukosesensorer. Den teknologiske udvikling med nye muligheder for behandling af patienter med behandlingsudstyr inden i, uden på og nær ved borgeren, blandt andet i eget hjem, kræver en høj grad af tryghed. Dette både for borgeren, som står over for meget håndgribelige konsekvenser ved en hændelse, og for aktørerne i sundhedssektoren, der står over for nye udfordringer med at holde dette udstyr sikkert og robust i forhold til cybersikkerhed.

Værdi

Der er allerede gjort en stor indsats på området fra sektorens aktører, og initiativet vil samle denne indsats. Der opbygges et løsningskatalog omkring den sikkerhed, aktørerne benytter til borgernært behandlingsudstyr. Løsningskatalog skal indeholde de krav, der er stillet til leverandører af løsningerne. Løsningskataloget vil hjælpe de af sektorens aktører, der endnu ikke har bevæget sig ind på området. I udarbejdelsen af løsningskataloget ensortes krav til leverandører og underleverandører. Dette vil give værdi både for sektorens aktører samt for leverandørerne, der møder ensartede sikkerhedskrav på tværs af sektoren. Løsningskataloget tænkes derfor sammen med det katalog, der udarbejdes i initiativ 2.5 'Katalog over eksisterende sikkerhedskrav til it-leverandører'.

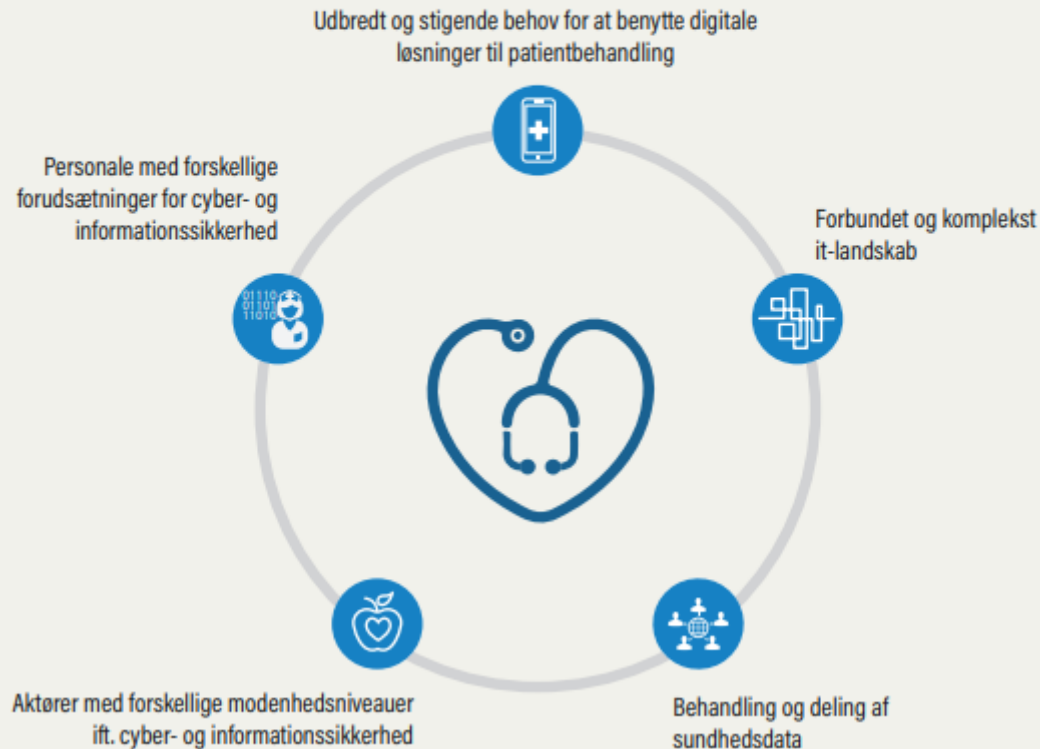
Indhold

I initiativets første fase samler en arbejdsgruppe med repræsentanter fra sektoren, der har erfaring med borgernært behandlingsudstyr, den eksisterende indsats, herunder eksisterende vejledninger og rammer, i et vejledningskatalog. Ud fra denne viden og vejledningskatalog udarbejder arbejdsgruppen en samlet sammenstilling af anbefalinger og krav til leverandører og underleverandører til sektoren inden for borgernært behandlingsudstyr.

Initiativet skal i relevant omfang koordineres med arbejdet i den fællesoffentlige digitaliseringsstrategi 2022-2025 samt arbejdet i sundhedsreformen 2022.

2.8 Cybersikkerhed hos de mindre aktører

Sundhedssektorens kendetegn



Formål

Flere af sundhedssektorens kerneopgaver understøttes af mindre aktører. Et potentielt angreb eller et længerevarende nedbrud hos disse mindre aktører vil kunne påvirke de større aktører og sektoren som helhed.

Disse mindre aktører (fx en lægepraksis eller mindre privat aktør i sundhedssektoren) står dog over for andre cyber- og informationssikkerhedsmæssige udfordringer end sektorens større aktører. Initiativet har derfor til formål at identificere barrierer hos de mindre aktører i deres arbejde med at styrke cybersikkerheden.

Værdi

En større hændelse for flere af de mindre aktører vil kunne have direkte eller indirekte konsekvenser for sundhedssektorens samfundsvigtige funktioner. En øget robusthed over for større hændelser hos de mindre aktører vil ikke blot skabe værdi for de mindre aktører og borgerne, men også bidrage til en øget robusthed for sektoren som helhed.

Indhold

De udfordringer, de mindre aktører står over for, er løbende blevet analyseret og rapporteret, men dette arbejde har ikke direkte hjulpet de mindre aktører til en fokuseret indsats for deres arbejde med deres cyber- og informationssikkerhedsmæssige udfordringer.

Første fase i dette initiativ er at udarbejde et samlet tiltagskatalog ud fra de eksisterende analyser med prioritering af de udfordringer, sundhedssektorens mindre aktører bør prioritere først. I næste fase nedsættes en arbejdsgruppe med relevante aktører, der har viden om udfordringerne hos de mindre aktører. Målet med arbejdsgruppen er at identificere de faktiske barrierer, de mindre aktører står overfor, når de højest prioriterede indsatser skal udmøntes. I fase tre vil arbejdsgruppen fokusere på at identificere mulige løsninger på disse barrierer og præsentere dem for styregruppen for udmøntning af strategien. En del af disse løsninger vil enten ikke kræve større investeringer for aktørerne, eller aktørerne vil selv skulle afholde udgifterne.

2.9 Bedre samarbejde om databeskyttelse ift. Digitalisering i sundhedssektoren



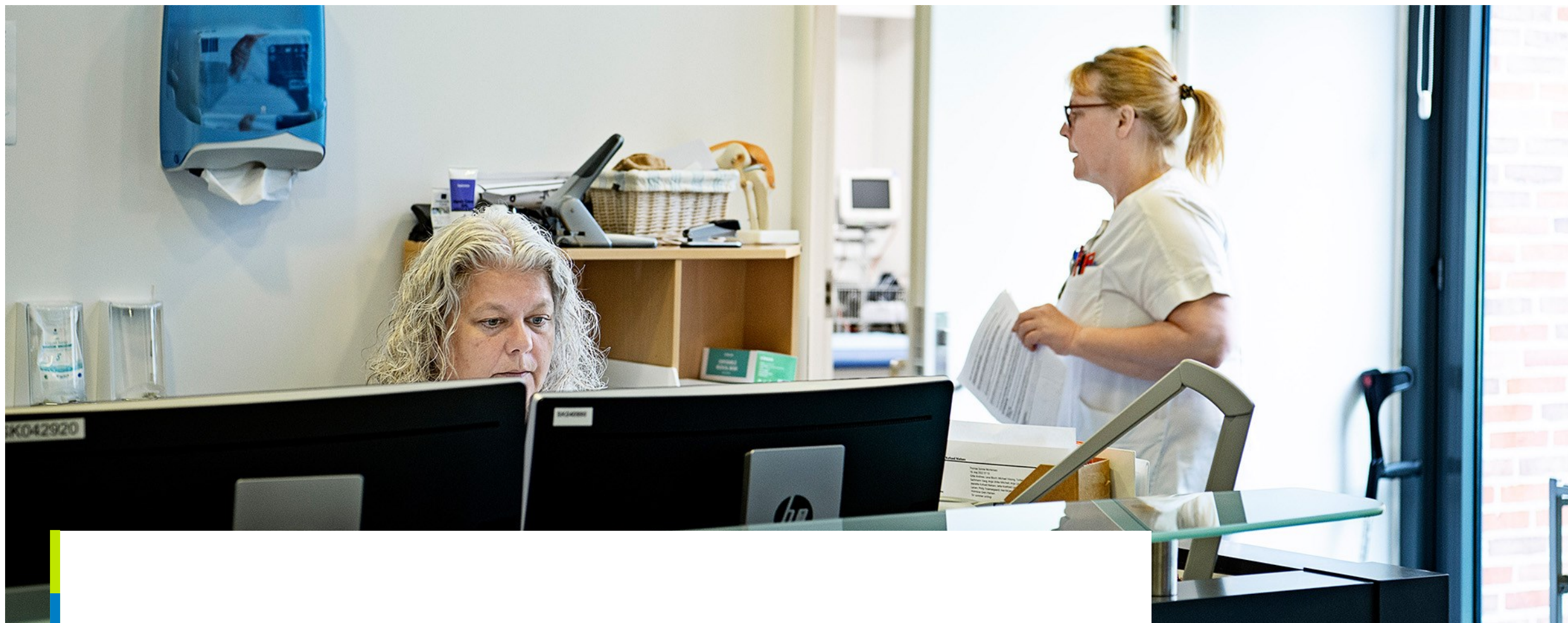
EU's Databeskyttelsesforordning

Databeskyttelsesforordningen (GDPR) trådte i kraft i maj 2018. Forordningen indeholder en lang række bestemmelser, der har til formål at sikre beskyttelsen af personoplysninger, fx bestemmelsen om forholdet mellem dataansvarlig og databehandler.

Den dataansvarlige afgør hvorfor (til hvilket formål) og hvordan (med hvilke hjælpemidler), personoplysninger behandles, mens databehandleren behandler oplysningerne på vegne af den dataansvarlige. Det indebærer blandt andet også, at den dataansvarlige i samarbejde med databehandleren skal sikre, at der er udarbejdet en databehandlersaftale mellem den dataansvarlige og databehandleren, som lever op til kravene i databeskyttelsesforordningen.

Bedre samarbejde om databeskyttelse ift. digitalisering i sundhedssektoren

Formål	I sundhedssektoren har de offentlige myndigheder et udvidet og tæt samarbejde omkring deling af data via digital infrastruktur, som bidrager til, at borgerne møder et sammenhængende sundhedsvæsen. Formålet med initiativet er at styrke dialogen om, hvordan de komplekse, tværoffentlige samarbejdskonstruktioner rent databeskyttelsesretligt kan håndteres i praksis samtidig med et fokus på, at borgernes rettigheder og følsomme personoplysninger fortsat beskyttes.
Værdi	Siden EU's databeskyttelsesforordning trådte i kraft, har de offentlige myndigheder arbejdet målrettet på at styrke arbejdet med databeskyttelse. Udmøntningen af den nye databeskyttelseslovgivning har været præget af et stærkt fokus på implementering af databeskyttelsesreglerne inden for rammerne af egen organisation i de enkelte offentlige myndigheder. Et styrket og struktureret samarbejde om databeskyttelse vil desuden kunne mindske barrierer både i forhold til øvrige initiativer i strategien samt i implementering af andre tværgående digitale løsninger i sundhedssektoren.
Indhold	De forskellige former for deling af data via fælles it-løsninger og infrastruktur i sundhedssektoren kategoriseres af en nedsat arbejdsgruppe med deltagelse af sektorens aktører. På baggrund af kategoriseringen identificeres de udfordringer, der særligt knytter sig til udmøntning af databeskyttelseslovgivningen i sundhedssektorens samarbejde om digitalisering. Arbejdsgruppen vil ligeledes se på mulige løsningsforslag, herunder hvordan samarbejdet mellem aktørerne bedst håndteres i forhold til bl.a. dataansvar, tilsyn, kontrol og håndtering af sikkerhedshændelser. Sundhedssektorens arbejde omkring dette koordineres med øvrigt arbejde inden for området, der pågår i sundhedssektoren, herunder 'Strategi for life science' samt med de nationale tiltag inden for samme område, herunder initiativ 3.7 i den nationale cyber- og informationssikkerhedsstrategi 2022-2024.



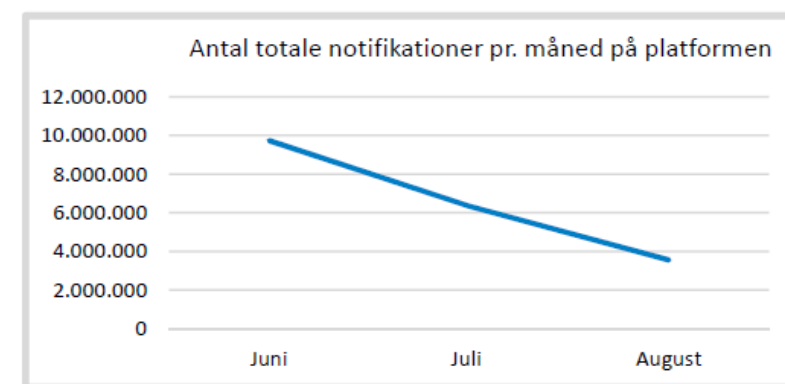
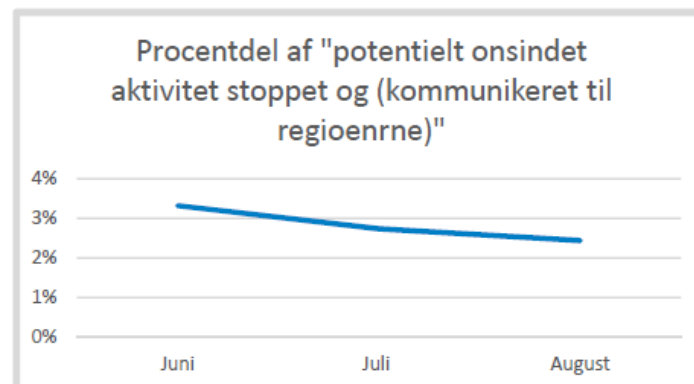
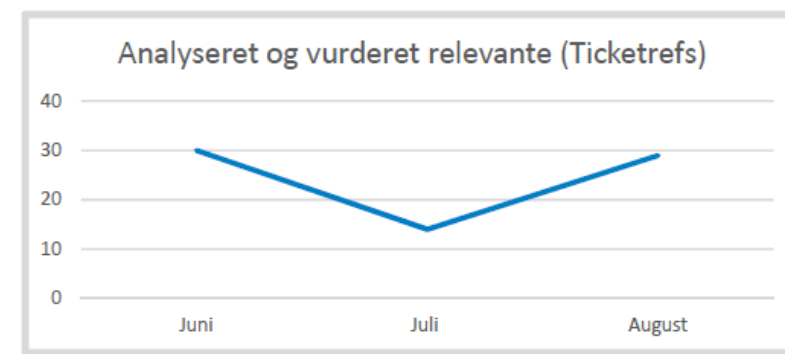
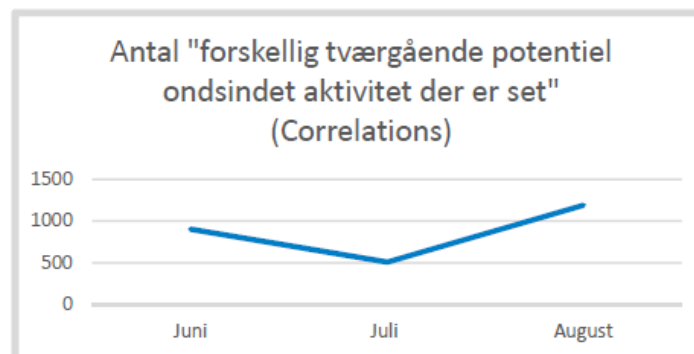
Status på 3.1 og 3.2

Muninn

- ▶ Platform har været i drift siden 1. juni
- ▶ Fem regioner er på
- ▶ Pilot for tre kommuner er ved at blive aftalt
- ▶ Analyse omkring tilslutning fra "praksis delen af sektoren" foretages af PLO.
- ▶ Der er åbent for nye aktører
 - Et privat hospital
 - SDS
- ▶ Vil du være med 😊?!

Skriv DCISsund@sundhedsdata.dk

	Juni	Juli	August	September	Oktober	November	December
Antal totale notifikationer pr. måned på platformen	9.736.863	6.352.241	3.557.414				
Antal "forskellig tværgående potentiel ondsindet aktivitet der er set" (Correlations)	903	511	1190				
Analyseret og vurderet relevante (Ticketrefs)	30	14	29				
Procentdel af "potentielt ondsindet aktivitet stoppet og (kommunikeret til regionerne)"	3%	3%	2%				
Antal kritiske tværgående angreb (med opringning)	0	0	1				

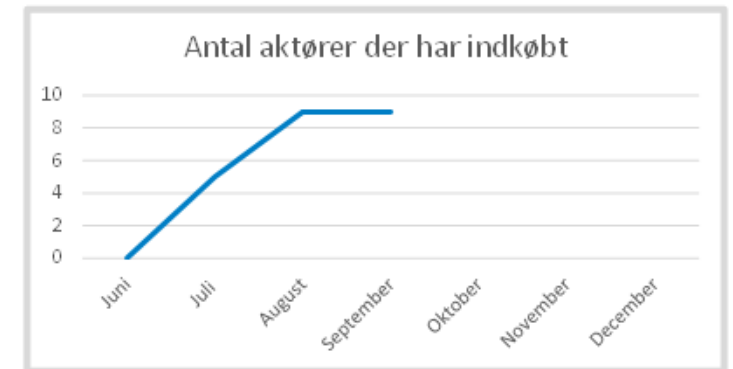
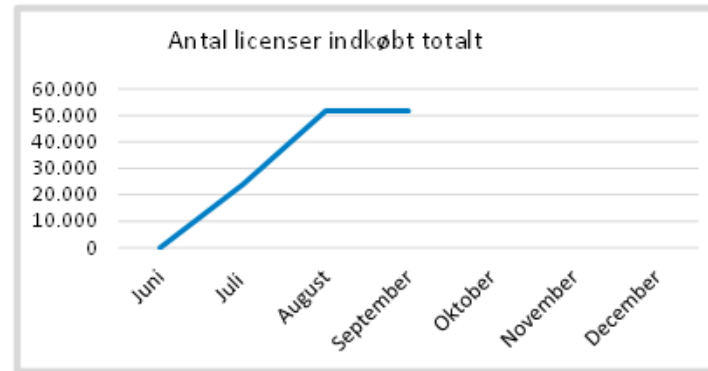


Rammeaftale for sårbarhedsscanning



- ▶ Rammeaftale færdig, licenser købes gennem Atea
- ▶ Konsulent arbejde kan I købe af jeres egne leverandører
- ▶ Produkt er Tenable.SC+
- ▶ Pris pr. licens pr. år 14,41 kr. (normalpris ligger mellem 105-160 kr.)

	Juni	Juli	August	September	Oktober	November	December
Antal licenser indkøbt totalt	0	24.000	51.800	51800			
Antal aktører der har indkøbt	0	5	9	9			
Antal aktører der har tilmeldt sig "Sektor overblik"	0	2	3	3			



- ▶ Vil du være med 😊?!

Skriv DCISsund@sundhedsdata.dk





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

NIS2, tjenester og alt det der!

Kort intro til NIS2 og hvad jeg tror det har af effekt.

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk



**SUNDHEDSDATA-
STYRELSEN**

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

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

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk



DCISSund på Twitter
[@dcissund](https://twitter.com/dcissund)

DCISSund information

<https://sundhedsdatastyrelsen.dk/informationssikkerhed>