

FÆLLES BESKYTTELSE OG ROBUSTHED GENNEM SAMARBEJDE OG SYNERGIER

Sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025



Sammen om et fortsat sikkert og robust sundhedsvæsen



Sophie Løhde
Indenrigs- og sundhedsminister

Christina Krzyrosiak Hansen
Formand for Sundheds- og Ældreudvalget

Anders Kühnau
Formand for Danske Regioner

Gode digitale løsninger og styrket brug af sundhedsdata er en afgørende del af at fremtidssikre det danske sundhedsvæsen. Digitale løsninger spiller allerede en stor rolle i vores sundhedsvæsen. Danmark er frontløber, når det drejer sig om anvendelsen af digitale løsninger og sundhedsdata. Det kan vi være stolte af, men der er fortsat et stort potentiale.

Vi skal bruge digitale løsninger og sundhedsdata, så borgerne oplever sammenhængende behandlingsforløb af høj kvalitet på tværs af sundhedsvæsenet. Vi skal understøtte smartere og smidigere arbejdsgange med bl.a. enklere adgang til relevante sundhedsoplysninger og frigive tid hos personalet til den enkelte patient. Vi skal bringe behandling og pleje endnu tættere på borgerens eget hjem.

Alt dette skal naturligvis foregå i trygge og sikre rammer. Med den stigende digitalisering af sundhedsvæsenet følger der ligeledes risici, som vi må tage hånd om. Det er en opgave, vi tager meget alvorligt. Det er helt afgørende, at når de digitale løsninger flytter ind, skal sikkerheden også følge med. Borgerne skal fortsat kunne stole på, at sundhedsvæsenet er tilgængeligt, når de har brug for det, og at sundhedsvæsenet passer godt på de

følsomme personoplysninger, som de betror sundhedsvæsenet i forbindelse med et behandlingsforløb.

Derfor er det nødvendigt, at vi viderefører det allerede gode samarbejde og i fællesskab fortsætter med at styrke cyber- og informationssikkerheden på tværs af sundhedsvæsenet. Samtidig er sundheds- og plejepersonalet sundhedsvæsenets allervigtigste ressource. Personalet skal have tid og rum til at løse kerneopgaven. Det kræver, at rammerne for at udføre deres arbejdsopgaver, herunder også hensynet til cyber- og informationssikkerhed, bedst muligt understøtter personalet i deres hverdag.

Sundhedssektorens hidtidige arbejde med cyber- og informationssikkerhed giver os et godt udgangspunkt for den fortsatte fælles indsats. Indsatserne fra den første fælles strategi for cyber- og informationssikkerhed i sundhedsvæsenet 2019-2022 udgør et stærkt fundament, som denne strategi bygger videre på. Vi vil således både fortsætte det gode arbejde, som allerede er i gang, og med udvalgte nye initiativer yderligere styrke den fælles koordinerede indsats inden for cyber- og informationssikkerhed. Sammen vil vi arbejde for et fortsat sikkert og robust sundhedsvæsen.

Indhold

2		Sammen om et fortsat sikkert og robust sundhedsvæsen
4		Et højt fælles cyber- og informationssikkerhedsniveau
8		Strategiske målsætninger
10		En risikobaseret dynamisk indsats
12		Strategien bygger på solide indsatser i sektoren
16		Governance og organisering
18	Spor 1 - Forudse	Bedre forudsigelse af potentielle angreb og hændelser
	Initiativ 1.1	Vedligeholdelse af overblikket over sundhedssektorens samfunds vigtige funktioner og kritisk it-infrastruktur
	Initiativ 1.2	Overblik over sundhedssektorens tværgående og samlede risici
22	Spor 2 - Forebygge	Bedre mulighed for at forebygge angreb og hændelser
	Initiativ 2.1	Cyber- og informationssikkerhed på de sundhedsfaglige uddannelser
	Initiativ 2.2	Rammer for rette og tidssvarende tekniske foranstaltninger
	Initiativ 2.3	Kortlægning af legacy-systemer i kritisk it-infrastruktur
	Initiativ 2.5	Katalog over eksisterende sikkerhedskrav til it-leverandører
	Initiativ 2.6	Udbygning af sektorens sikkerhedsarkitektur
	Initiativ 2.7	Borgernært behandlingsudstyr og cybersikkerhed
	Initiativ 2.8	Cybersikkerhed hos de mindre aktører
	Initiativ 2.9	Bedre samarbejde om databaseskyttelse ift. digitalisering i sundhedssektoren
30	Spor 3 - Opdage	Bedre mulighed for at opdage angreb og hændelser
	Initiativ 3.1	Fælles rammer og værktøjer til understøttelse af aktørernes løbende test af cybersikkerheden
	Initiativ 3.2	Udbredelse af overvågnings- og analysefunktioner på tværs af sektoren
34	Spor 4 - Håndtere	Hurtig håndtering i tilfælde af angreb og hændelser
	Initiativ 4.3	Udbredelse af beredskabsøvelser for fælles systemer og forsyningskæder

Strategien indeholder to dele

Første del af strategien beskriver de overordnede rammer, visioner og målsætninger. Herefter følger et overblik over de initiativer, der er sat i verden for at udmønte strategien i praksis, og som DCIS faciliterer et sektorsamarbejde om at drive fremad i løbet af strategiperioden.

Et højt fælles cyber- og informationssikkerhedsniveau

Tusindvis af borgere er hver dag i berøring med og afhængige af sundhedssektoren, og det er afgørende, at sektorens sundhedsprofessionelle kan levere rettidig behandling og pleje. Et højt niveau af cyber- og informationssikkerhed er et vigtigt led i arbejdet med at sikre, at borgerne kan få den rette behandling og pleje, når de behøver den.

Den danske sundhedssektor er kendetegnet ved en høj grad af digitalisering med stadig mere samarbejde om behandling og pleje på tværs af sektoren, som samtidig rykker endnu tættere på borgerens eget hjem. Fælles digitale løsninger er med til at skabe rammerne for en mere helhedsorienteret sundhedssektor på tværs af hospitaler, praktiserende læger og kommunale sundhedstilbud. Med en digitaliseret sundhedssektor, hvor digitale løsninger er integrerede med hinanden og med et højt niveau af datadeling, følger også et stort behov for at beskytte sektoren mod cyberangreb.

Arbejdet med at sikre et trygt og tilgængeligt sundhedsvæsen er et kontinuerligt arbejde og kræver samarbejde. Med sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025 fokuseres og rammesættes sektorens fortsatte fælles indsats for yderligere at styrke den samlede robusthed over for cyber- og informationssikkerhedshændelser.

Cybertruslen er i dag en af de alvorligste trusler mod vores sundhedssektor, og hver dag ses forsøg på cyberangreb mod både myndigheder, leverandører og borgere i udlandet såvel som i Danmark. Dette kan være alt fra phishing-angreb til supply-chain angreb. Truslen udvikler sig konstant med nye angrebsformer og udnyttelse af nye sårbarheder.

Udviklingen i den geopolitiske situation medfører, et mere komplekst og hybridt trusselsbillede, hvor cybertrusler og fysiske trusler flyder sammen og interagerer. Den geopolitiske udvikling nødvendiggør et anderledes fokus på fysiske trusler og scenarier inden for cyber- og informationssikkerhed, hvor energidistribution, sundhedssektoren og anden kritisk infrastruktur direkte bliver truet udefra. Dette gør arbejdet med at gøre sundhedssektoren robust over for cyber- og informationssikkerhedshændelser endnu vigtigere og tidskritisk.

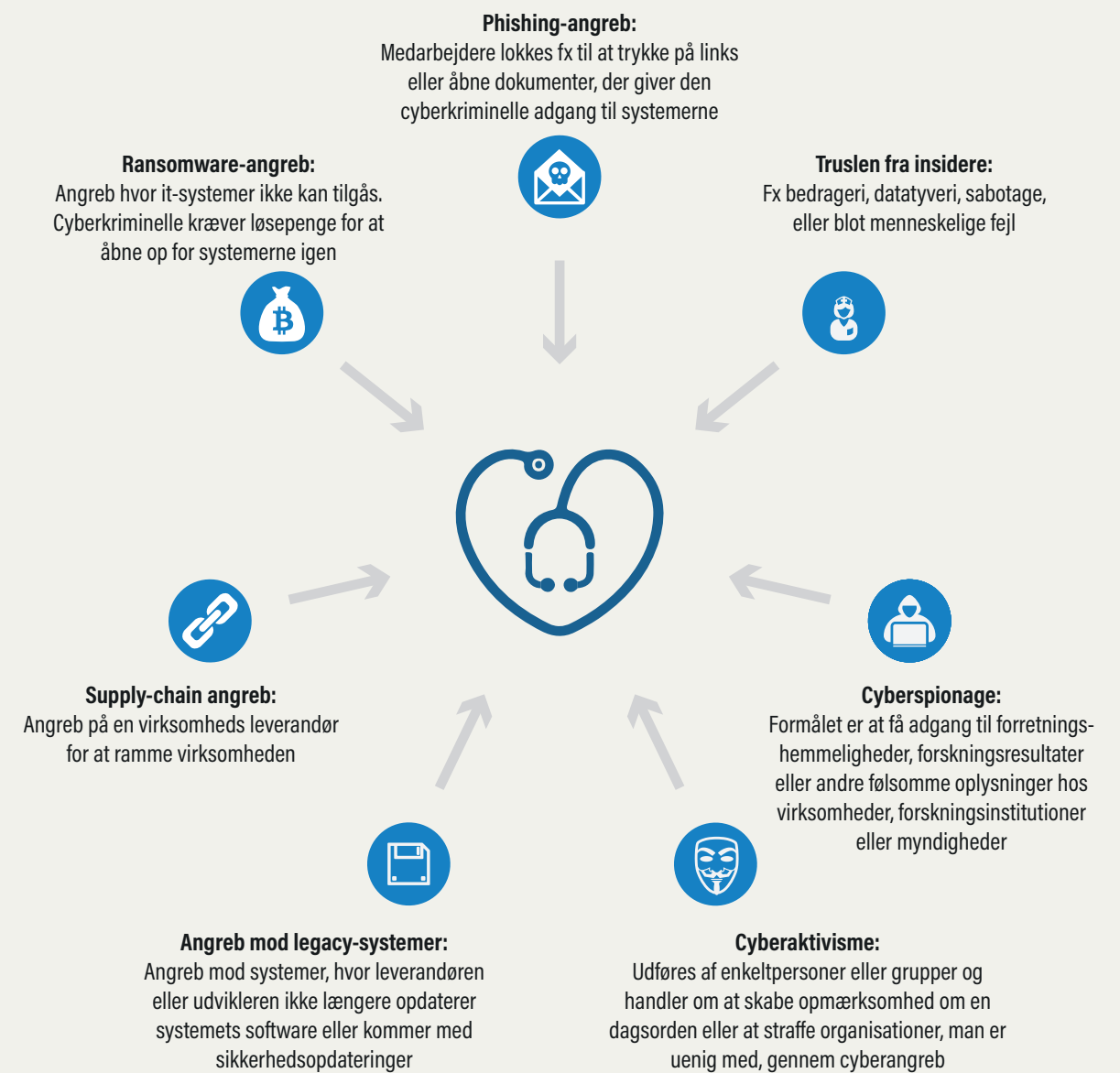
Sundhedssektorens aktører

Samtlige organisationer og myndigheder, der direkte eller indirekte udfører tjenester eller ydelser i sundhedssektoren, benævnes i strategien som aktører.

Den fælles benævnelse omfatter i tillæg til regioner, kommuner og statslige myndigheder også aktører i det nære sundhedsvæsen samt andre organisationer og leverandører, der udfører eller er nødvendige for vigtige funktioner i sundhedssektoren, fx apoteker, privathospitaler, MedCom, sundhed.dk mv. Det er vigtigt, at disse organisationer inkluderes i strategiens arbejde, da sundhedssektoren er tæt forbundet, og aktørerne er afhængige af hinanden på kryds og tværs af sektoren for at kunne udgøre en samlet sikker sundhedssektor.

FIGUR

Sundhedssektorens største trusler

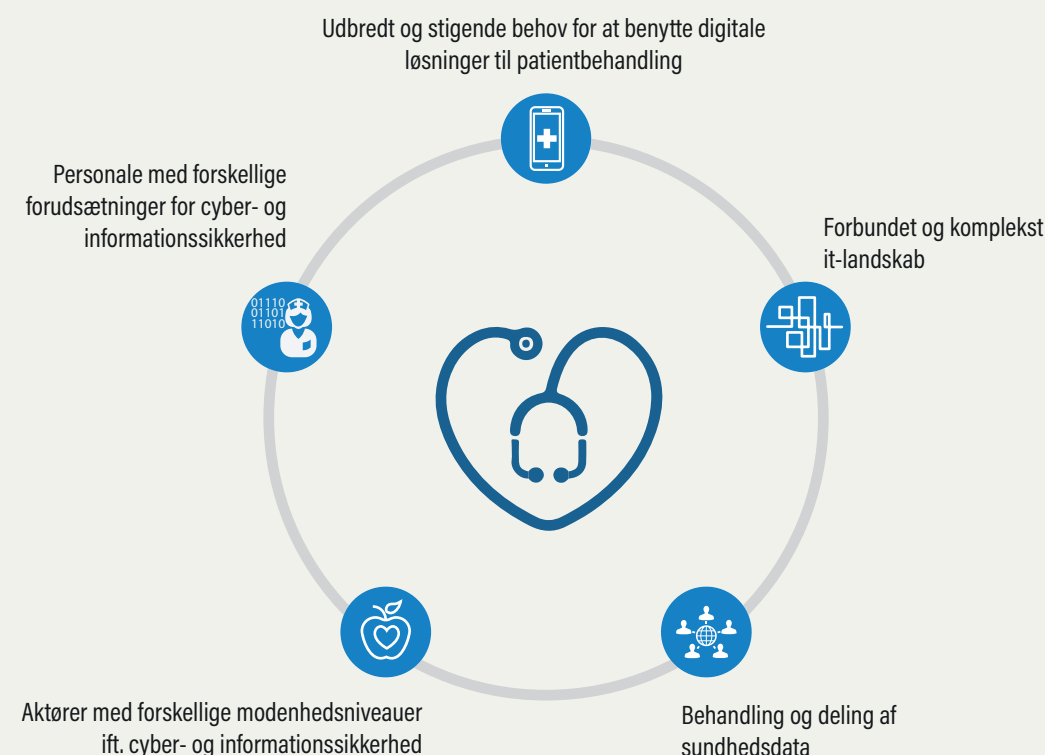


En høj trussel behøver ikke betyde en høj risiko

En sårbarhed udgør en potentiel svaghed, der kan udnyttes, mens en trussel er et udtryk for, om nogen har til hensigt at gøre skade. Sårbarhed og trussel giver til sammen en indikation af sandsynligheden for, om fx ondsindede aktører kan trænge ind i et it-system eller organisation. Konsekvensen af hændelsen indikerer, hvor slemt det vil være, hvis nogen udnytter sårbarheden og dermed udløser en sikkerhedshændelse. Det samlede billede af de tre aspekter udgør den risiko, man løber ved fx at have en sårbarhed i et it-system.

Et eksempel kan være risikoen for indbrud i et hus, hvor tyven udgør truslen, mens sårbarheden kan bestå i, om der er lås på døren. Konsekvensen består i, om der er noget værd at stjæle i huset. På trods af en høj trussel (mange indbrud i nabolaget), kan risikoen nedsættes ved fx at have låst døren og pakket værdigenstandene godt væk.

Sundhedssektorens kendetegn



Udbredt og stigende behov for at benytte digitale løsninger til patientbehandling

Sektorens aktører samarbejder i udpræget grad om behandling og pleje ved hjælp af digital udveksling af sundhedsdata, der bidrager til sammenhængende patientforløb på tværs af sundhedssektoren.

Samtidig rykker patientbehandlingen tættere på borgeren med tilbud om øget behandling i borgernes eget hjem i form af blandt andet monitorering, konsul-

tationer og behandling. Det kræver teknisk understøttelse i form af behandlingsudstyr, mobilt udstyr eller andre værktøjer af teknisk karakter, som borgeren får stillet til rådighed i eget hjem til sin behandling. Det stiller krav til både den tekniske sikkerhed i udstyret samt personalets og borgernes forståelse for, at udstyr og sundhedsoplysninger skal håndteres sikkert og forsvarligt.



Forbundet og komplekst it-landskab

Sundhedssektoren er underbygget af et komplekst it-landskab med forbundne systemer og infrastruktur til fx deling af sundhedsdata. Kombinationen af et komplekst it-landskab og den høje værdi, som sundhedsdata har på det sorte marked, gør sekto-

ren særligt interessant for cyberkriminelle. At sektorens aktører er tæt forbundne digitalt betyder også, at et cyberangreb hos bare én aktør eller leverandør potentielt kan spredes med store konsekvenser for både sektoren og borgerne.



Behandling og deling af sundhedsdata

Sundhedssektoren behandler store mængder af følsomme personoplysninger og sundhedsdata til gavn for borgernes behandlingsforløb, forskning og kvalitetsudvikling.

Med udviklingen i øget behandling i det nære sundhedsvæsen kommer kommunerne og de privatpraktiserende klinikker til at spille en større rolle i sundhedsvæsenet. Det medfører deling af sundhedsdata i en større skala end tidligere i det nære sundhedsvæsen. En øget brug og deling af sundhedsdata er med til at øge risikoen for cyberangreb imod disse aktører,

hvilket potentielt også kan medføre en større samlet konsekvens for sundhedssektoren som helhed.

Det øgede behov for digital deling af følsomme personoplysninger på tværs accelererer desuden behovet for at finde løsninger på de databeskyttelsesretslige udfordringer, aktørerne står overfor, når behovet for adgang til og deling af sundhedsdata på tværs af sektoren yderligere forøges. Fx at aktørerne hver især skal bruge ressourcer på at udarbejde et stort antal databehandlersaftaler eller føre tilsyn på den samme løsning med den samme databehandler.



Aktører med forskellige modenhedsniveauer ift. cyber- og informationssikkerhed

Sundhedssektoren består af mange forskellige aktører; både offentlige og private, store, mellemstore og små aktører. Modenhedsniveauet for cyber- og informationssikkerhed er derfor også meget forskelligt aktørerne imellem. Der kan være store forskelle på, hvor mange ressourcer de enkelte aktører kan dedikere til arbejdet med cyber- og informations-

sikkerhed. Spørgsmålet omkring aktørernes modenhedsniveau aktualiseres i takt med, at der deles langt flere sundhedsdata på tværs af aktørerne end tidligere. Det forventes, at også aktører, som på nuværende tidspunkt har lav modenhed inden for cyber- og informationssikkerhed, fremover vil skulle behandle væsentligt flere sundhedsdata.



Personale med forskellige forudsætninger for cyber- og informationssikkerhed

Sundhedssektorens medarbejdere arbejder inden for både patientbehandling, pleje, administrative opgaver, it og servicefaget. Det betyder, at personalet har vidt forskellige forudsætninger for at forholde sig til informationssikkerhedsmæssige problemstillinger, også inden for samme organisation.

Personalemangel i sundhedssektoren betyder samtidig, at tiden til patientbehandling og pleje er udfordret. I en travl hverdag risikerer passende cyber- og informationssikkerhedsadfærd, som fx at logge af og låse sin skræm, at blive glemt, hvilket kan føre til sikkerhedshændelser såsom uautoriseret adgang til patientoplysninger.



Hvorfor er sundhedsdata så interessante for cyberkriminelle?

Sundhedsdata har en utrolig høj værdi for cyberkriminelle. Dette skyldes, at sundhedsdata er følsomme helbredsoplysninger – ofte fra fødsel til død. Samtidig er de statiske og har en lang levetid.

Cyberkriminelle kan udnytte sundhedsdata til kriminelle aktiviteter, og de har en stor økonomisk værdi. Fx kan et nyligt stjålet kreditkort kun indbringe \$1 på det sorte marked, da det ikke indeholder mange informationer og mister sin værdi, når det bliver spærret; mens en fuld sundhedsjournal kan indbringe mellem \$250-1000. Cyberkriminelle kan også bruge stjålne sundhedsdata til afpresning af enten den organisation, hvor dataene stammer fra, eller afpresning af borgeren direkte.

Strategiske målsætninger

Strategien har overordnet til formål at understøtte et samlet sikkerhedsløft i sektoren, således at sektorens kapacitet til at forudse, forebygge, opdage og håndtere cyber- og informationssikkerhedshændelser styrkes.

Strategien sætter fire strategiske målsætninger for sektorens arbejde med cyber- og informationssikkerhed. De strategiske målsætninger suppleres desuden af et eller to underpunkter, der uddyber formålet med hver strategisk målsætning.



Sektoren skal øge robustheden over for cyber- og informationssikkerhedshændelser

Sektorens aktører skal kunne opretholde samfundsvigtige funktioner, være i stand til at agere koordineret med kort varsel samt hurtigt og sikkert kunne genoprette almindelig drift i tilfælde af alvorlige cyberhændelser

Den omskiftelige geopolitiske situation samt den stigende trussel fra cyberkriminelle gør det nødvendigt at fokusere på arbejdet med en øget robusthed over for cyber- og informationssikkerhedshændelser. Sundhedssektorens aktører er tæt forbundne, hvilket poten-

tielt gør konsekvensen af eventuelle hændelser større. Derfor skal robustheden øges hos sektorens både større og mindre aktører, således at sektoren samlet kan opretholde de samfundsvigtige funktioner – også i en krisesituation.



Et højt niveau af cyber- og informationssikkerhed skal sikre tryghed hos borgeren

Sektorens fortsætter det hidtidige arbejde med at styrke sikkerheden både i centrale systemer og i borger-nært behandlingsudstyr, så tilliden til, at sundhedsvæsenet passer godt på borgerens data, fastholdes.

Sektorens aktører understøtter gennem vidensdeling en tryk og sikker anvendelse af borgernært behandlingsudstyr til flere områder og brugsscenerier.

Med den øgede digitalisering og den øgede brug af digitale løsninger til patientbehandling tættere på borgeren, fx i borgerens eget hjem, er der ikke længere kun tale om at styrke sikkerheden i systemerne centralt hos sektorens aktører. Udviklingen er ikke ny, og en del af sektorens aktører arbejder allerede med sikker anvendelse af borgernært behandlingsudstyr.

Et styrket samarbejde både inden for cybersikkerhed, informationssikkerhed og databeskyttelse på tværs af sektorens aktører skal sikre tryghed hos borgeren igennem hele behandlingsforløbet, også i borgerens eget hjem.



Sundhedspersonalet skal kunne arbejde sikkert med teknologi og data

Sektorens aktører fokuserer i arbejdet med strategiens initiativer på, at løsninger og sikkerhedstiltag ikke uforholdsmæssigt øger arbejdsbyrden eller kompleksiteten af sundhedspersonalets arbejde.

Sektorens aktører understøtter indsatsen for at sikre uddannelsen af nye cyber- og informationssikkerhedsspecialister samt udviklingen af eksisterende kompetencer i sektoren.

De nuværende udfordringer med mangel på arbejdskraft i sundhedssektoren understreger vigtigheden af, at det skal være så let og smidigt som muligt for de ansatte at agere sikkert i deres daglige arbejde med borgerne.

Samtidig skal sikkerhedsniveauet i sektoren være passende sammenholdt med både konsekvenserne ved en hændelse og hensynet til den almindelig behandling og pleje af borgeren.



Samarbejdet skal styrkes på tværs af de kritiske sektorer og sundhedssektorens egne aktører

Sundhedssektoren indgår aktivt i samarbejde og vidensdeling med de andre sektorer, herunder også i arbejdet med kortlægning af afhængigheder på tværs af sektorerne.

Sundhedssektorens aktører udbygger den fælles indsats og samarbejdet på tværs både inden for teknisk og organisatorisk sikkerhed.

Sundhedssektoren er afhængig af andre sektors services, herunder især strøm, varme, vand og internet. Sektoren samarbejder derfor på tværs af de andre sektorer med blandt andet vidensdeling og

kortlægning af disse afhængigheder. Aktørerne i sektoren kan også lære af hinanden, og vidensdeling inden for både teknisk og organisatorisk sikkerhed skaber robusthed og sikkerhed på tværs.



Definition af samfundsvigtige funktioner og kritisk it-infrastruktur

I National strategi for cyber- og informationssikkerhed 2022-2024 gives følgende definitioner, som sundhedssektorens strategi følger:

- Samfundsvigtige funktioner:** De aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed. Fx medicinbehandling og sundhedsberedskabet.
- Kritisk infrastruktur:** Infrastruktur, herunder systemer, tjenester, processer, netværk og aktiver samt serviceydelser, der er nødvendige for at opretholde eller genoprette samfundsvigtige funktioner. Fx hospitaler og andre vigtige enheder i sundhedssektoren.
- Kritisk it-infrastruktur:** Den delmængde af kritisk infrastruktur, der omfatter den digitale infrastruktur, der er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner. Fx den nationale infrastruktur og den nationale serviceplatform (NSP), der sikrer deling af data på tværs af sundhedssektoren.

En risikobaseret dynamisk indsats

Strategien skal baseres på en helhedsorienteret og risikobaseret tilgang, hvor der sættes ind der, hvor behovet og effekten er størst.

Arbejdet med cyber- og informationssikkerhed skal følge med udviklingen. Det gælder såvel i forhold til sundhedssektorens opgaver og arbejdsgange som, at sektoren skal kunne tilpasse sig ved løbende skift i trusselsbilledet.

Strategiens indsatser for at styrke cyber- og informationssikkerheden baseres på en risikobaseret tilgang, hvor initiativerne prioriteres og justeres i forhold til de væsentligste risici for sektoren. Det er nødvendigt løbende at vurdere, hvor en potentiel sikkerhedshændelse vil være mest kritisk i forhold til at sikre det sammenhængende sundhedsvæsen og den fortsatte patientbehandling. Denne dynamiske tilgang indebærer blandt andet en årligt tilbagevendende proces, hvor strategiens indsatser holdes op imod det aktuelle trusselsbillede, aktørernes egne risikovurderinger og den samlede indsats i sektoren. Styregruppen for udmøntning af strategien skal løbende prioritere initiativporteføljen i forhold til aktuelle risikobillede. Herved sikres, at fokus i arbejdet

med cyber- og informationssikkerhed lægges der, hvor behovet er størst, og der kan opnås den største samlede værdi for sektoren.

Relevansen af en risikobaseret, dynamisk tilgang afspejles desuden i de krav eller minimumsanbefalinger som følger af National strategi for cyber- og informationssikkerhed 2022-2024 samt EU's databeskyttelsesforordning (GDPR) og NIS2-direktiv. Ved enten at implementere det internationale styringsværktøj for informationssikkerhed, ISO 27001-standarden, som det gør sig gældende for staten, at efterleve principperne i informationssikkerhedsstandarden, som det gør sig gældende for regionerne, eller at følge principperne i standarden, som det gør sig gældende for kommunerne, eller ved at følge anden best practice kommer aktørerne langt i arbejdet med at kunne håndtere sikkerhedsudfordringerne og leve op til kravene i de nuværende europæiske direktiver og dansk lovgivning.



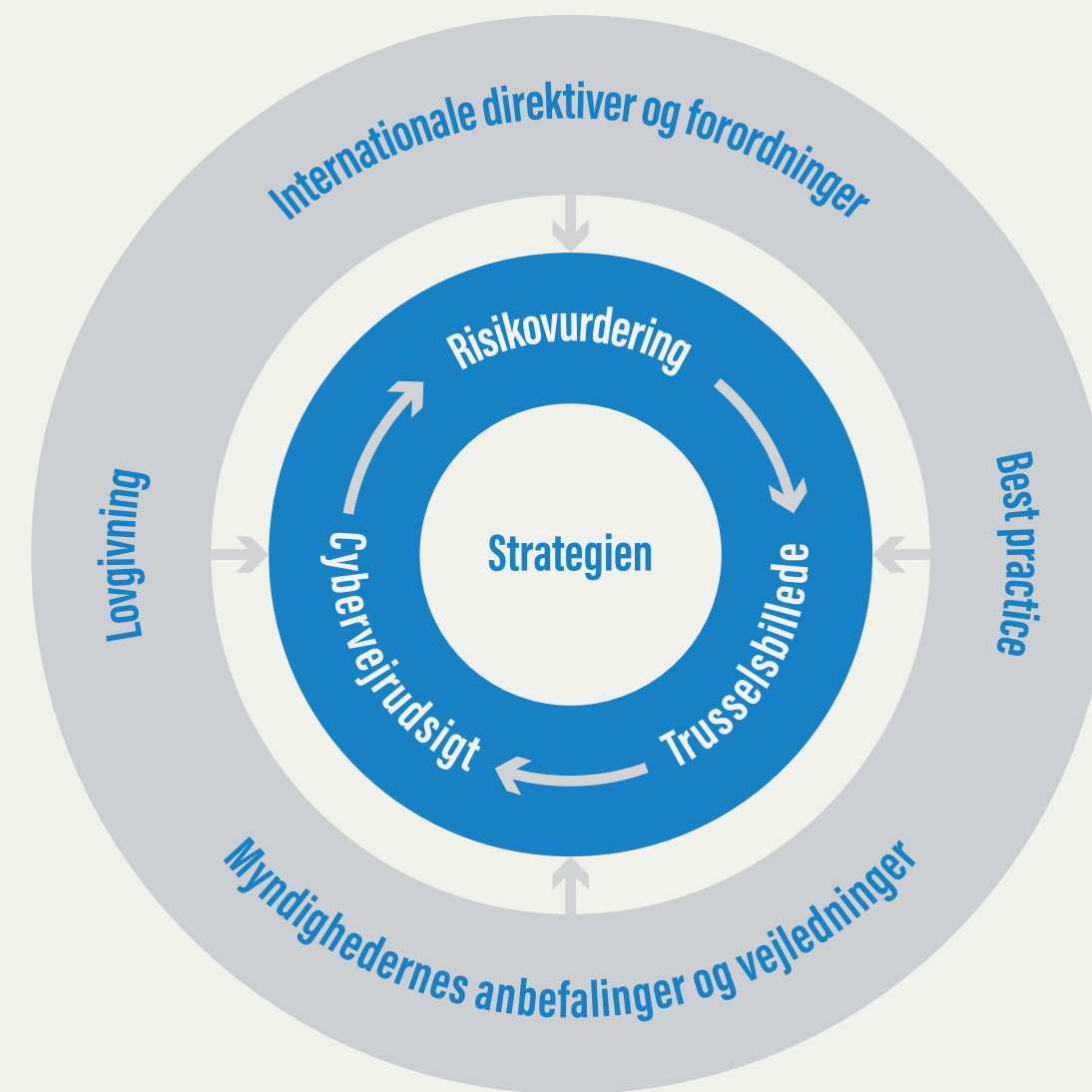
Cyber- og informationssikkerhed på europæisk plan

Også på europæisk plan fokuseres der på at øge niveauet for cyber- og informationssikkerhed på tværs af landegrænser.

- Med EU's Net- og Informationssikkerhedsdirektiv (NIS) samarbejder de europæiske medlemslande for at opnå øget robusthed inden for cyber- og informationssikkerhed. Med vedtagelsen af NIS2-direktivet ensrettes og skærpes lovkravene til cyber- og informationssikkerhed på tværs af medlemslandene.
- Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) bidrager til EU's politik for cybersikkerhed og samarbejder med medlemsstater og EU-organer. Agenturet arbejder med vidensdeling, kapacitetsopbygning og oplysningskampagner på tværs af Europa.
- Europa-Kommissionens forslag til forordningen 'European Health Data Space' støtter: At enkeltpersoner får kontrol over deres egne sundhedsdata; anvendelsen af sundhedsdata med henblik på bedre levering af sundhedsydelser, bedre forskning, innovation og politikudformning; og sætter EU i stand til fuldt ud at udnytte det potentiale, der ligger i sikker udveksling, brug og genanvendelse af sundhedsdata.

FIGUR

En dynamisk, strategisk indsats



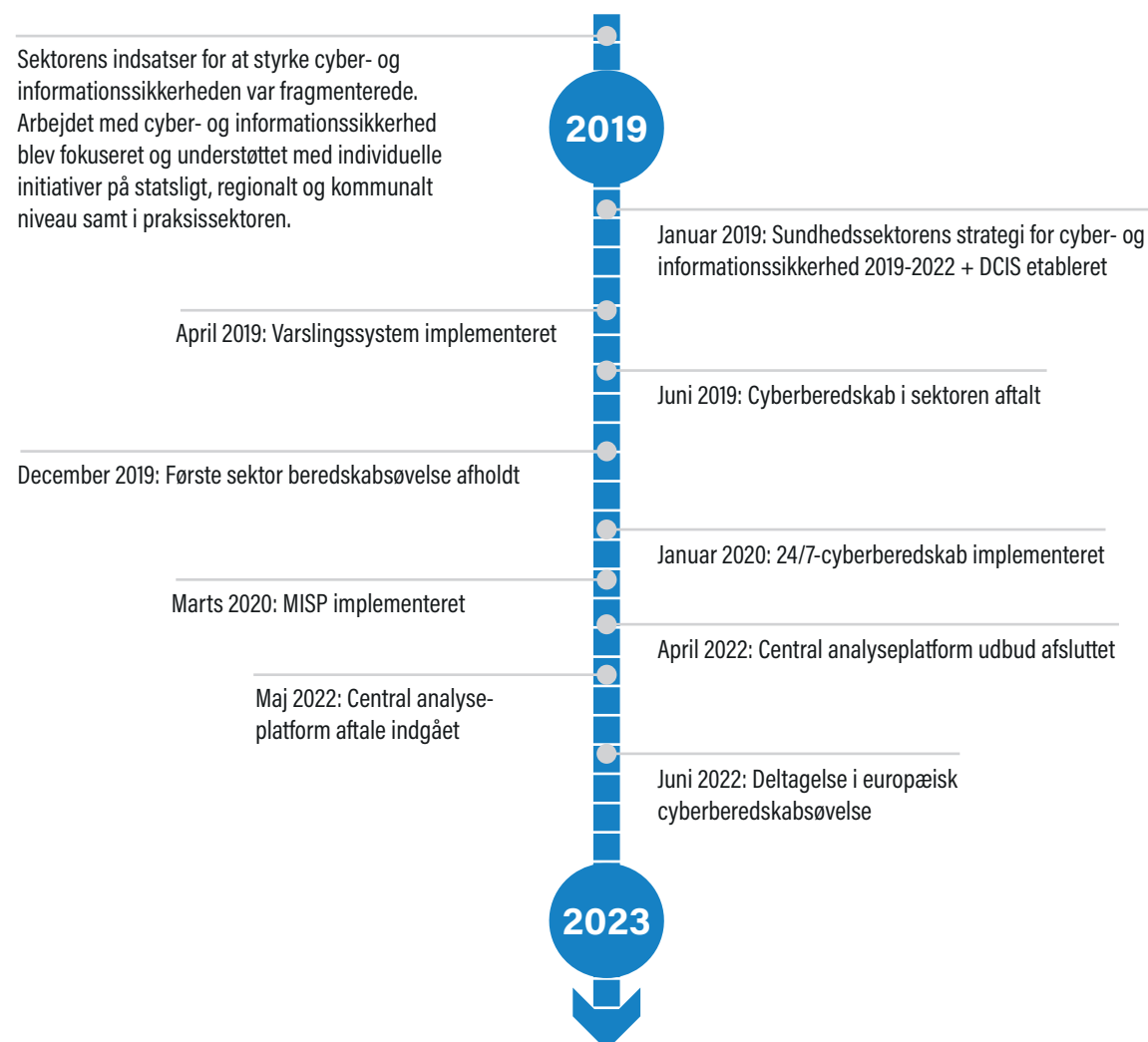
Strategien er baseret på en helhedsorienteret og risikobaseret tilgang til prioritering af strategiens initiativer. Strategiens indsatser holdes løbende op imod det aktuelle trusselsbillede, sektorens risikobillede og de kvartalsvise cybervejudsigter for sektoren. Herved sikres, at strategiens indsatser sætter ind der, hvor behovet og effekten er størst for sektoren som helhed

Strategien bygger på solide indsatser i sektoren

Strategien baseres på og understøtter sundhedssektorens eksisterende koordinering og samarbejde om cyber- og informationssikkerhed på tværs af sektorens aktører.

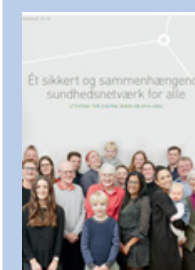
Cyber- og informationssikkerhed er ikke en ny opgave for sundhedssektoren. Sektorens aktører arbejder allerede med tiltag på de forskellige niveauer i sundhedssektoren: Fællesoffentligt, statsligt, imellem regionerne, kommunalt og i praksissektoren. Med den foregående sektorstrategi for cyber- og informationssikkerhed for 2019-2022 blev en del af indsatsen koordineret på tværs af aktørerne. Samarbejdet om

den fælles indsats for at styrke sundhedssektorens samlede kapacitet i forhold til cyber- og informationssikkerhed udbygges i denne strategiperiode, hvor strategien sigter mod at styrke det fælles fundament ved både at nå bredere ud til flere af sektorens aktører samt gå mere i dybden med de fælles sikkerhedsindsatser, sektoren allerede er sammen om.



Strategi for cyber- og informationssikkerhed 2023-2025 er desuden en del af et større strategilandskab på digitaliseringsområdet – ikke kun i sundhedssektoren men også tværoffentligt. Strategien sigter mod at understøtte indsatserne inden for cyber- og infor-

mationssikkerhed i disse strategier, hvor også flere af strategiens initiativer har samarbejdsflader op mod andre strategier. Nedenfor beskrives kort de forskellige tværoffentlige strategier med fokus på cyber- og informationssikkerhed.



Strategi for digital sundhed 2018-2024

Strategien indeholder tværgående digitale indsatser på sundhedsområdet, der skal bidrage til, at den enkelte oplever sundhedsvæsenet som ét sikkert og sammenhængende netværk.

Det digitale samarbejde om sundhed for hver enkelt borger skal styrkes gennem tillid og sikkerhed om data. Sundhedsvæsenets parter skal opnå et styrket fællesskab om cyber- og informationssikkerhed gennem en række fælles initiativer i sektorens strategi for cyber- og informationssikkerhed.

Strategi for life science 2021

Strategien sætter en vision for initiativsporet 'Bedre brug af sundhedsdata', hvor Danmark skal være internationalt førende i at anvende sundhedsdata til forskning, udvikling og offentlige myndighedsopgaver på en tidssvarende, innovativ og sikker måde.

Med udgangspunkt i visionen sætter strategien en række initiativer for blandt andet at udvikle en moderne og sikker datainfrastruktur til at imødekomme nye tekniske behov og muligheder inden for anvendelse af sundhedsdata. Cyber- og informationssikkerhed er en væsentlig faktor i realiseringen af disse initiativer for at sikre borgernes sundhedsdata.



Den fællesoffentlige digitaliseringsstrategi 2022-2025

Med strategien skal digitalisering være en central del af svaret på de store samfundsudfordringer, som Danmark står over for.

Samarbejdet om sikkerhedsindsatsen på tværs af den offentlige sektor skal fortsættes for at ruste sektoren til at håndtere digitale trusler og understøtte en god sikkerhedsadfærd hos borgere og virksomheder.

Aftale om sundhedsreformen 2022

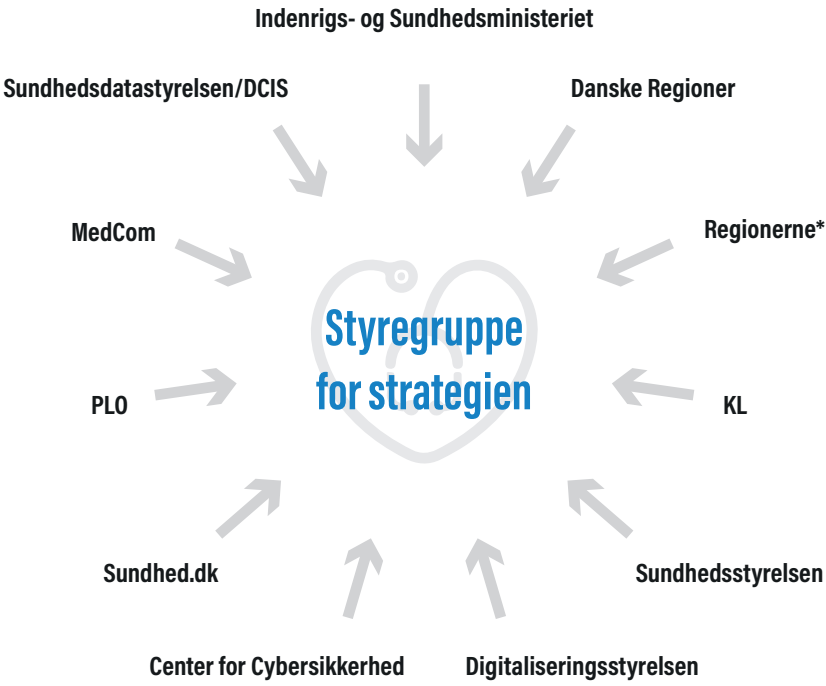
Folketingets partier har bl.a. aftalt en vision om mere behandling i eget hjem med digitale løsninger. Indsatsen skal ses i sammenhæng med omstillingen til det nære sundhedsvæsen samt øget datadeling for at sikre sammenhængende patientforløb. Sundhedssektorens cyber- og informationssikkerhedsstrategi understøtter disse indsatser blandt andet med initiativ om krav til it-leverandører samt initiativ om borgernært behandlingsudstyr og cybersikkerhed.



Governance og organisering

Sundhedssektorens aktører står i fællesskab bag sektorens strategi for cyber- og informationssikkerhed 2023-2025.

Strategien er forankret i Den nationale bestyrelse for sundheds-it, mens arbejdet med at udmønte strategien og følge op på denne og dens initiativer er placeret i styregruppen for Cyber- og informations-sikkerhed. Styregruppen er bredt repræsenteret af sektorens aktører. Styregruppen mødes fire gange årligt. Styregruppens formand afrapporterer to gange årligt til Den nationale bestyrelse for sundheds-it om fremdriften i arbejdet med at udmønte strategien.



**Region Hovedstaden, Region Midtjylland og Region Nordjylland*

 **Den decentrale cyber og informationssikkerhedsenhed**

Sundhedssektorens decentrale cyber- og informationssikkerhedsenhed (DCIS) er forankret i Sundhedsdatastyrelsen. Enheden er ansvarlig for udmøntningen af sektorstrategien for cyber- og informationssikkerhed i tæt samarbejde med sektorens aktører. Herudover har DCIS også en operationel kapacitet og koordinerer varsler og tværgående hændelser i sektoren. DCIS yder desuden rådgivning til sektorens aktører inden for beredskab, tekniske løsninger og andre områder inden for cyber- og informationssikkerhed.

Log4j samlede sundhedssektoren

Da Log4j-sårbarheden blev kendt i december 2021, viste sundhedssektorens hidtidige indsats inden for cyber- og informationssikkerhed sin værdi.

Log4j er en sikkerhedsmæssig sårbarhed i en softwarekomponent, der anvendes i en lang række it-systemer globalt. Log4J vurderes af mange it-sikkerhedseksperters som årtiets mest kritiske sårbarhed. Årsagen til, at den er så kritisk, er, at den er nem at udnytte og giver direkte adgang til at overtage kontrol med et givet system.

Da cyberberedskabet blev aktiveret, mødtes sundhedssektorens aktører på fælles statusmøder med +100 deltagere. Sektorens aktører samarbejdede på tværs og delte viden og knowhow. Uden denne ekstra indsats og det store samarbejde på tværs af hele sektoren kunne Log4j-sårbarheden hurtigt have eskaleret til en endnu større trussel for sundhedssektoren.



Bedre forudsigelse af potentielle angreb og hændelser

Sundhedssektorens samarbejde om at sikre sektorens evne til at forudsige mulige cyber- og informations-sikkerhedshændelser er en væsentlig forudsætning for, at sektoren som helhed og de enkelte aktører kan træffe de rette beslutninger om nødvendige sikkerhedstiltag.

INITIATIV 1.1

Vedligeholdelse af overblikket over sundhedssektorens samfundsvigtige funktioner og kritisk it-infrastruktur

Formål	Initiativet har til formål at vedligeholde og opdatere den løbende kortlægning af sektorens samfundsvigtige funktioner og understøttende kritiske it-infrastruktur.
Værdi	En vedligeholdelse af dette overblik bidrager til sektorens evne til at prioritere og fokusere indsatsen ved cyber- og informationssikkerhedshændelser.
Indhold	Initiativets vedligehold bygger videre på det nuværende overblik udarbejdet i strategiperioden 2019-2022. Overblikket vil fremover – i tråd med den nationale strategi for cyber- og informationssikkerhed 2022-2024 – fokusere på "samfundsvigtige funktioner", "kritisk infrastruktur" og "kritisk it-infrastruktur". På denne måde sikres også en ensartet tilgang til definition og kriterier for identifikation af kritisk it-infrastruktur. I vedligeholdelsen inddrages desuden resultatet af den nationale kortlægning af afhængigheder mellem infrastruktur i regi af initiativ 1.11 i den nationale strategi for cyber- og informationssikkerhed 2022-2024, hvor sundhedssektorens afhængigheder til kritisk infrastruktur i andre sektorer identificeres.

Resultater af sektorens samarbejde i strategiperioden 2019-2022

- ✓ Første fase af kortlægning af sektorens samfundsvigtige funktioner og kritisk it-infrastruktur med udgangspunkt i Net- og Informationssikkerhedsdirektivet (NIS) er udført
- ✓ Årlig trusselsvurdering for sundhedssektoren udarbejdes
- ✓ Årlig samlet sårbarheds- og risikovurdering for sektoren udarbejdes
- ✓ Sektoren deler uden forsinkelse varsler via vidensdelingsværktøjer (Malware Information Sharing Platform (MISP) og et varselsmailsystem)
- ✓ Etablering af et stærkt samarbejde med nordiske og internationale enheder giver vidensdeling fra andre landes sundhedssektorer til Danmark
- ✓ Kvartalsvise Cybervejrudsigter for sundhedssektoren, der giver ledelsesinformation og fremhæver de igangværende tendenser og trusler for sektoren inden for cybersikkerhed, udarbejdes

Overblik over sundhedssektorens tværgående og samlede risici

Formål	Sundhedssektorens samfundsvigtige funktioner understøttes af tætforbunden kritisk it-infrastruktur, og sektorens aktører udveksler samtidig løbende data og følsomme personoplysninger som led i behandlingen af borgerne. Initiativet har til formål at skabe et overblik over sektorens samlede risikobillede særligt i forhold til den tværgående kritiske it-infrastruktur og understøttende systemer, der benyttes af sektoren.
Værdi	Herved får sektoren mulighed for at prioritere indsatsen både lokalt men også på tværs af sektoren. De tætforbundne it-systemer og den gensidige afhængighed mellem sektorens aktører understreger vigtigheden i og værdien af et overblik over sektorens risici som helhed. Initiativet skal bidrage til, at sektoren samlet set kan mitigere og/eller på anden vis forebygge for de risici, som samlet eksponerer sektorens tværgående afhængigheder for uacceptable risici.
Indhold	For at skabe mest mulig værdi på tværs af sektoren og for de lokale aktører skal der i initiativet arbejdes med at forbedre metoden for indmeldelse af de lokale risikovurderinger til brug i udarbejdelsen af sektorens samlede risikovurdering. Fokus for metoden vil være samarbejde og vidensdeling mellem sektorens aktører for at berige et fælles overblik på tværs. De enkelte aktører udarbejder og opdaterer egne risikovurderinger. Sundhedssektorens trusselsbillede, der publiceres årligt af DCIS, kan anvendes i dette arbejde. Trusselsbilledet giver et grundlæggende overblik over aktuelle trusler og et indblik i trusselstendenser mod sundhedssektoren. Aktørernes sårbarheds- og risikovurderinger af den it-infrastruktur, der igennem initiativ 1.1 'Identifikation af sundhedssektorens samfundsvigtige funktioner og kritisk it-infrastruktur' identificeres som kritisk, skal som minimum være en del af aktørens samlede risikovurdering og dermed indgå i det samlede billede for sektoren.



Bedre mulighed for at forebygge angreb og hændelser

Effektiv forebyggelse af hændelser på tværs af en stor og kompleks sektor som sundhedssektoren er en omfangsrig og vedvarende indsats.

IIINITIATIV 2.1

Cyber- og informationssikkerhed på de sundhedsfaglige uddannelser

Formål	Sundhedssektorens medarbejdere håndterer hver dag store mængder sundhedsoplysninger digitalt. Sektorens store medarbejderkreds betyder desuden, at medarbejderne har forskellige forudsætninger for cyber- og informationssikkerhed. For at imødekomme disse forskellige forudsætninger og sikre et fælles basalt videns- og kompetenceniveau i sektoren har initiativet til formål at indføre cyber- og informationssikkerhed på alle de sundhedsfaglige uddannelser.
Værdi	Manglende opmærksomhed på cybersikkerhed er blandt de største sårbarheder i forbindelse med et muligt cyberangreb. Det er derfor vigtigt, at sundhedssektorens medarbejdere er bevidste om, hvordan de passer på sundhedsoplysningerne. Med indførelsen af cyber- og informationssikkerhed på de sundhedsfaglige uddannelser understøttes sektorens kommende sundhedspersonale i at indtænke gode vaner for cyber- og informationssikkerhed i deres daglige arbejdsgange.
Indhold	Der indgås fra centralt hold en dialog med relevante uddannelsesinstanser samt myndigheder, herunder blandt andet Uddannelses- og Forskningsstyrelsen samt Sundhedsstyrelsen, om at opbygge kapacitet og kompetencer inden for cyber- og informationssikkerhed hos de studerende på de sundhedsfaglige uddannelser. I arbejdet med initiativet kan der potentielt oprettes en arbejdsgruppe med deltagelse af sektorens aktører til idéudveksling og input til pensum til de sundhedsfaglige uddannelsesinstitutioner. Initiativet skal i relevant omfang koordineres med arbejdet i den fællesoffentlige digitaliseringsstrategi 2022-2025.

Resultater af sektorens samarbejde i strategiperioden 2019-2022

- ✓ Sektorens aktører bidrager aktivt til at styrke kompetencerne inden for cyber- og informationssikkerhed hos både sektorens sundhedspersonale og studerende på sundhedsfaglige uddannelser
- ✓ Et forum for erfaringsudveksling og vidensdeling inden for tekniske sikkerhedstiltag er etableret
- ✓ Revidering af sundhedssektorens referencearkitektur for informations-sikkerhed er gennemført

Rammer for rette og tidssvarende tekniske foranstaltninger

Formål	Initiativet har fokus på at dele viden om teknisk sikring af kritisk it-infrastruktur og styrke de tekniske cyber- og informationssikkerhedskompetencer i sundhedssektoren. Målet er at udnytte den eksisterende viden i sektoren omkring sikring af it-infrastruktur til at opstille vejledninger og rammer for rette og tidssvarende tekniske foranstaltninger.
Værdi	Dette initiativ vil give aktørerne mulighed for at udnytte hinandens viden og samlet styrke kapaciteten på tværs af sektoren og hos den enkelte aktør.
Indhold	Sektorens aktører skal i fællesskab løbende prioritere fokusområderne for vidensdeling og rammesætning baseret på det aktuelle trusselsbillede samt på sektorens risikovurderinger, så sikkerhedstiltagene prioriteres i forhold til de væsentligste risici for sektoren. Arbejdet med revidering af sundhedssektorens referencearkitektur i initiativ 2.6 'Udbygning af sektorens sikkerhedsarkitektur' affødte i den seneste strategiperiode blandt andet ønske om, at der sikres en fælles forståelse og best practice på tværs af sektoren af hvordan og hvornår, man bør kryptere.

Kortlægning af legacy-systemer i kritisk it-infrastruktur

Formål	En del af sundhedssektorens it-infrastruktur udgøres af legacy-systemer, hvor leverandøren eller udvikleren ikke længere opdaterer på softwaren i systemet eller kommer med sikkerhedsopdateringer, og/eller som afvikles på en platform, der benytter usupporterede operativsystemer. Disse udgør en risiko og kan være sårbare over for potentielle cyberangreb. Initiativet har derfor til formål at kortlægge legacy-systemer i sektorens kritiske it-infrastruktur.
Værdi	Legacy-systemer bør håndteres gennem mitigerende foranstaltninger. Gennem en kortlægning af de af sektorens legacy-systemer, som udgør kritisk it-infrastruktur, vil aktørerne bedre kunne prioritere indsatsen og fokusere på håndtering af de mest kritiske systemer først.
Indhold	Sektorens aktører skal udbygge kortlægningen af legacy-systemer fra den forgangne strategiperiode, hvor sektoren har kortlagt legacy-systemer baseret på den hidtidige kortlægning af kritiske systemer i regi af strategiens initiativ 1.1. Udbygningen af kortlægningen af legacy-systemer baseres ligeledes på den it-infrastruktur, der er vurderet kritisk i regi af initiativ 1.1 'Identifikation af sundhedssektorens samfundsvigtige funktioner og kritisk it-infrastruktur'. Initiativet indeholder ikke aktiviteter eller eventuel finansiering til udbedring af udfordringer på dette område. Kortlægningen vil via vidensdeling kunne bruges til at tilføje andre aktørers mitigerende foranstaltninger til aktørernes egne værktøjskasser.

Katalog over eksisterende sikkerhedskrav til it-leverandører

Formål	For at styrke og målrette indsatsen for at gøre sektoren mere robust har initiativet til formål at sikre, at private og offentlige it-leverandører mødes af ensartede sikkerhedskrav fra sektorens aktører.
Værdi	Arbejdet med at sikre, at leverandørernes arbejde med at opretholde et passende sikkerhedsniveau, bliver gjort lettere for både sektorens aktører og sektorens leverandører ved at samle et katalog med de krav og anbefalinger, både i nationalt og internationalt regi, der er relevante for at højne sektorens sikkerhed.
Indhold	I et samarbejde mellem sektorens aktører og DCIS skal der desuden udarbejdes en plan for udbredelse af kendskabet til kataloget hos sektorens aktører og it-leverandører, herunder også ved opdateringer af nye gældende krav.

Udbygning af sektorens sikkerhedsarkitektur

Formål	Initiativet skal bidrage til, at der på tværs af sundhedssektoren arbejdes mere ensartet med it-sikkerhedsmæssige krav i forbindelse med videreudvikling af eksisterende systemer eller nyanskaffelser.
Værdi	Initiativet skal understøtte sektorens arbejde med at skabe sikre rammer for behandling af borgerne og deres følsomme personoplysninger.
Indhold	Sektorens aktører har revideret referencearkitekturen for informationssikkerhed i den seneste strategiperiode. Igennem dette arbejde blev byggeblokke for den fælles infrastruktur fra Strategi for digital sundhed 2018-2024 introduceret. For at understøtte ensartede it-sikkerhedsmæssige standarder og krav hen mod en fælles arkitekturforståelse på tværs af sektoren, skal der i den kommende strategiperiode arbejdes videre med at definere en del af de byggeblokke, der er relevante for informationssikkerhedsområdet. Initiativet koordineres med den fællesoffentlige og den fælleskommunale rammearkitektur. Det fælles videre arbejde fortsætter i regi af initiativets arbejdsgruppe for sikkerhedsarkitektur. Initiativet skal i relevant omfang koordineres med arbejdet i den fællesoffentlige digitaliseringsstrategi 2022-2025.



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 ensartes 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.



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.

Cybersikkerhed hos de mindre aktører

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.

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.

 **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 databehandleraftale mellem den dataansvarlige og databehandleren, som lever op til kravene i databeskyttelsesforordningen.

Bedre mulighed for at opdage angreb og hændelser

Cyber- og informationssikkerhed er under konstant udvikling, og sundhedssektorens kapacitet til at opdage angreb og hændelser, som er under opsejling, skal følge med udviklingen.

INITIATIV 3.1

Fælles rammer og værktøjer til understøttelse af aktørernes løbende test af cybersikkerheden

Formål	For at bidrage til robustheden over for cyber- og informationssikkerhedshændelser for sundhedssektoren samlet set bygger initiativet oven på indsatsen fra den forgangne strategiperiode ved at udvide den nuværende sikkerhedstestportefølje for sektorens systemer og udstyr.
Værdi	Med en fælles testportefølje skabes gode fælles rammer i sektoren for at understøtte de lokale indsatser inden for cyber- og informationssikkerhed. Ligeledes udgør samarbejdet om en fælles testportefølje et godt grundlag for vidensdeling på tværs af sektoren.
Indhold	Sektorens aktører skal afklare behovet og mulighederne for at tilføje yderligere testværktøjer eller rammeaftaler til testporteføljen. Afklaringen heraf skal tage afsæt i det aktuelle trusselsbillede og sektorens risikovurdering, så indsatsen prioriteres i forhold til de væsentligste risici.

Sundhedsdatanettet (SDN)

Sundhedsdatanettet er et sikret netværk til datakommunikation mellem både offentlige og private aktører i sundhedssektoren. SDN binder lokale, sikrede net sammen i en fælles it-infrastruktur. Netværket anvendes blandt andet af sundhed.dk, Fælles Medicinkort (FMK) og en række tværsektorielle og tværregionale løsninger.

Resultater af sektorens samarbejde i strategiperioden 2019-2022

- ✓ Sundhedssektorens centrale analysecenter (SAC) er etableret, og regionernes respektive Security Operations Centers (SOC) er tilsluttet
- ✓ Opbygning af service der kan sårbarhedsscanne Sundhedsdatanettet (SDN)
- ✓ Opbygning og udbredelse af et værktøj, der scanner de af sundhedssektorens løsninger, der er vendt mod internettet, og rapporterer, hvor en cyberkriminell vil kunne angribe
- ✓ Månedlige vidensdelingsfora til teknisk sparring med sektorens aktører er etableret

Udbredelse af overvågnings- og analysefunktioner på tværs af sektoren

Formål	For at styrke sundhedssektorens samlede kapacitet og evne til at opdage uvedkommende aktivitet og cyberhændelser på tværs af sektorens aktører udbredes en overvågnings- og analyseplatform til sundhedssektorens aktører. Den centrale del af platformen (SAC) udfører tværgående overvågning af systemer og netværk i sundhedssektoren og gennemfører analyser på baggrund af denne overvågning.
Værdi	Sundhedssektorens analyseplatform tilføres tværgående informationer om cyberaktiviteter, til gavn for sektorens tilsluttede aktører, der understøttes i deres prioritering af håndtering af aktiviteter på eget netværk. Derudover bliver platformen et operativt omdrejningspunkt for samarbejdet om cyber- og informationssikkerhed på tværs af sektorens aktører, hvor aktørerne kan udnytte hinandens styrker og skabe synergier på tværs.
Indhold	Arbejdet med at udbrede overvågning- og analysefunktionens platform til flere af sektorens aktører videreføres i denne strategiperiode. Fokus vil være på at skabe så bred dækningsgrad som muligt og få mest mulig synergi ud af udbredelsen på tværs af sektoren, også til aktører der ikke er direkte med på platformen. Regionerne fortsætter brugen af platformen og kan udvide antallet af appliances, udover det der er dækket centralt, hvis de selv vurderer, at det er tjenstværdigt. Kommunerne afklarer i strategiperioden, hvordan de kan organisere sig i forhold til den centrale del af platformen (SAC-funktionen) samt tilslutning til denne. De specifikke rammer aftales i forbindelse med udmøntningen. De praktiserende læger afklarer ligeledes i strategiperioden, hvordan de kan organisere sig i forhold til den centrale del af platformen (SAC-funktionen) samt tilslutning til denne. De specifikke rammer aftales i forbindelse med udmøntningen. Aktører i sundhedssektoren kan frivilligt og ved selvfinansiering tilslutte sig til den centrale platform og samarbejdet efter aftale med Sundhedsdatastyrelsen.

 **Langt fra alle sårbarheder bliver udnyttet**

En sårbarhed er en fejl eller uhensigtsmæssighed i software, servere og systemer, som en cyberkriminell kan udnytte.

Man kender ikke til alle sårbarheder, og ud af det samlede antal sårbarheder, man faktisk kender til, udnytter de cyberkriminelle kun 5,5 %. Det betyder, at de cyberkriminelle potentielt har mulighed for at udnytte mange flere sårbarheder til at angribe organisationers it-systemer.

Det centrale analysecenter for cyber- og informationssikkerhed i sundhedssektoren

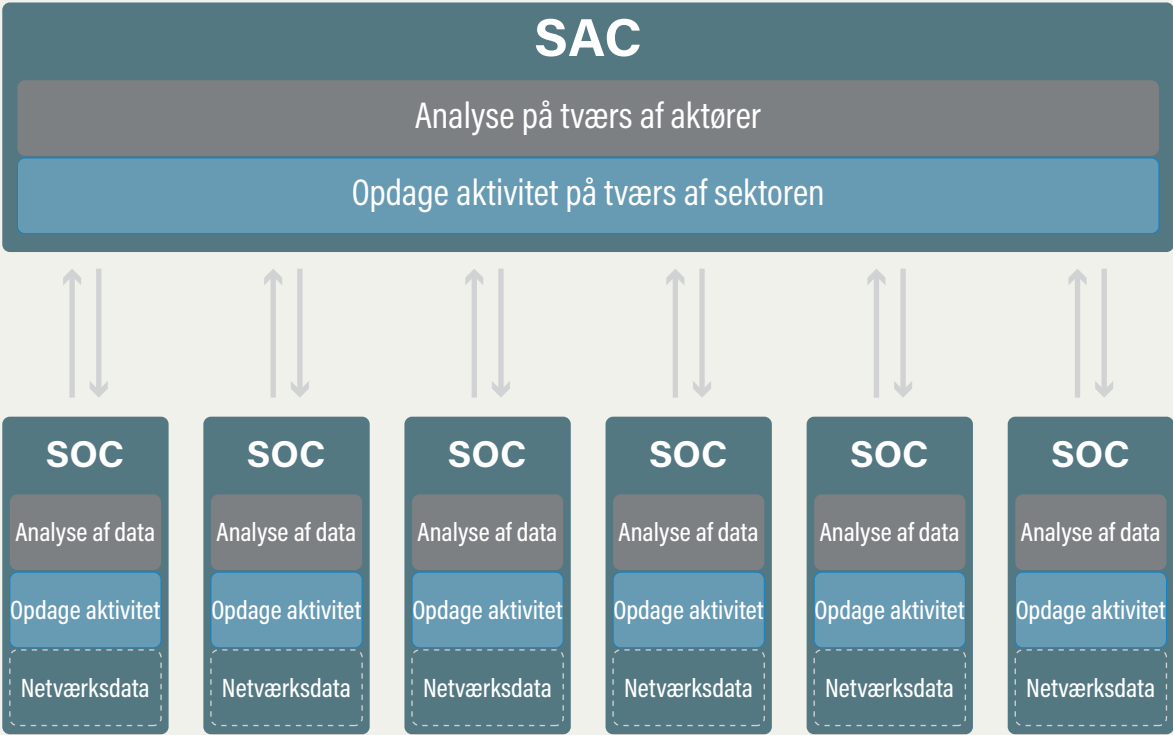
Overvågning og analyse af aktivitet udgør en vigtig del af den fælles modstandsdygtighed mod angreb og sikkerhændelser i sektoren. Med etableringen af sundhedssektorens centrale analysecenter (SAC) har sektorens aktører iværksat et samarbejde på tværs, der vil agere krumtap for mange af aktiviteterne i det videre arbejde med cyber- og informationssikkerhed i sundhedssektoren. Samarbejdet omkring og den viden, det centrale analysecenter og de tilsluttede aktører opbygger, er med til markant at øge muligheden for at opdage cyberhændelser på tværs af sektoren og dermed øge den generelle robusthed i sektoren.

operativt samarbejde på tværs af sektoren mellem de operative enheder hos aktørerne. Disse enheder kaldes for Security Operations Centre (SOC). Viden og læring fra dette samarbejde vil også komme resten af sundhedssektoren til gode gennem andre etablerede vidensdelingsværktøjer.

Det centrale analysecenter er placeret hos den decentrale cyber- og informationssikkerhedsenhed (DCIS) i Sundhedsdatastyrelsen.

Når der ses tværgående trusler i sektoren, får de lokale SOC-enheder besked. Herved kan aktørerne prioritere og hurtigt sætte ind for at håndtere aktiviteten lokalt.

Samtidig med den tekniske etablering og udbredelse af platformen opbygges et dagligt teknisk og



Hurtig håndtering i tilfælde af angreb og hændelser

I tilfælde af et angreb eller en større hændelse i sundhedssektoren skal sektoren hurtigt kunne genoprette systemer og de samfundsvigtige funktioner.

INITIATIV 4.3

Udbredelse af beredskabsøvelser for fælles systemer og forsyningskæder

Formål	I tilfælde af en tværgående cybersikkerhedshændelse i sundhedssektoren skal sektorens aktører være i stand til at reagere koordineret og effektivt. Formålet med initiativet er at øge initiativets dækningsgrad således, at flere af sektorens aktører og, hvor muligt, deres leverandører deltager i sektorens fælles beredskabsøvelser.
Værdi	Gennem fælles beredskabsøvelser styrkes sektorens samlede evne til på effektiv vis at håndtere cyber- og informationssikkerhedshændelser. Dette giver værdi i det tilfælde, at en sådan hændelse rammer et fælles system. Samtidig øges muligheden for samarbejde på tværs af sektoren, hvis en enkel aktør bliver ramt af en større cyberhændelse. Større bredde i øvelsesscenarierne vil desuden give flere aktører en struktureret tilgang til at sikre, at de får testet eget it-beredskab.
Indhold	Sektorens samarbejde om it- og cyberhændelser afprøves gennem årlige fælles beredskabsøvelser. Initiativet skal desuden fokusere på at skabe en så bred dækningsgrad som muligt og få mest mulig synergi ud af samarbejdet og vidensdeling om cyberhændelser på tværs af sektoren.

Resultater af sektorens samarbejde i strategiperioden 2019-2022

- ✓ Et fælles cyberberedskab til håndtering af tværgående hændelser i sundhedssektoren er etableret
- ✓ Cyberberedskabet understøttes af en vagttelefon, der kan kontaktes 24/7 for rådgivning, anmodning om assistance eller et situationsoverblik
- ✓ DCIS, regionerne og MedCom har etableret dedikeret og redundant kommunikation i forbindelse med cyberberedskabet i form af SI-NE-radioer
- ✓ Sektoren afholder årligt en cyberberedskabsøvelse
- ✓ Deltagelse i europæisk cyberberedskabsøvelse på tværs af sundhedssektorerne i EU's medlemslande
- ✓ Et velfungerende samarbejdsforum med regionerne og kommuner er etableret. Månedlige statusmøder afholdes, hvor der deles viden om sårbarheder og løsninger til håndtering af disse



**SUNDHEDSDATA-
STYRELSEN**



**INDENRIGS- OG
SUNDHEDSMINISTERIET**



**DANSKE
REGIONER**

Strategi for cyber- og informationssikkerhed i sundhedssektoren
2023-2025