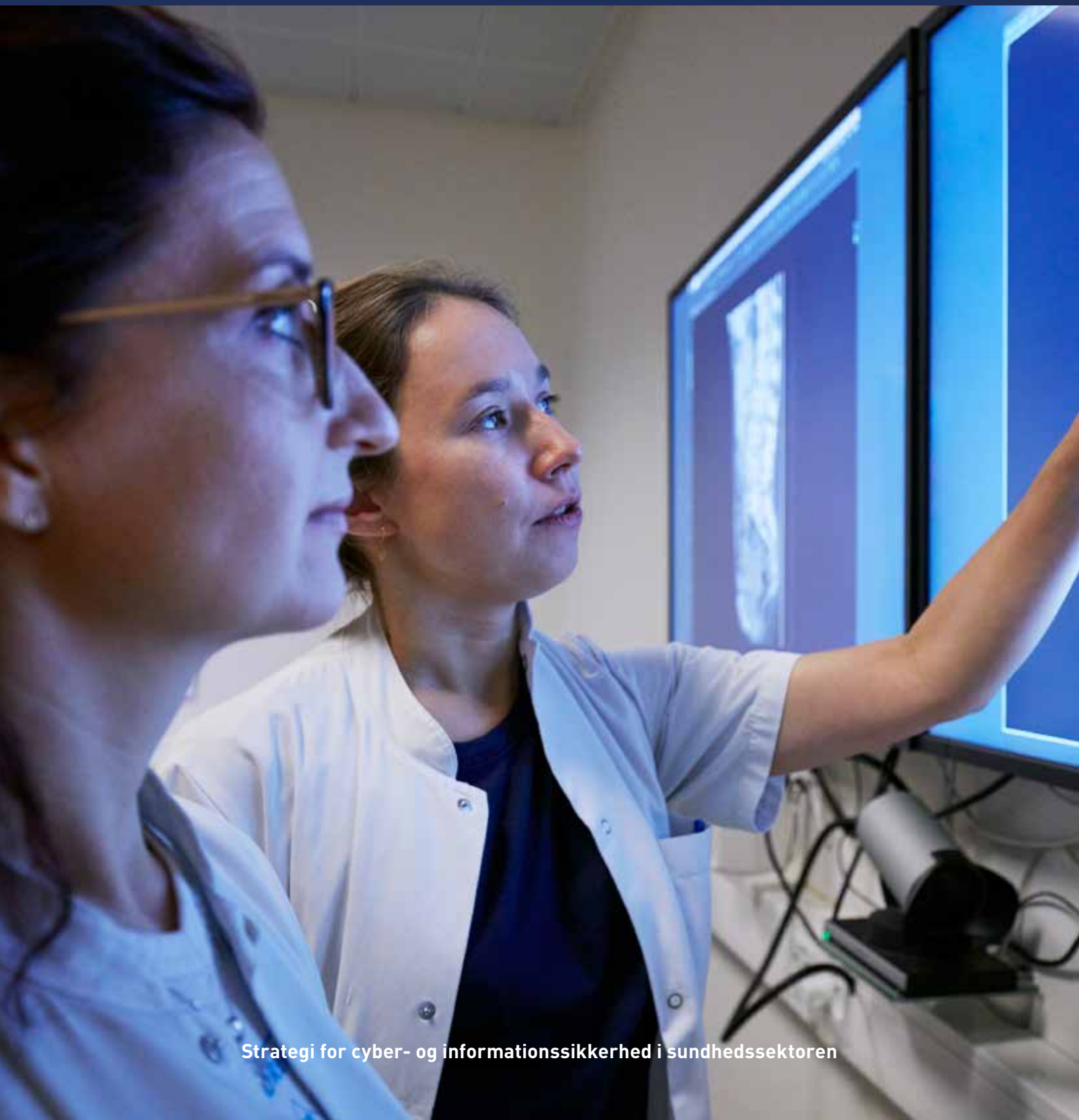
STRATEGI 2019-2022

En styrket, fælles indsats for cyber- og informationssikkerhed



Strategi for cyber- og informationssikkerhed i sundhedssektoren

Indhold

Øget tryghed i et digitaliseret sundhedsvæsen

Sikkerhed har altid været en central opgave for sundhedsvæsenet. Sundhedsvæsenet er sat i verden for at sikre borgernes liv og helbred. En grundlæggende forudsætning er, at behandling og pleje finder sted i trygge og sikre rammer. Sikkerhed er således allerede en integreret del af hverdagen i det danske sundhedsvæsen.

I takt med at digitale løsninger spiller en stadig større rolle i vores sundhedsvæsen, handler trygge og sikre rammer også om stærk cyber- og informationssikkerhed. Med digitale værktøjer vil vi kunne tilbyde borgere og pårørende et trygt, tilgængeligt og sammenhængende sundhedsvæsen. Et sundhedsvæsen hvor borgeren let kan komme i kontakt med egen læge og sygehuset, hvor alle relevante oplysninger følger borgeren gennem behandlingsforløb på tværs af sundhedsvæsenet, og hvor behandling og pleje kan ske tættere på borgeren. Fordelene er mange. Det danske sundhedsvæsen er allerede blandt de mest digitaliserede i verden, og potentialet er fortsat stort.

Det danske sundhedsvæsen er allerede blandt de mest digitaliserede i verden, og potentialet er fortsat stort.

Med digitaliseringen følger dog også nye udfordringer. Efterhånden som personer og udstyr på regionale sygehuse, i kommunal pleje, på praksisområdet og hos andre sundhedsaktører bliver stadig mere forbundne, stiger kompleksiteten i systemerne og dermed sundhedsvæsenets sårbarhed over for blandt andet cyberangreb også. Truslerne er mangeartede og i konstant udvikling. Det er en udfordring, vi tager meget alvorligt. Med de mange igangværende cyber- og informationssikkerhedsindsatser ude i de enkelte dele af sundhedsvæsenet har vi et stærkt udgangspunkt for at løfte hele sektoren samlet.

Borgernes forhold til sundhedsvæsenet hviler på et fundament af tillid. Tillid til at der bliver stillet den rette diagnose. Tillid til at borgeren får den rigtige behandling og pleje. Og ikke mindst tillid til at sundhedsvæsenet passer godt på de følsomme personoplysninger, som borgerne afleverer til sundhedsvæsenet i forbindelse med et behandlingsforløb. Det er afgørende at fastholde borgernes tillid. Både borgere og sundhedsprofessionelle skal fortsat kunne stole på, at oplysninger opbevares forsvarligt og sikkert, at de relevante oplysninger kan tilgås, når det er nødvendigt for behandlingen, og ikke mindst at de er korrekte, så behandlingen sker på rette grundlag.

Et sammenhængende sundhedsvæsen kræver også øget sammenhæng i forhold til cyber- og informationssikkerhed. Det er vigtigt, at vi løfter i flok. Det er nødvendigt for at kunne høste frugterne af den fortsatte digitalisering. Et højt, fælles cyber- og informationssikkerhedsniveau er et afgørende element i arbejdet med at fremtidssikre vores sundhedsvæsen.

Med denne strategi vil vi styrke den fælles, koordinerede indsats på området yderligere. Vi ønsker at sætte en fælles dagsorden og retning for sundhedsvæsenets videre arbejde med cyber- og informationssikkerhed. Sammen påbegynder vi således en fælles rejse, men endemålet er ikke givet med strategien alene. Det er en rejse, der indebærer, at sundhedssektorens parter i fællesskab løbende i strategiperioden prioriterer aktiviteter og aftaler finansiering heraf. Med strategien tager vi de første fælles skridt.

POLITISK CYBERFORUM FOR SUNDHEDSSEKTOREN

Ellen Trane Nørby Sundhedsminister

Jette Skive Formand for KL's Sundheds- og Ældreudvalg

Stephanie Lose Formand for Danske Regioner

En styrket, fælles indsats

Sundhedssektoren er en samfundskritisk sektor i Danmark. Tusindvis af borgere er hver dag i berøring med sundhedsvæsenet, og for mange er det kritisk, at sundhedssektorens aktører kan levere rettidig behandling og pleje. Derfor er det vigtigt, at sektoren kan sikre, at den rette behandling og pleje er tilgængelig for borgerne, når de behøver den.

Den danske sundhedssektor er i dag kendetegnet af stigende digitalisering. Hver dag håndteres store mængder sundhedsoplysninger digitalt på tværs af mange behandlingsenheder. Sektorens aktører arbejder i retning af stadig mere samarbejde om behandling og pleje ved hjælp af digital udveksling af informationer, for at borgerens vej gennem sundhedsvæsenet opleves så tryg og sømløs som muligt. Dermed stiger afhængigheden af digital infrastruktur og dataudveksling på tværs.

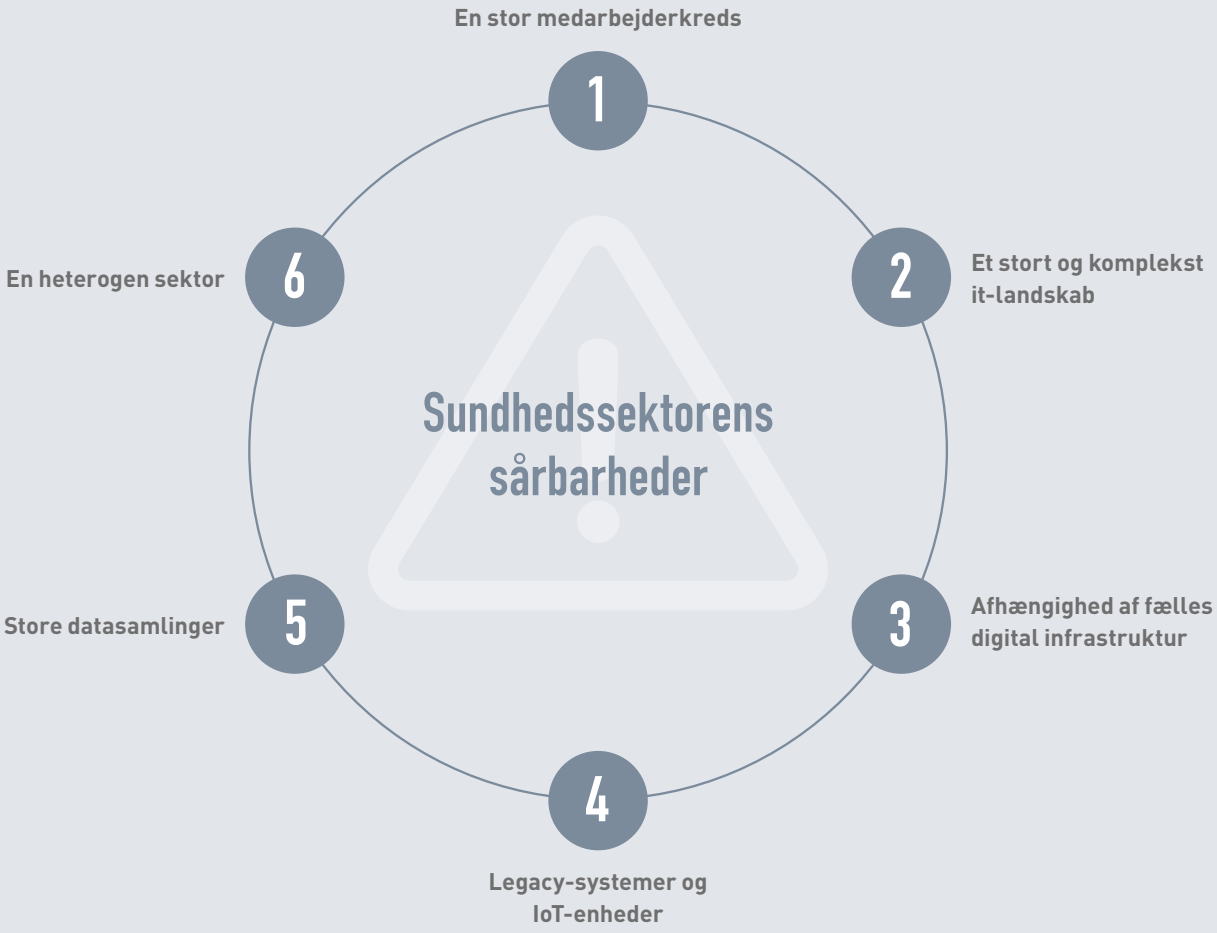
Digitaliseringen har mange fordele. De mange forbundne enheder og aktører og de store mængder følsomme personoplysninger gør dog også sundhedssektoren sårbar over for cyber- og informationssikkerhedshændelser – som fx et potentielt cyberangreb. Derfor er det nødvendigt med en styrket, fælles cyber- og informationssikkerhedsindsats for at sikre den fortsatte behandling og pleje af borgerne og beskytte deres følsomme personoplysninger.

Sundhedssektoren består af mange forskellige aktører, der er forskelligt organiseret og drevet; fra store, regionale sygehuse med højt specialiseret behandling og kommunale enheder for opfølgning og pleje til mindre lægepraksisser, klinikker og apoteker. Hovedparten af sektoren er offentligt drevet, men en lang række mindre aktører – fx praktiserende læger, speciallæger, fysioterapeuter, tandlæger mfl. – er selvstændige erhvervsdrivende.

Derudover rummer sektorens portefølje af it-systemer en udpræget kompleksitet, der håndteres forskelligt; fra store systemlandskaber i regionerne med tusindvis af brugere og understøttet af nogle af landets største it-afdelinger til små systemer i praksissektoren med få brugere. Hertil kommer udfordringer med legacy-systemer og IoT-enheder med varierende sikkerhedsniveau – som det også ses i andre samfundskritiske sektorer. Udskiftning er ofte ikke mulig eller hensigtsmæssig, da kritisk behandling afhænger af brugen af et bestemt apparatur. Endelig benytter sundhedssektoren sig af mange leverandører af både it-systemer og infrastruktur. Sikkerhed og stabilitet er derfor væsentlige faktorer i brugen af eksterne leverandører i sektoren. Det øger behovet for fælles basiskrav til styring og opfølgning på leverandørernes sikkerhed.

FIGUR

Seks overordnede sårbarheder



1. En stor medarbejderkreds
Sektoren har flere hundredetusinde medarbejdere med vidt forskellig forudsætninger for cyber- og informationssikkerhed.

2. Et stort og komplekst it-landskab
Sektoren er bundet sammen af et stort og komplekst landskab af systemer, der behandler personhenførbare oplysninger, hvilket gør arbejdet med cyber- og informationssikkerhed til en kompleks og omfangsrig opgave.

3. Afhængighed af fælles digital infrastruktur
Sektoren er tæt digitalt forbundet gennem bl.a. Sundhedsdatanettet, som bruges til udveksling af patientdata mv. Manglende tilgængelighed, integritet og fortrolighed kan have store konsekvenser for sektoren og ikke mindst borgerne.

4. Legacy-systemer og IoT-enheder
Kritisk medicinsk udstyr kan være forbundet til legacy-systemer, som ikke nødvendigvis har et tilstrækkeligt sikkerhedsniveau, men ikke kan udskiftes. Samtidig er antallet af meget forskelligartede IoT-enheder stigende i sektoren.

5. Store datasamlinger
I patientjournaler, nationale registre og kliniske kvalitetsdatabaser opbevares store mængder af data om aktiviteten i sundhedsvæsenet, som det er væsentligt at opretholde tilgængeligheden, integriteten og fortroligheden af.

6. En heterogen sektor
Sektoren rummer aktører med forskellige modenhedsniveauer ift. cyber- og informationssikkerhed – lige fra store, højtspecialiserede sygehuse med tusindvis af ansatte til små, private lægeklinikker med få ansatte.

Cyber- og informationssikkerhed handler ikke kun om teknologi, men i lige så høj grad om mennesker. En stærk sikkerhedsindsats stiller også krav til medarbejdernes viden og kompetencer. Sundhedssektorens mange tusinde medarbejdere har vidt forskellige forudsætninger, når det kommer til cyber- og informationssikkerhed. Derfor er der også behov for en målrettet indsats i forhold til sektorens mange forskellige faggrupper med henblik på at understøtte et fælles, højt videns- og kompetenceniveau vedrørende cyber- og informationssikkerhed og en robust sikkerhedskultur på tværs af sundhedssektorens aktører.

Cyber- og informationssikkerhed handler ikke kun om teknologi, men i lige så høj grad om mennesker.

Udfordringerne forbundet med cyber- og informationssikkerhed er både mangeartede og omskiftelige. Formålet med sundhedssektorens strategi er at understøtte et samlet sikkerhedsløft i sektoren, således at sektorens kapacitet til at forudse, forebygge, opdage og håndtere cyber- og informationssikkerhedshændelser styrkes. Det kræver en helhedsorienteret indsats og tværgående koordinering samt et højt, fælles sikkerhedsniveau på tværs af sektorens aktører.

En væsentlig komponent i en helhedsorienteret indsats er, at den er risikobaseret. Sundhedssektoren er en samfundskritisk sektor, men det er ikke alle processer og it-systemer, der er lige kritiske for sektoren som helhed. Sikkerheden i sektoren som helhed skal hæves til et niveau, der står mål med risikoen for cyber- og informationssikkerhedshændelser under hensyntagen til sundhedsområdets overordnede produktivitet, kvalitet og krav om tilgængelighed. Det er nødvendigt at vurdere, hvor risiciene er størst, og hvor en potentiel sikkerhedshændelse ville være mest kritisk med henblik på at prioritere sikkerhedstiltagene i forhold til de væsentligste risici.

Dette skal bidrage til at sikre en helhedsorienteret indsats på tværs af hele sektoren. Det er også helt centralt, at der er balance mellem håndteringen af de enkelte risici og hensynet til den almindelige behandling og pleje. I sidste ende skal sikkerhedstiltagene netop understøtte kvaliteten i behandlingen og plejen og borgernes tillid til den.

FAKTA

Cybersikkerhed og informationssikkerhed. To størrelser, men kun ét sigte:

INFORMATIONSSIKKERHED

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

CYBERSIKKERHED

Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.

TRYGHED FOR BORGEREN

Alene en indsats der tager udgangspunkt i både cyber- og informationssikkerhed kan skabe et grundlag, hvor den enkelte borger kan føle tryghed i forhold til sin behandling og sine sundhedsdata.

Sektoren har ansvar for at opretholde sikkerheden omkring borgerens behandling og sundhedsdata, således at fortrolighed, integritet og tilgængelighed bevares

I den nationale strategi for cyber- og informationssikkerhed lægges der vægt på, at fordelingen af ansvaret for arbejdet med cyber- og informationssikkerhed i Danmark bygger på sektoransvarsprincippet: Den myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret i forbindelse med konkrete cyber- og informationssikkerhedshændelser. Ansvaret for cyber- og informationssikkerhed i sundhedssektoren ligger således hos sundhedssektorens aktører ved konkrete hændelser.

Alle i vores sektor værner om borgerne og deres sundhedsdata

Cyber- og informationssikkerhed er ikke en ny opgave for sundhedssektoren. Strategien bygger oven på et godt fundament blandt sektorens aktører for at styrke den fælles indsats i sektoren yderligere.

Den øgede opmærksomhed på cyber- og informationssikkerhed kommer til udtryk i en række tiltag på de forskellige niveauer i sundhedssektoren:

På **fællesoffentligt** niveau har regeringen, Danske Regioner og KL med ønsket om at skabe en fælles, overordnet forståelse for udviklingen af trusler mod sundhedssektoren nedsat et politisk cyberforum med deltagelse af sundhedsministeren, formanden for Danske Regioner samt formanden for KL's Sundheds- og Ældreudvalg. Forummet har til formål at drøfte politiske hensyn og afvejninger med hensyn til cyber- og informationssikkerhed og sikre gensidig orientering, erfaringsdeling og videnopbygning for at styrke samarbejdet om cyber- og informationssikkerhed i sundhedssektoren.

På **statsligt** niveau arbejdes der i Sundheds- og Ældreministeriets koncern systematisk med styrket cyber- og informationssikkerhed, bl.a. med gennemførelsen af awareness-kampagner, certificering af medarbejdere samt løbende sikkerhedstests og beredskabsøvelser. Desuden er der lagt vægt på et højt cyber- og informationssikkerhedsniveau i forbindelse med etableringen af Nationalt Genom Center og etableringen af Sundhedsdataplatformen, der skal understøtte Sundhedsdatastyrelsens nuværende og fremtidige behov for modtagelse, opbevaring og levering af sundhedsdata. Blandt andet behandles data altid i pseudonymiseret form, så data ikke umiddelbart kan føres tilbage til en identificerbar, fysisk person.

Regionerne har bl.a. udarbejdet en politisk linje for informationssikkerhed som en del af det regionale udspil Sundhedsdata i spil. I forlængelse af den politiske linje har regionerne godkendt en fællesregional informationssikkerhedspolitik, som understøtter, at de følger ISO 27001. Dertil har regionerne udarbejdet et tværregionalt pejlemærke for informationssikkerhed, der støtter op om implementeringen af den politiske linje og sikrer en fælles tilgang til indsatsen for informationssikkerhed og databeskyttelse i regionerne. Arbejdet med pejlemærkets tværregionale leverancer har været med til yderligere at styrke arbejdet og højne det faglige niveau i den enkelte region; bl.a. gennem fælles rammer, retningslinjer og sparring. Der er i forlængelse af pejlemærket nedsat en permanent,

tværregional styregruppe for informationssikkerhed. Parallelt hermed arbejder hver enkelt region med at sikre, at informationssikkerhed vedvarende er en integreret del af de ydelser, der leveres til borgere, patienter, virksomheder, samarbejdspartnere mfl.

På det **kommunale** område har man som led i den fælleskommunale digitaliseringsstrategi etableret Sikkerhedsprogrammet, der skal understøtte kommunernes arbejde med at øge sikkerheden for alle områder i kommunerne, herunder implementeringen af principperne i ISO 27001 og udvikling af elementer til kommunernes fælles rammearkitektur med fokus på datasikkerhed. Dertil skal programmet understøtte øget opmærksomhed på datasikkerhed blandt ledere såvel som medarbejdere i kommunerne. For at støtte op om og sikre et kontinuerligt fokus på informationssikkerhed i de enkelte kommuner gennemfører KL frem mod 2020 en årlig analyse af kommunernes modenhedsniveau på sikkerhedsområdet. Dette har ført til viden om, hvilke områder der med størst fordel kan arbejdes med i fællesskab, således at KL kan støtte kommunernes arbejde. Analysens resultater har bl.a. affødt, at der i højere grad end tidligere i de enkelte kommuner afsættes midler til at højne bevidstheden om informationssikkerhed blandt de ansatte. Dertil har analysen bidraget til en øget kompetenceopbygning i kommunernes informationssikkerhed og tilknyttede juridiske funktioner.

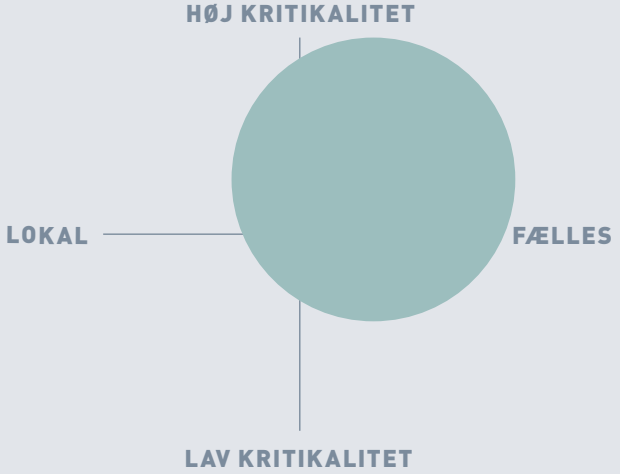
For **praksissektoren** understøtter Praktiserende Lægers Organisation (PLO) en generelt øget opmærksomhed på informationssikkerhed blandt læger i almen praksis, hvor PLO i 2017 har udarbejdet informationsmateriale vedrørende sektorens juridiske ansvar samt vejledning i relevant sikkerhedsadfærd i forhold til beskyttelse af systemer og persondata. Dette arbejde er i 2018 fulgt op af informationstiltag rettet direkte mod landets alment praktiserende læger.

Strategien skal sikre, at sektorens cyber- og informationssikkerhed koordineres og samstemmes på tværs af sundhedsområdets aktører.

Med udgangspunkt i den eksisterende indsats skal strategien styrke sektorens samlede kapacitet i forhold til cyber- og informationssikkerhed. Strategien skal sikre, at sundhedssektorens cyber- og informationssikkerhedsindsats koordineres og samstemmes på tværs af sundhedsområdets aktører, herunder at den tværgående viden- og erfaringsudveksling styrkes. Den skal skabe større klarhed vedrørende de enkelte aktørers roller og ansvar – både i det daglige arbejde og i tilfælde af sikkerhedshændelser. Dertil skal strategien sikre, at indsatsen prioriteres og løbende videreudvikles, således at sundhedssektorens sikkerhedsniveau og -tiltag følger udviklingen i forhold til nye typer af cyber- og informationssikkerhedshændelser.

FIGUR

Kortlægning af sektorens kritiske og fælles processer og systemer



Den grønne cirkel angiver i simplificeret form det overordnede fokus for initiativerne defineret i nærværende strategi. Der sigtes kort sagt på at øge sikkerheden, hvor konsekvenserne af en hændelse er størst, og hvor systemerne har flest snitflader. En kortlægning af sektorens kritiske og fælles processer og systemer er følgelig en primær opgave for sektoren. Opgaven er defineret under Indsatsområde 1, se Initiativ 1.1.

På sikkerhedsområdet er vi allerede i dag midt i en opbygning

I sundhedssektoren sker der på nuværende tidspunkt en generel kapacitetsopbygning i forhold til cyber- og informationssikkerhed; bl.a. med indsatsen for at følge ISO 27001 og EU's regulering på området i form af Net- og informationssikkerhedsdirektivet (NIS) og databeskyttelsesforordningen (GDPR).

EU's Net og informationssikkerhedsdirektiv (NIS-direktivet)

NIS-direktivet trådte i kraft den 9. maj 2018 og har til formål at øge sikkerheden i de tjenester, der er afhængige af net- og informationsteknologi. Sundhedssektoren skal således leve op til direktivets krav om bl.a. indberetning af sikkerhedshændelser og udpegning af operatører af væsentlige tjenester.

EU's Persondataforordning (GDPR)

EU's Persondataforordning (GDPR) trådte i kraft den 25. maj 2018 og indeholder en lang række bestemmelser, som har til formål at sikre beskyttelsen af personhenførbare oplysninger; bl.a. lægger GDPR vægt på databeskyttelse gennem design og standardindstillinger og giver mulighed for at pålægge myndigheder og virksomheder anselige bøder for brud på datasikkerheden. Et sygehus i Barreiro i Portugal er som et af de første blevet idømt en bøde i regi af GDPR. Bøden på €400.000 skyldtes, at sygehuset ikke havde passende tiltag på plads til at begrænse personalets adgang til patienternes data, og at sygehuset ikke i tilstrækkelig grad havde sikret fortroligheden, integriteten, tilgængeligheden og modstandsdygtigheden for sine it-systemer.

Sundhedssektorens aktører er enige om at følge ISO 27001

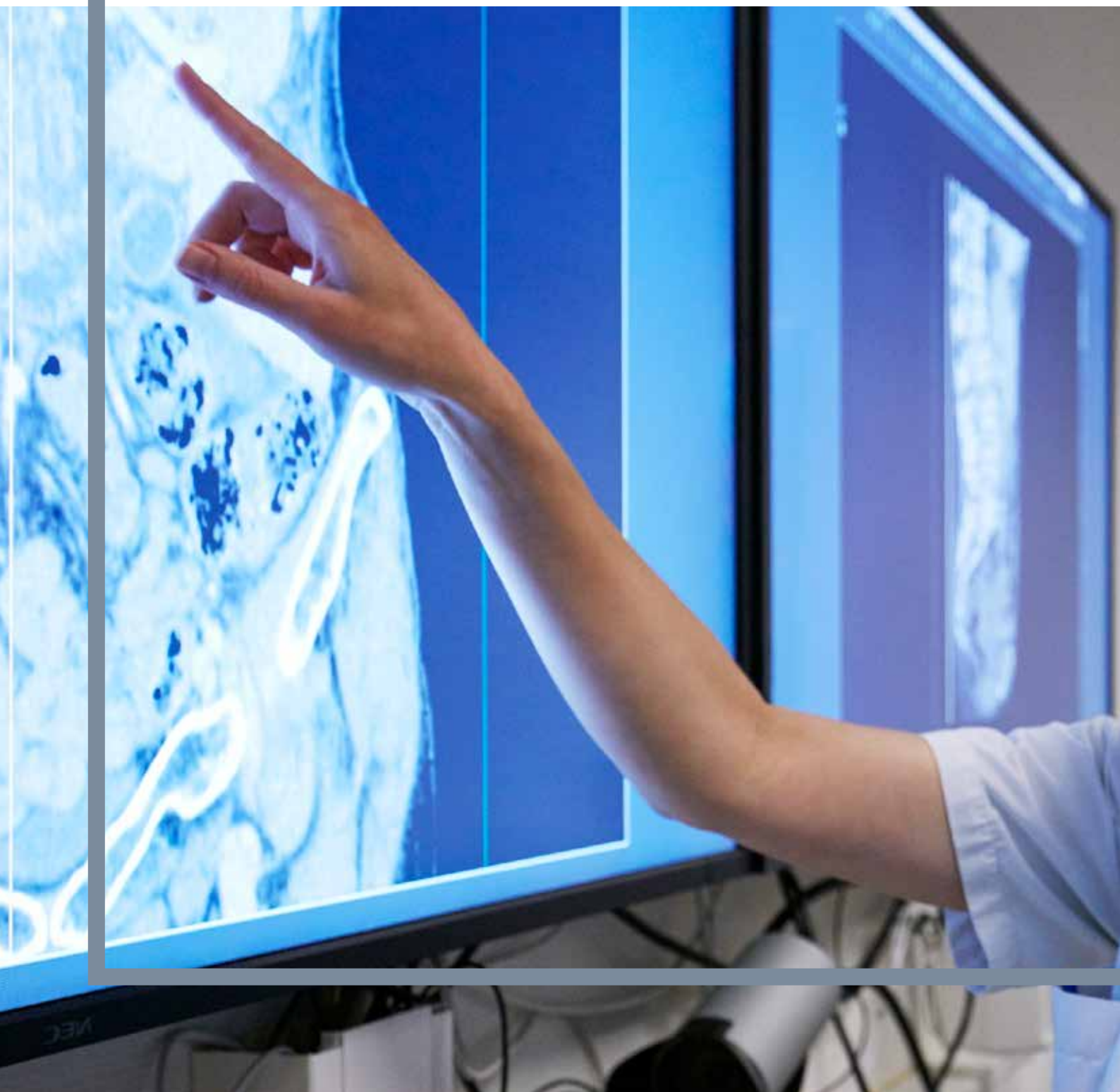
Det er obligatorisk for alle statslige myndigheder i Danmark at følge ISO 27001, en international standard for styring af informationssikkerhed. Regionerne har tilsvarende valgt at følge ISO 27001, ligesom kommunerne har forpligtet sig på at leve op til standardens principper. I udarbejdelsen af strategien og dens initiativer har sundhedssektoren også ladet sig inspirere af National Institute of Standards and Technologys (NIST) rammeværktøj for cybersikkerhed. Truslerne er dynamiske, og derfor har det været nødvendigt at supplere den obligatoriske ISO 27001's fokus på styring og processer med nogle hurtigere, mere agile og tekniske tiltag for at understøtte en helhedsorienteret styrkelse af sektorens kapacitet i forhold til cyber- og informationssikkerhed.

→ Den nationale strategi udstikker rammen

I National strategi for cyber- og informationssikkerhed 2018-2021 stilles der krav om, at sundhedssektoren i lighed med fem øvrige samfundskritiske sektorer (energi-, finans-, søfart-, tele- og transportsektoren) udarbejder en sektorspecifik strategi for cyber- og informationssikkerhed og etablerer en decentral cyber- og informationssikkerhedsenhed (DCIS) i sektoren. Med offentliggørelsen af denne strategi og etableringen af den decentrale cyber- og informationssikkerhedsenhed (DCIS) for sundhedssektoren i Sundhedsdatastyrelsen tages der højde for disse krav, ligesom strategiens initiativer løfter en række øvrige krav stillet i den nationale strategi.

BAGGRUND OG ANALYSE

Trusler, sårbarheder og risici i sektoren



Cyber- og informationssikkerhed i sundhedssektoren knytter an til en række forskellige trusler, sårbarheder og risici. Sammen med den teknologiske udvikling og opfindsomheden på modstandersiden gør det cyber- og informationssikkerhed til en kompleks og dynamisk udfordring. Det er et område i konstant bevægelse.

Trusselsbilledet er både komplekst og i bevægelse

Der sker en løbende udvikling af sundhedssektoren og dens opgaver og arbejdsgange – bl.a. som følge af digitaliseringen af sundhedsvæsenet og behandlings- og plejeopgaver, som rykkes tættere på borgeren. I takt hermed sker der også en løbende udvikling i trusselsbilledet.

Center for Cybersikkerhed offentliggjorde i juli 2018 den første sektorspecifikke trusselvurdering for sundhedssektoren. Baseret på internationale erfaringer peger Center for Cybersikkerhed på, at truslen mod sundhedssektoren kan komme fra en række forskellige aktører – såvel statslige aktører som kriminelle – og i mange forskellige former; lige fra spionageoperationer til ransomware og phishing-mails.

Cyber- og informationssikkerhed i sundhedssektoren kan dog ikke reduceres til et spørgsmål om at beskytte sektoren mod fjendtligsindede, eksterne aktører alene. Sideløbende med Center for Cybersikkerheds trusselsvurdering er der som led i strategiarbejdet udarbejdet en sårbarhedsvurdering for at kortlægge og vurdere sundhedssektorens forskellige sårbarheder. Sårbarhedsvurderingen peger overordnet på en række sårbarheder i sundhedssektoren, som det er særligt væsentligt at sætte ind imod; bl.a. legacy-systemer og -udstyr, leverandørstyring, aktørernes gensidige afhængigheder i de forskellige teknologiers samspil samt cyber- og informationssikkerhedskompetencer blandt sektorens mange forskellige medarbejdergrupper.

Sundhedssektoren er en samfundskritisk sektor, og mange af sektorens processer og systemer er per definition kritiske. Det er dog ikke dem alle, der er lige kritiske for sektoren som helhed. Således er de processer og systemer, som indgår direkte i behandlingen og plejen af borgerne og håndtering og opbevaring af deres følsomme personoplysninger, alt andet lige mere kritiske end processer og systemer, der understøtter det administrative arbejde i sektoren. Fx er det mere kritisk, hvis sektorens laboratoriesystemer eller billeddiagnostik påvirkes sammenlignet med sektorens processer og systemer til afregning og udbetalinger. På samme måde er processer og systemer, som anvendes og drives af flere af sektorens aktører i fællesskab også mere kritiske end systemer, som kun anvendes lokalt af én enkelt aktør.

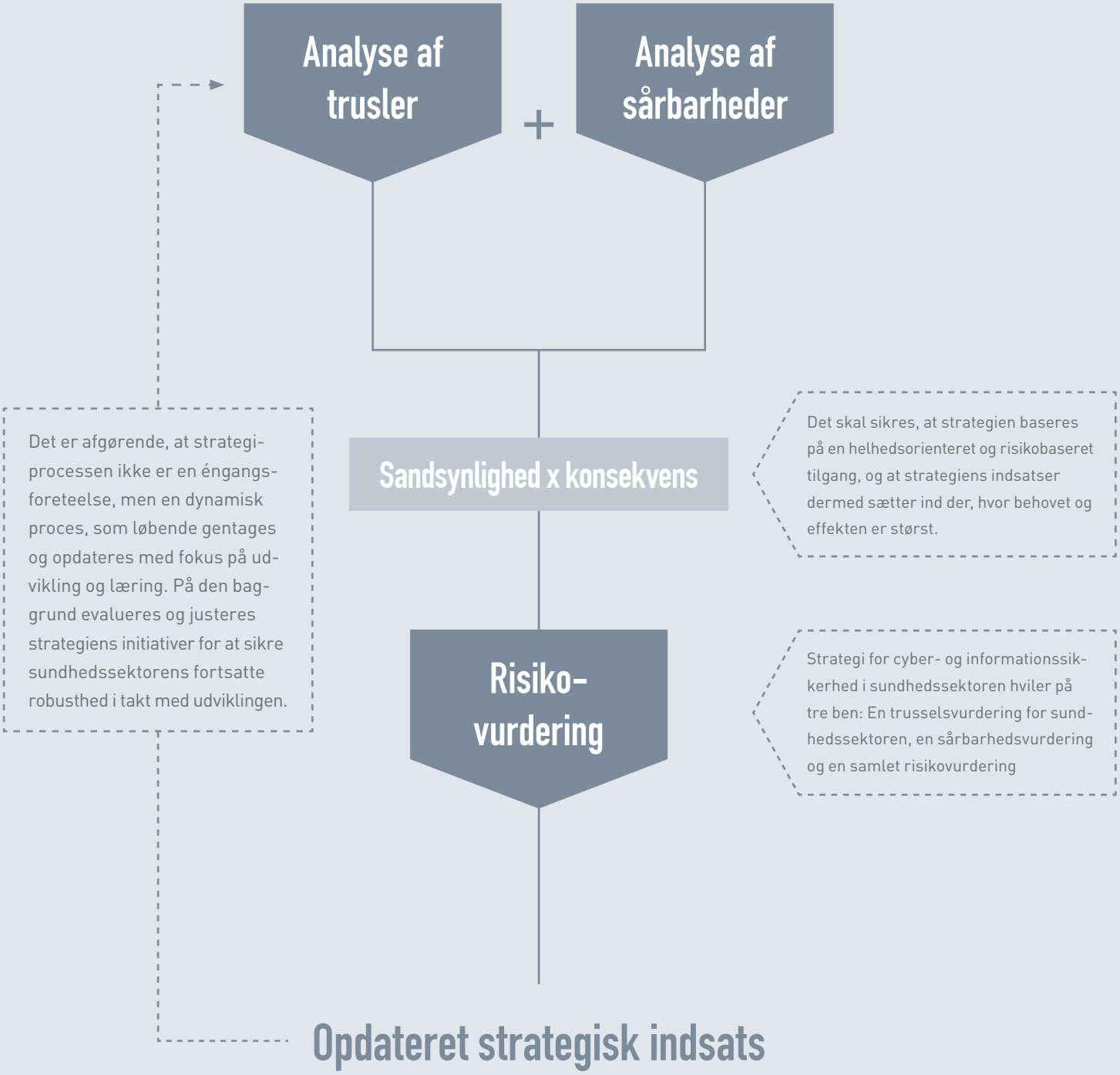
På baggrund af sektorens sårbarhedsvurdering og Center for Cybersikkerheds trusselvurdering er der derfor udarbejdet en samlet risikovurdering for sundhedssektoren for at understøtte en helhedsorienteret og risikobaseret tilgang til cyber- og informationssikkerhed. Her er konsekvenserne for sundhedssektoren vurderet ud fra de forskellige risici, hvilket bidrager til at kunne prioritere sektorens indsats i forhold til de største risici og mest kritiske processer og systemer. Derudover bidrager risikovurderingen til at vurdere det passende sikkerhedsniveau i forhold til den enkelte risiko sammenholdt med både konsekvenserne ved en hændelse og hensynet til den almindelige behandling og pleje af borgerne.

→ Center for Cybersikkerhed vurderer, at truslen fra

- cyberspionage mod den danske sundhedssektor er **meget høj**
- cyberkriminalitet mod den danske sundhedssektor er **meget høj**
- cyberaktivisme mod den danske sundhedssektor er **lav**
- cyberterrorisme mod den danske sundhedssektor er **lav**

FIGUR

Processen bygger på fortløbende og gentagne analyser og konklusioner



WannaCry-angrebet og det britiske sundhedsvæsen

Sundhedssektorens høje grad af digitalisering indebærer en større sårbarhed over for cyber- og informations sikkerhedshændelser. Fx blev det britiske sundhedsvæsen National Health Service (NHS) i maj 2017 ramt af ransomware som led i det såkaldte WannaCry angreb, der inficerede flere hundredetusinde computere verden over. WannaCry gjorde en lang række systemer utilgængelige og medførte over 19.000 aflyste behandlinger, og at mange patienter måtte omdirigeres. Samlet anslås WannaCry at have kostet NHS omkring £92 mio.

Vi skal styrke cyber- og informationssikkerheden i fire spor

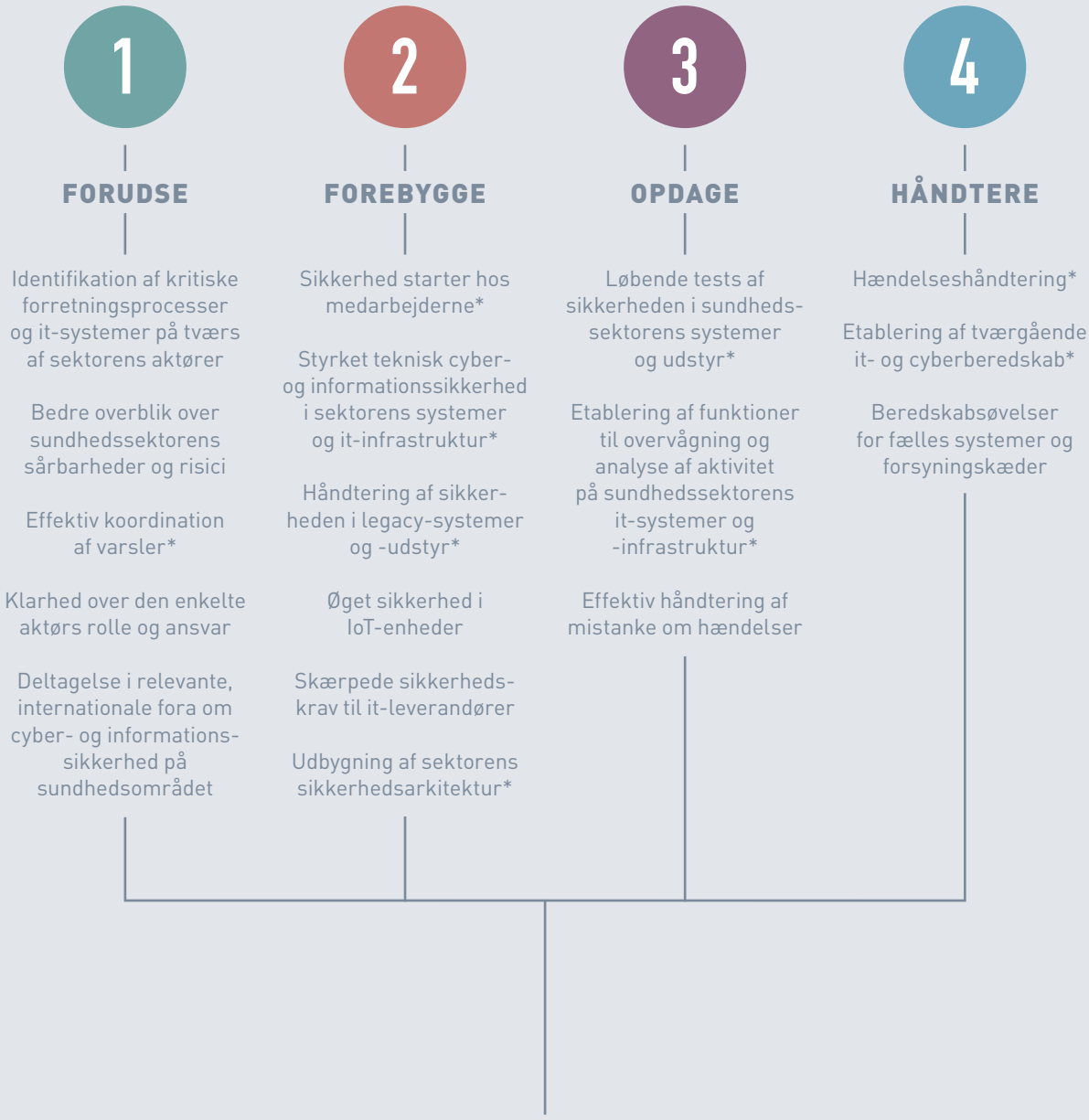
For at sundhedssektoren løbende kan modstå og tage hånd om aktuelle og kommende trusler og risici, er der behov for en tværgående styrkelse af sektorens samlede og fælles cyber- og informationssikkerhedsindsats. Derfor er strategien inddelt i fire indsatsområder: Strategien sigter mod at styrke sundhedssektorens kapacitet til at forudse, forebygge, opdage og håndtere cyber- og informationssikkerhedshændelser. For hvert indsatsområde er der udpeget en række konkrete initiativer, som sektorens aktører i fællesskab vil løfte. Nogle initiativer bygger videre på indsatser, som allerede er i gang hos enkelte aktører, mens andre initiativer består af nye, fælles tiltag i sektoren. Samtidig skal nogle af strategiens initiativer medvirke til at binde en række aktiviteter i sektoren sammen i tværgående aktiviteter via sundhedssektorens decentrale cyber- og informationssikkerhedsenhed (DCIS) i Sundhedsdatastyrelsen.

Alle aspekter af cyber- og informationssikkerhed bliver adresseret og vurderet.

Tilgangen skal sikre, at der med strategien anlægges en helhedsorienteret tilgang til indsatsen med at styrke sundhedssektorens samlede sikkerhedsniveau, så alle aspekter af cyber- og informationssikkerhed bliver adresseret og vurderet.

DE FIRE SPOR

En logisk systematik styrer arbejdet med at skabe tryghed

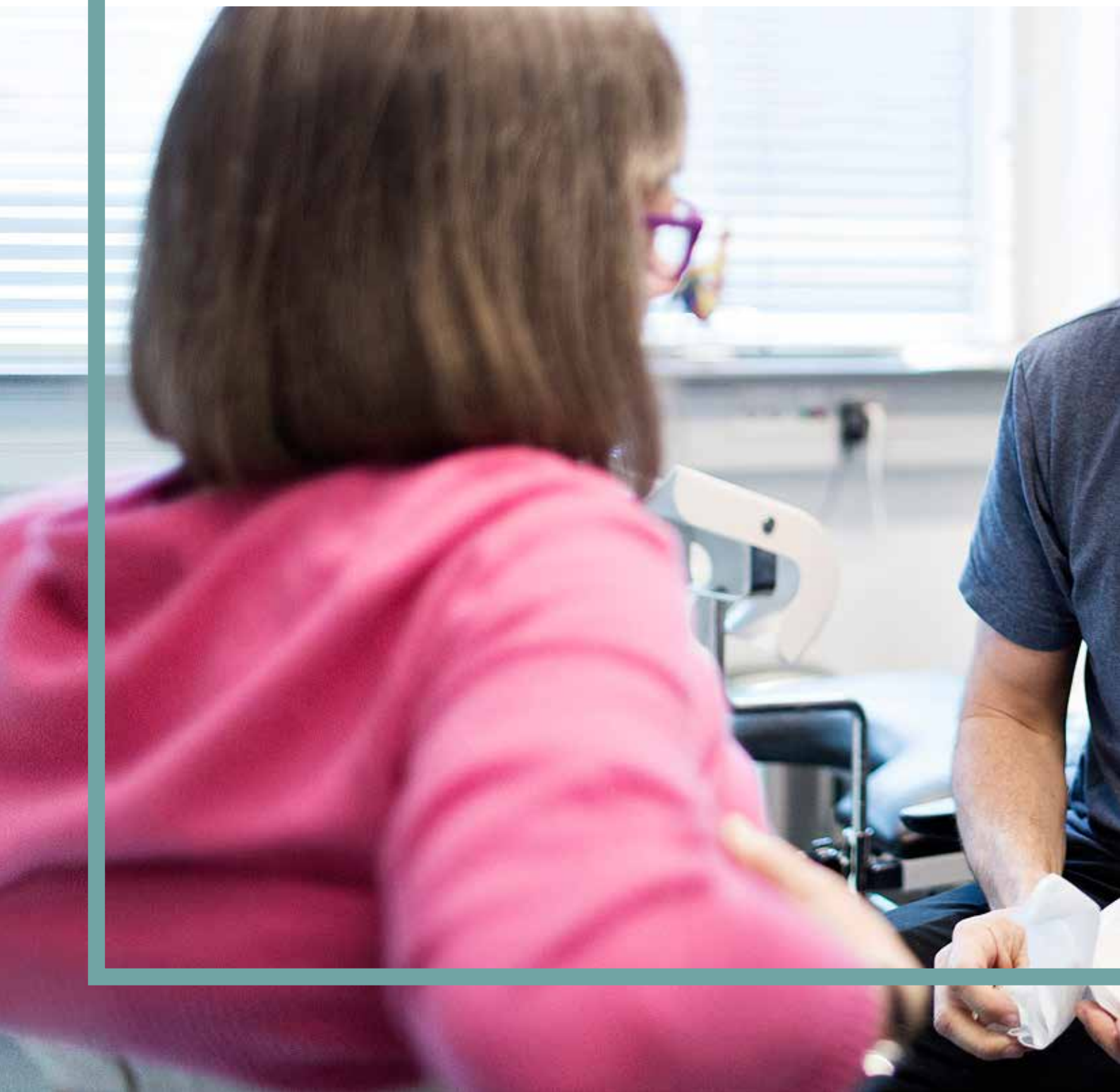


Udmøntning og organisering

*Initiativer hvor én eller flere aktiviteter forudsætter særskilt aftale om finansiering.

SPOR 1 - FORUDSE

Bedre forudsigelse af potentielle angreb og hændelser



Bedre forudsigelse af potentielle cyber- og informationssikkerhedshændelser er afgørende for at kunne sætte effektivt ind med de rette sikkerhedstiltag i tide på de rette niveauer. Det er en væsentlig forudsætning for, at sektoren som helhed og de enkelte aktører kan træffe de rette beslutninger om det nødvendige sikkerhedsniveau.

SPOR 1

Mulige angreb og hændelser kan i mange tilfælde forudsiges

Evnen til at forudsige mulige cyber- og informationssikkerhedshændelser er blandt andet betinget af viden om kritiske processer og systemer, et overblik over sårbarheder og risici, hurtig og effektiv formidling af varsler om mulige sikkerhedshændelser under opsejling til alle relevante aktører, klarhed over roller og ansvar og deling af den nyeste viden på området med relevante, internationale partnere.

Eksempelvis kan der tages udgangspunkt i informationer om angreb i udlandet, som kan ramme sundhedsvæsenet i Danmark.

På den baggrund skal strategien sikre, at sundhedssektoren som helhed får en mere præcis beskrivelse af sektorens kritiske processer, systemer og gensidige afhængigheder samt en mere fælles og ensartet forståelse af de sårbarheder og risici og roller og ansvar, der er forbundet hermed.

Center for Cybersikkerheds trusselsvurderinger for sektoren skal ledsages af sårbarheds- og risikovurderinger både for hele sektoren og for de enke lte aktører med udgangspunkt i ISO 27001.

Samtidig skal strategien sikre, at alle relevante aktører i sektoren hurtigere og mere præcist bliver varslet i tilfælde af fx angreb i udlandet, så de har et klart billede af den aktuelle trusselsituation og kan igangsætte de rette forholdsregler. Dette skal styrkes ved, at der etableres klare og sikre kommunikationslinjer – såvel mellem sektoren og Center for Cybersikkerhed som internt i sektoren på tværs af alle aktører.

→ Det er vigtigt, at trusselsvurderinger kommunikeres

Center for Cybersikkerhed udarbejder vurderinger af cybertruslen specifikt mod sundhedssektoren, som bidrager til at understøtte sundhedssektorens cyber- og informationssikkerhedsindsats. Det er væsentligt, at alle relevante aktører i sundhedssektoren orienteres hurtigt og effektivt om opdaterede trusselsvurderinger, så der lokalt kan ageres derefter. Den decentrale cyber- og informationssikkerhedsenhed (DCIS) i Sundhedsdatastyrelsen skal derfor i samarbejde med resten af sektoren fastlægge procedurer for, hvordan sektorens aktører informeres om trusselvurderingerne.

→ Initiativer

1. Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører
2. Bedre overblik over sundhedssektorens sårbarheder og risici
3. Effektiv koordination af varsler
4. Klarhed over den enkelte aktørs rolle og ansvar
5. Deltagelse i relevante, internationale fora om cyber- og informationssikkerhed på sundhedsområdet

INITIATIV 1.1.

Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører

For at sikre en målrettet tilgang til arbejdet med cyber- og informationssikkerhed er det nødvendigt at udpege sektorens mest kritiske forretningsprocesser samt de it-systemer, som understøtter dem. DCIS faciliterer i en årlig proces udarbejdelsen af en oversigt over sektorens kritiske forretningsprocesser, it-systemer og forsyningskæder med input fra sundhedssektorens aktører. Første version udarbejdes inden udgangen af 1. halvår 2019.

INITIATIV 1.2.

Bedre overblik over sundhedssektorens sårbarheder og risici

Det er nødvendigt løbende at vedligeholde lokale og tværgående vurderinger af sårbarheder og risici. Det er de enkelte aktørers ansvar at udarbejde og opdatere egne sårbarheds – og risikovurderinger samt sikre ledelsesforankring. DCIS udarbejder i 2019 i samarbejde med sektorens aktører vejledninger til at understøtte arbejdet, således at vurderingerne over tid bliver metodisk ensartede. Vejledningerne vil desuden være obligatoriske at følge for sårbarheds – og risikovurderinger af fælles, prioriterede, kritiske systemer. DCIS har desuden til opgave at udarbejde den samlede sårbarheds- og risikovurdering for hele sektoren.

INITIATIV 1.3.

Effektiv koordination af varsler

Sektorens evne til at forudsige mulige angreb og sikkerhedshændelser skal styrkes ved, at DCIS i 1. kvartal 2019 etablerer en samlet model for effektiv koordination af varsler om mulige angreb og sikkerhedshændelser. Det omfatter bl.a. en første version af en funktion til modtagelse og afsendelse af varsler, abonnementslister, regler for udsendelse af varsler mv. Det skal sikre, at alle relevante parter hurtigere og mere præcist får viden om, at et angreb kan være undervejs, så der kan igangsættes de rette forholdsregler. Modellen implementeres af sektorens aktører inden for egne budgetter. Etablering af en udvidet løsningsmodel forudsætter særskilt aftale.

INITIATIV 1.4.

Klarhed over den enkelte aktørs roller og ansvar

Kendskab til eget ansvar og egen rolle i forbindelse med cyber- og informationssikkerhed er afgørende for, at hver aktør i sundhedssektoren kan reagere hurtigt og effektivt i tilfælde af cyber- og informationssikkerhedshændelser. I forbindelse med udarbejdelsen af strategi for cyber- og informationssikkerhed i sundhedssektoren er der udarbejdet en første beskrivelse af de enkelte aktørers roller og ansvar på tværs af sektoren. DCIS får til opgave i løbet af 1. halvår 2019 at videreudvikle dette arbejde og vedligeholde det med inddragelse af sektorens aktører. DCIS skal desuden sikre, at de omfattede aktører er bekendt med indholdet heraf.

INITIATIV 1.5.

Deltagelse i relevante, internationale fora om cyber- og informationssikkerhed på sundhedsområdet

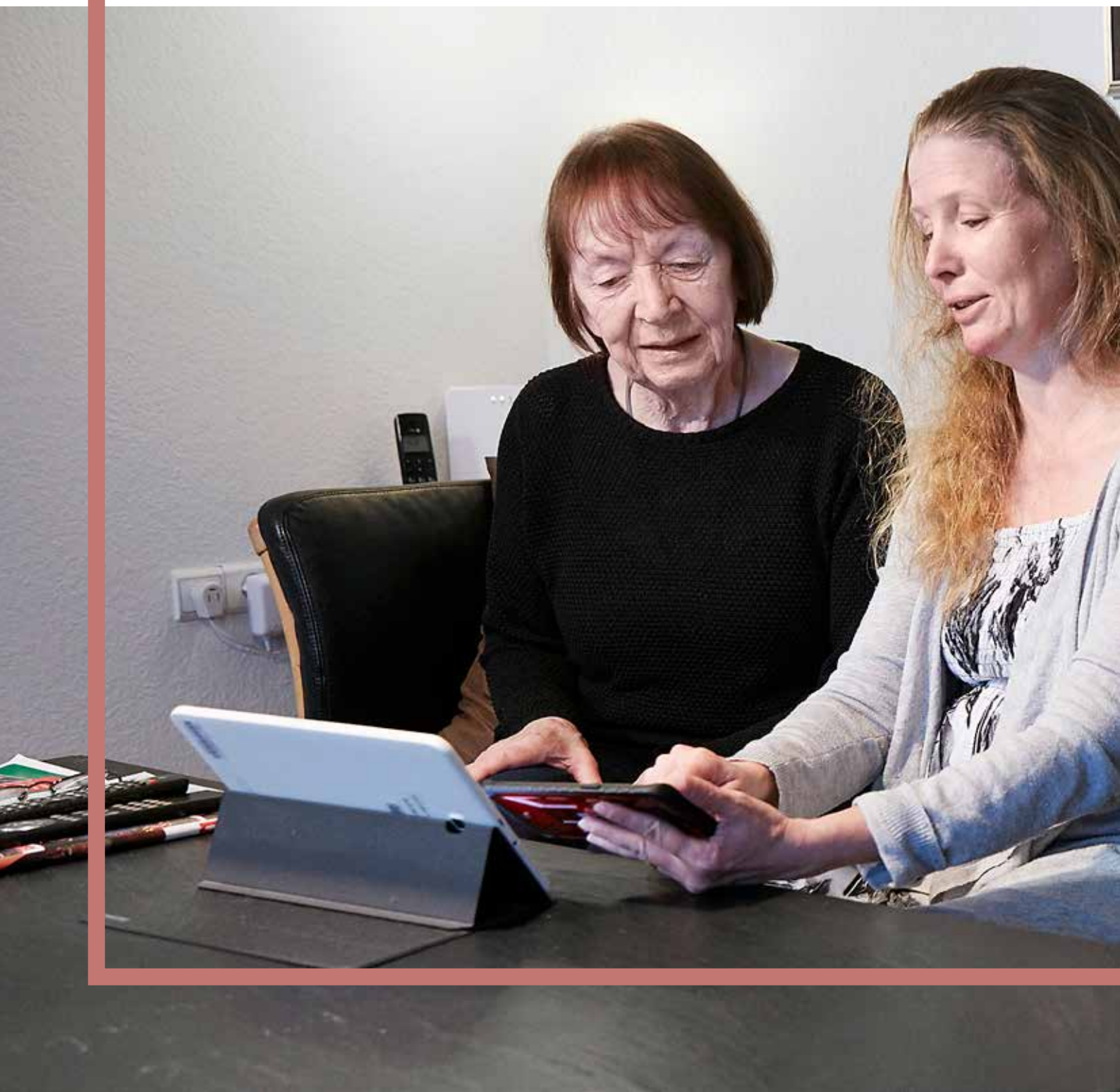
Cyber- og informationssikkerhed og mulige tiltag til at imødegå et skiftende trusselsbillede er i hastig udvikling. Det er derfor afgørende, at cyber- og informationssikkerhedsindsatsen i sundhedssektoren baseres på seneste, internationale viden og tendenser inden for teknologi, analysemetoder mv. DCIS skal derfor identificere og deltage i relevante, internationale fora, hvor cyber- og informationssikkerhed i relation til sundhedssektoren behandles, og etablere et netværk til relevante cyber- og informationssikkerhedsenheder på sundhedsområdet. DCIS skal desuden sikre, at relevant viden herfra videreformidles til sundhedssektorens aktører.

INITIATIV 1.4.

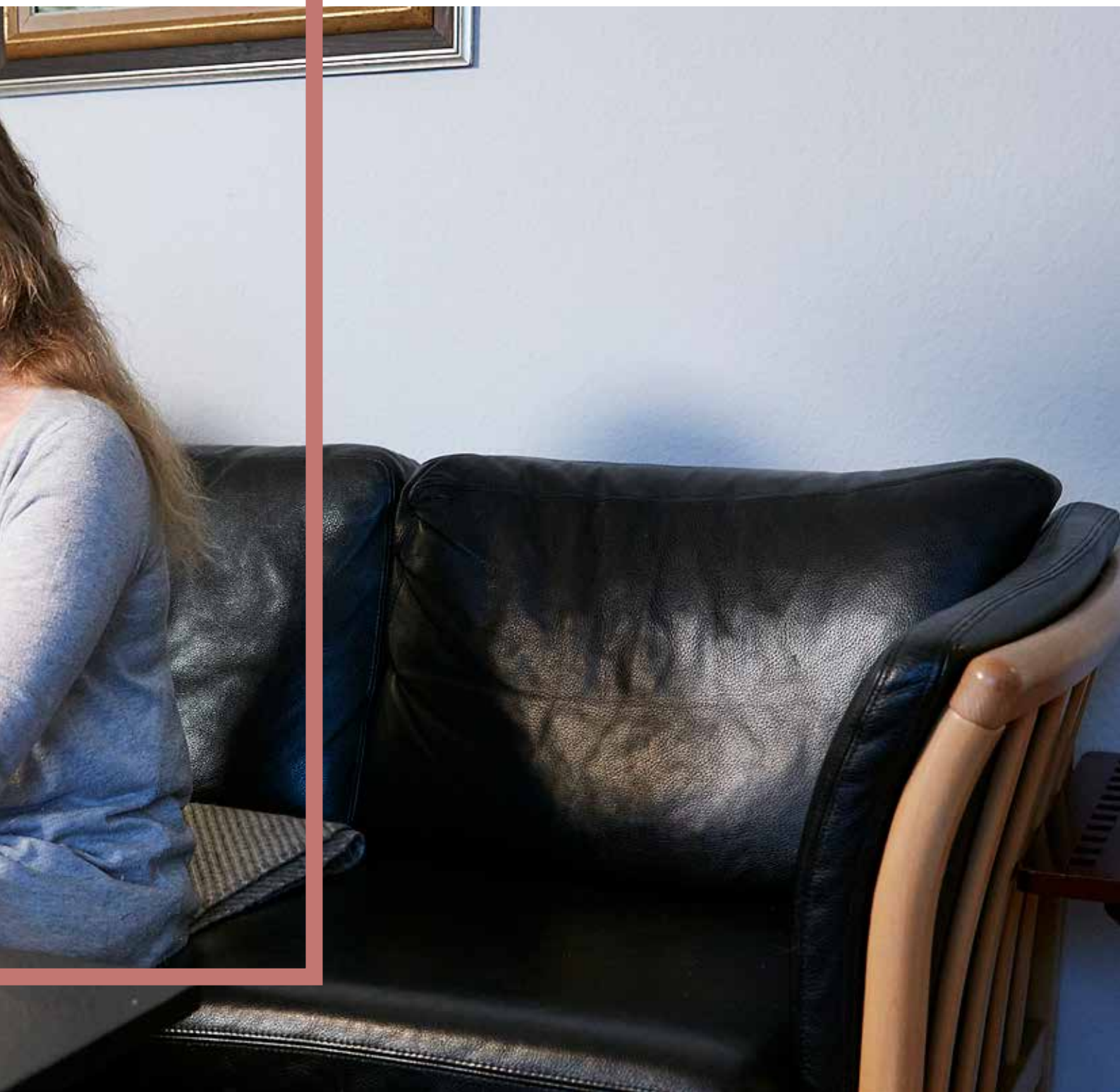
Kendskab til eget ansvar og egen rolle i forbindelse med cyber- og informationssikkerhed er afgørende for, at hver aktør i sundhedssektoren kan reagere hurtigt og effektivt.

SPOR 2 - FOREBYGGE

Bedre mulighed for at forebygge angreb og hændelser



Evnen til at forebygge cyber- og informationssikkerhedshændelser afhænger af en lang række faktorer – tekniske, organisatoriske, menneskelige mv. – som alle må være på plads, for at risikoen for en uønsket hændelse effektivt kan reduceres.



SPOR 2

Effektiv forebyggelse handler i høj grad om kultur

Det er helt afgørende for at sikre effektiv forebyggelse, at der i hele sektoren er en stærk og robust cyber- og informationssikkerhedskultur. Dette omfatter bl.a., at medarbejderne har den fornødne viden og kompetencer i forhold til cyber- og informationssikkerhed, så følsomme personoplysninger håndteres forsvarsligt og sikkert, og medarbejderne er opmærksomme på fx phishing-mails og andre typer af angrebsforsøg.

Effektiv forebyggelse kræver, at der i hele sektoren er en tilstrækkelig stærk cyber- og informationssikkerhedskultur.

Tekniske sikkerhedstiltag er naturligvis også vigtige i bestræbelserne på at forebygge cyber- og informationssikkerhedshændelser, men hvis ikke medarbejdernes viden og forståelse af behovet for disse tiltag er på plads, er der en risiko for, at de uforvarende kan komme til at omgå dem i en travl hverdag. Derfor skal bedre og mere kompetenceudvikling for sundhedssektorens mange forskellige medarbejdergrupper højne deres opmærksomhed på – og viden om – cyber- og informationssikkerhed og sikre en passende sikkerhedsadfærd.

Ud over awareness-aktiviteterne rettet mod sektorens medarbejdere sætter strategien også ind med en række andre indsatser for at styrke sektorens evne til at forebygge cyber- og informationssikkerhedshændelser. Med udgangspunkt i en risikobaseret tilgang skal der blandt andet lokalt såvel som på de fælles it-systemer implementeres de rette tekniske sikkerhedsforanstaltninger til at forebygge angreb og sikkerhedshændelser.

Som led i styrkelsen af den tekniske sikkerhed i sektoren er der også behov for at tage hånd om den udfordring, som håndtering af legacy-systemer udgør. Mange af disse systemer lever ikke nødvendigvis op til gældende sikkerhedsstandarder, men det kan være svært eller uhensigtsmæssigt at udskifte eller opdatere dem, da de ofte er nødvendige for behandlingen. En yderligere udfordring i denne henseende er IoT-enheder, som er tilsluttet internettet.

For at styrke indsatsen for forebyggelse på tværs af sektoren vil sundhedssektorens aktører arbejde med fælles basissikkerhedskrav i kontrakter med de leverandører, der leverer it-løsninger og it-drift til sektoren. De fælles leverandørkrav vil bl.a. tage udgangspunkt i det arbejde med leverandørkontrakter, som igangsættes med den nationale strategi for cyber- og informationssikkerhed. Derudover vil sektorens aktører i fællesskab også arbejde på at udbygge og styrke sektorens sikkerhedsarkitektur gennem bl.a. øget fokus på databeskyttelse gennem design.

→ Sikkerhedspolitikker

Sundhedssektorens aktører skal hver især have anvendte sikkerhedspolitikker og konkrete retningslinjer, der retter sig mod deres medarbejdere og processer. Den aktørspecifikke sikkerhedspolitik skal opdateres svarende til behovet og udviklingen i trusselsbilledet.

→ Initiativer

1. Sikkerhed starter hos medarbejderne
2. Styrket teknisk cyber- og informationssikkerhed i sektorens systemer og it-infrastruktur
3. Håndtering af sikkerheden i legacy-systemer og -udstyr
4. Øget sikkerhed i IoT-enheder
5. Skærpede sikkerhedskrav til it-leverandører
6. Udbygning af sektorens sikkerhedsarkitektur

INITIATIV 2.1.

Sikkerhed starter hos medarbejderne

Høj opmærksomhed blandt medarbejderne i sundhedssektoren på risikoen for cyber- og informationssikkerhedshændelser er en nøglefaktor i arbejdet med at styrke sektorens evne til at forebygge mulige cyber- og informationssikkerhedshændelser. Derfor skal alle medarbejdere i sundhedsvæsenet uddannes i cyber- og informationssikkerhed; fx ved brug af de uddannelsespakker om cyber- og informationssikkerhed, som er udviklet i regi af den fællesoffentlige digitaliseringsstrategi 2016-2020, eller gennem lokale initiativer. DCIS får desuden til opgave at indgå i et igangværende arbejde med at styrke fokus på cyber- og informationssikkerhed i relevante uddannelsesforløb, herunder på de sundhedsfaglige uddannelser. Desuden skal kendskabet til cyber- og informationssikkerhed styrkes på alle ledelsesniveauer, ligesom der skal sikres de rette kompetencer for de medarbejdere, der til daglig arbejder med cyber- og informationssikkerhed i sundhedssektoren. Gennemførslen af fælles aktiviteter forudsætter særskilt aftale.

INITIATIV 2.2.

Styrket teknisk cyber- og informationssikkerhed i sektorens systemer og it-infrastruktur

Den tekniske cyber- og informationssikkerhed i sundhedssektorens it-infrastruktur skal styrkes gennem etableringen af de rette og tidssvarende tekniske foranstaltninger med henblik på at øge kapaciteten til at beskytte data og systemer og forebygge cyber- og informationssikkerhedshændelser. Derfor er der i skabelonen for den fællesoffentlige databehandleraftale på sundhedsområdet indsat en række tekniske krav, som skal afholdes ved benyttelsen af aftalen. Samtidig igangsættes der som led i en national målsætning om end-to-end-kryptering i sundhedssektorens it-infrastrukturer en målrettet indsats for at endepunktskryptere (eller begrundet fravalg) de services, som regionerne udstiller via Sundhedsdatanettet. Ydermere bør indkøb og ibrugtagning af ny teknologi planlægges for at understøtte, at sektoren forholder sig strategisk til ny teknologi med udgangspunkt i en risikobaseret tilgang.

INITIATIV 2.3.

Håndtering af sikkerheden i legacy-systemer og -udstyr

Sundhedssektorens aktører skal tage hånd om sikkerheden i legacy-systemer og -udstyr, som ikke overholder tidssvarende standarder for sikkerhed. DCIS faciliterer derfor, at der i 2. halvår 2019 påbegyndes en kortlægning af sektorens legacy-systemer og -udstyr ud fra en risikobaseret tilgang og med særligt fokus på de systemer, der er identificeret som fælles, kritiske systemer. Yderligere fælles indsatser forudsætter særskilt aftale.

→ Almindelig it-driftshygiejne er en væsentlig faktor

Almindelig it-driftshygiejne er et væsentligt fundament for arbejdet med cyber- og informationssikkerhed. Den kan naturligvis ikke stå alene over for det skærpede trusselsbillede, men det er afgørende at have styr på den daglige it-drift og have basale processer og procedurer på plads for at sikre et godt og robust udgangspunkt for det øvrige arbejde med cyber- og informationssikkerhed. Det er vigtigt, at de enkelte aktører dokumenterer og benytter veldefinerede og velafprøvede processer for fx anskaffelse af nye systemer, videreudvikling og vedligehold af eksisterende it-systemer samt opdateringer og konfigurationsændringer. Almindelig it-driftshygiejne inkluderer bl.a. anerkendte metoder til fx life cycle management og change management. Dette bidrager til, at der til enhver tid opretholdes et ensartet, højt og robust sikkerhedsniveau.

INITIATIV 2.1.

Høj opmærksomhed blandt medarbejderne i sundhedssektoren på risikoen for cyber- og informationssikkerhedshændelser er en nøglefaktor i arbejdet med at styrke sektorens evne til at forebygge.

INITIATIV 2.4.

Øget sikkerhed i IoT-enheder

Sikkerheden i sektoren skal styrkes i forhold til IoT-enheder, der er forbundet til et netværk. Dette skal i første omgang ske ved, at Lægemiddelstyrelsen og DCIS i 2019 indleder et strategisk samarbejde om at dele relevant viden, drøfte nyeste regulatoriske krav på området mv. I den forbindelse vil Center for Cybersikkerhed i løbet af 2019 udarbejde en særskilt vurdering af cybertruslen mod netværksforbundet medicinsk udstyr. Desuden faciliterer DCIS, at sektorens aktører kan dele viden og erfaringer, herunder best practices for håndtering af medicinsk udstyr.

INITIATIV 2.5.

Skærpede sikkerhedskrav til it-leverandører

Sundhedssektorens aktører benytter i stort omfang private leverandører ved anskaffelse og udvikling af fx ny teknologi, ligesom dele af sundhedssektorens it-systemer drives af private leverandører eller af en offentlig aktør på vegne af hele sektoren. For at sikre at private og offentlige it-leverandører mødes af ensartede krav om et højt sikkerhedsniveau fra alle sektorens aktører, skal der udarbejdes fælles sikkerhedskrav samt processer og værktøjer til understøttelse af efterlevelsen af disse krav. Initiativet igangsættes i andet halvår af 2019. Udgangspunktet er bl.a. det fællesoffentlige klausulbibliotek. MedCom skal desuden gennemføre en analyse af muligheden for at gennemføre bl.a. leverandørstyring gennem Sundhedsdatanettet.

INITIATIV 2.6.

Udbygning af sektorens sikkerhedsarkitektur

På tværs af sundhedssektoren skal der arbejdes ensartet med it-sikkerhedsmæssige krav, fx vedr. databeskyttelse gennem design og i forbindelse med videreudvikling af eksisterende systemer eller nyanskaffelser. For at sikre et passende og ensartet højt niveau af databeskyttelse gennem design og standardindstillinger skal sektoren lægge sig fast på et fælles sæt af metodikker og standarder, der gælder for hele sektoren. DCIS får som grundlag herfor til opgave at opdatere den samlede sikkerhedsarkitektur for sektoren inkl. fastlæggelse af standarder og udarbejdelse af værktøjer og vejledninger. Initiativet igangsættes i 2. halvår af 2019. Pilotafprøvning af den nye sikkerhedsarkitektur forudsætter særskilt aftale.

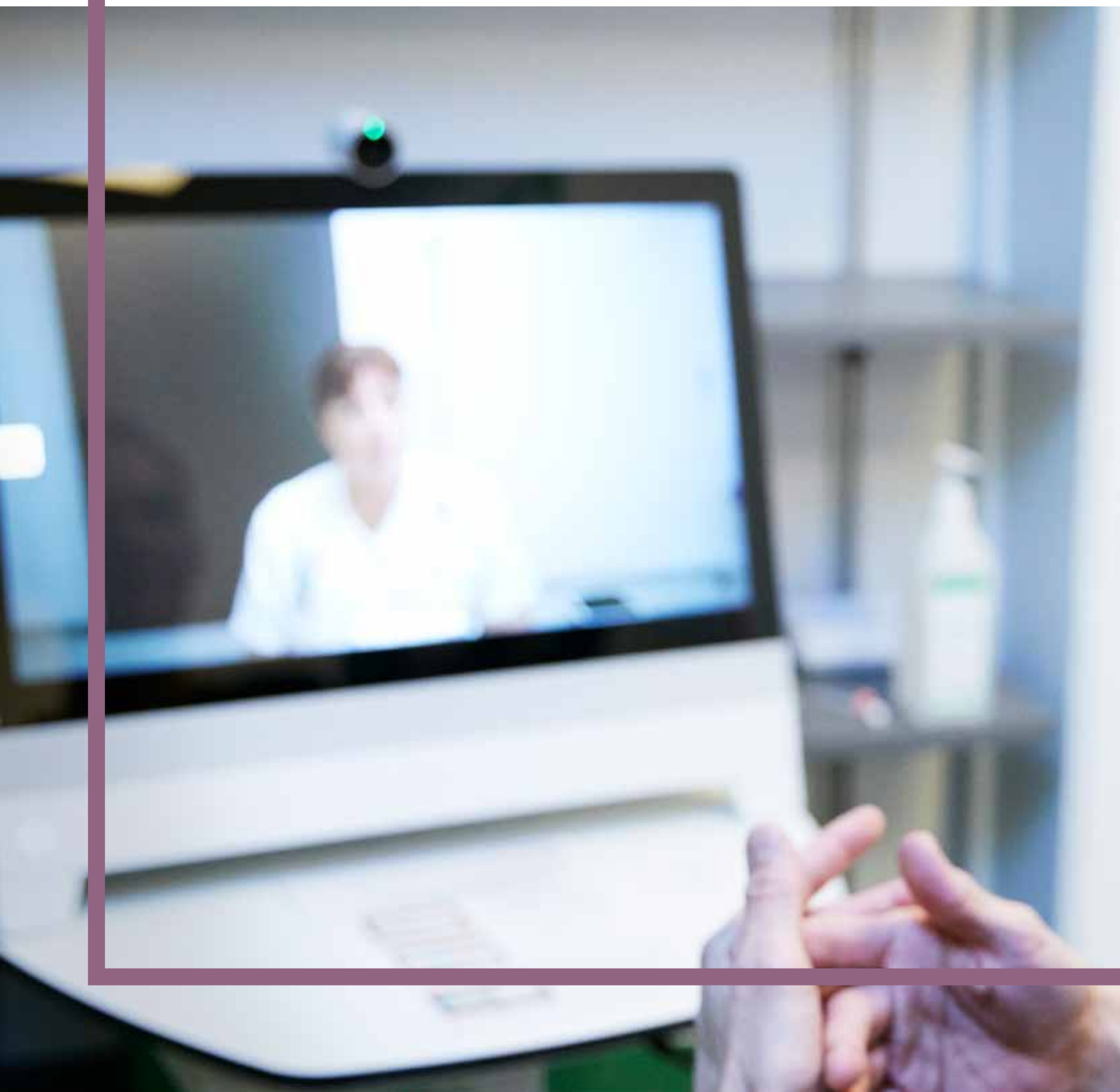
→ Cyberforsvar der virker

Der er en række grundlæggende tiltag, som man bør iværksætte med henblik på at styrke cyber- og informationssikkerheden i en organisation. I publikationen Cyberforsvar der virker skitserer Center for Cybersikkerhed og Digitaliseringsstyrelsen syv trin på vejen til et godt cyberforsvar, heriblandt ledelsesforankring, tekniske kompetencer, awareness og fire grundlæggende sikringstiltag:

- **Udarbejd positivliste over applikationer**
- **Opdatér programmer**
- **Opdatér operativsystem**
- **Begræns antallet af brugerkonti med domæne- eller lokaladministratorprivilegier**

SPOR 3 - OPDAGE

Bedre mulighed for at opdage angreb og hændelser



Ud over at være bedre til at forudsige og forebygge cyber- og informationssikkerhedshændelser skal sundhedssektoren opbygge kapaciteten til at opdage hændelser og angreb, som er under opsejling – fx i tilfælde af at udefrakommende uretmæssigt har skaffet sig adgang til sektorens systemer.

SPOR 3

Det handler om intelligent overvågning og om at være opmærksom i hverdagen

For at understøtte opdagelse af angreb og sikkerhedshændelser er der behov for, at sektorens aktører proaktivt overvåger aktivitet på såvel fælles som lokal infrastruktur og systemer. Det kræver, at de rette overvågningsfunktioner er på plads på de rette steder i sektoren, og at sektoren også på dette område er velkoordineret med henblik på at styrke kapaciteten til at opdage brud på cyber- og informationssikkerheden på tværs af sektorens aktører. Med et fælles højt niveau skal sektoren styrke den fælles modstandsdygtighed mod angreb og sikkerhedshændelser.

Dernæst er det vigtigt, at sundhedssektorens overvågningsfunktioner er tænkt sammen med kommunikationslinjer, beredskab og handlingsplaner inden for sektoren. Det gælder også på tværs af de samfundskritiske sektorer og på tværs af sundhedssektorerne i de lande, vi minder om og arbejder sammen med på cyber- og informationssikkerhedsområdet. Hvis uheldet er ude, skal en hændelse hurtigt kunne opdages og inddæmmes, således at den ikke spreder sig i eller på tværs af sektorer.

Med et fælles højt niveau skal sektoren styrke den fælles modstandsdygtighed mod angreb og sikkerhedshændelser.

Cyber- og informationssikkerhed er under konstant udvikling. Trusselsbilledet ændrer sig hastigt, og nye former for angreb ser dagens lys. Sektorens kapacitet til at opdage nye former for cyber- og informationssikkerhedshændelser skal følge med udviklingen, og sektorens overvågningsfunktioner skal stå mål med både det aktuelle trusselbillede og de risici, som truslerne udgør for borgeren, den sundhedsprofessionelle og for samfundet generelt. Derfor bør sektorens aktører løbende foretage sikkerhedstests af både den fælles og den lokale infrastruktur, således at nye sårbarheder og sikkerhedshuller opdages og håndteres.

Opdagelse af nye sårbarheder og sikkerhedshuller beror også på overvågenhed både blandt egne medarbejdere og eksterne aktører såsom såkaldte etiske hackere. Sektoren skal derfor stå parat og have procedurer til at håndtere henvendelser fra medarbejdere og andre om mulige sårbarheder i sektorens systemer eller mistanke om, at de er blevet kompromitteret.

Samlet skal disse tiltag gøre sektoren i stand til at tage hånd om disse udfordringer, blive bevidst om de skiftende mønstre i cyber- og informationssikkerhedshændelser og varsle relevante parter om en igangværende trussel.

→ MedCom og Sundhed.dk er på forkant

Sundhedssektoren er allerede i gang med indsatser for at styrke sikkerheden på tværs af sektoren. MedCom har implementeret en ny version af Sundhedsdatanettet med bl.a. en yderligere styrkelse af sikkerheden. Sundhedsdatanettet er fundamentet for størstedelen af den digitale kommunikation på tværs af sundhedssektoren. Ligeledes opretholder Sundhed.dk – mange borgeres primære indgang til egne sundhedsdata på tværs af sektoren – et højt sikkerhedsniveau gennem bl.a. tilbagevendende sikkerhedstests af portalen samt overvågning af tilkoblede systemer og gentagne sikkerheds-reviews af tilhørende apps, processer og procedurer samt infrastrukturen, der bruges rundt om portalen.

SPOR 3 – OPDAGE

→ Initiativer

1. Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr
2. Etablering af funktioner til overvågning og analyse af aktivitet på sundhedssektorens it-systemer og -infrastruktur
3. Effektiv håndtering af mistanke om hændelser

INITIATIV 3.1.

Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr

For at sundhedssektoren samlet set formår at opretholde en robusthed over for cyber- og informationssikkerhedshændelser, er det nødvendigt at gennemføre regelmæssige tests af sikkerheden i sundhedssektorens systemer og udstyr. DCIS får til opgave at afklare grundlaget for, om sektorens allerede eksisterende testaktiviteter skal udbygges og eventuelt kan samles i et egentligt testprogram, som kan omfatte sårbarhedsscanninger, penetrationstests og red team-tests. Etableringen af programmet – inkl. en platform til fortrolig videndeling om testresultater mv. – forudsætter særskilt aftale. DCIS skal desuden afklare muligheden for samarbejde om større sikkerhedstest med andre samfundskritiske sektorer.

INITIATIV 3.2.

Etablering af funktioner til overvågning og analyse af aktivitet på sundhedssektorens it-systemer og -infrastruktur

Sundhedssektoren skal være i stand til effektivt at opdage lokale såvel som tværgående cyber- og informationssikkerhedshændelser. Derfor er der behov for løbende at overvåge og analysere aktiviteten på såvel den fælles som den lokale it-infrastruktur med henblik på at opdage og håndtere uautoriseret eller uregelmæssig aktivitet. Som et første led i arbejdet med at afdække potentialet i at etablere fælles funktioner til overvågning og analyse af aktivitet igangsætter DCIS i samarbejde med sektorens aktører en afdækning af sundhedssektorens samlede behov på området. Dette skal føre frem til, at der kan træffes beslutning om, hvordan funktionerne bedst etableres.

INITIATIV 3.3.

Effektiv håndtering af mistanke om hændelser

Sundhedssektorens aktører kan opleve tilfælde, hvor medarbejdere – fx sundhedsprofessionelle og it-teknikere – eller eksterne aktører får mistanke om, at der kan have fundet en cyber- og informationssikkerhedshændelse sted, eller en hændelse kan være under opsejling. For at sikre at sektorens aktører er i stand til hurtigt og effektivt at reagere på en sådan mistanke, skal der hos hver aktør fastlægges klare procedurer for modtagelse og håndtering af henvendelser om mulige cyber- og informationssikkerhedshændelser. Udgifter hertil afholdes inden for aktørernes egne budgetter.

→ Hvad er en red team-test?

Red team-tests tester en organisations cyber- og informationssikkerhed og -beredskab gennem scenariebaserede angreb fra såkaldt etiske hackere (eller white hat-hackere), som påtager sig de fjendtlige aktørers rolle og forsøger at finde en vej ind i organisationen. Til forskel fra fx sårbarhedsscanninger og penetrationstests fokuserer denne type test ikke blot på den tekniske angrebsflade, men på alle sprækkerne i forsvaret og tester dermed også andre parametre så som organisationens fysiske sikkerhed og dens medarbejderes agtpågivenhed.

INITIATIV 3.1

"Det er nødvendigt at gennemføre regel
mæssige tests af sikkerheden i sund
hedssektorens systemer og udstyr.

SPOR 4 - HÅNDTERE

Hurtig håndtering i tilfælde af angreb og hændelser

I tilfælde af at sikkerheden – på trods af forudseende og forebyggende initiativer – alligevel kompromitteres gennem fx et cyberangreb eller et utilsigtet brud på informationssikkerheden, skal sektoren hurtigt kunne genoprette systemer og komme tilbage til normalen, således at patientbehandling kan genoptages.

SPOR 4

Det handler om kompetencer, værktøjer og den rette organisation

For at potentielle cyber- og informationssikkerhedshændelser får mindst mulig indflydelse på sektorens opgaveudførsel, skal de håndteres hurtigt, effektivt og præcist. Hændelsen skal inddæmmes og afsondres, så skaden begrænses, og sektorens øvrige systemer og funktioner påvirkes i mindst muligt omfang.

Sektorens aktører skal både i fællesskab og lokalt løfte håndtering og beredskab i forhold til cyber- og informationssikkerhedshændelser. I denne henseende udgør det eksisterende beredskab i sundhedssektoren et solidt og gennemprøvet fundament at bygge videre på. Det er dog nødvendigt også at styrke kapaciteten i sektoren som helhed til at håndtere cyber- og informationssikkerhedshændelser med de rette kompetencer og værktøjer. Dette skal bidrage til en styrket, koordineret indsats i forhold til både akut håndtering af konkrete sikkerhedshændelser og et tværgående beredskab, så de implicerede systemer og datas fortrolighed, integritet og tilgængelighed kan genoprettes.

Hændelsen skal inddæmmes og afsondres, så skaden begrænses, og sektorens øvrige systemer og funktioner påvirkes mindst muligt.

Et væsentlig element heri er gennemtestede kommunikationslinjer, så sektorens aktører ved, hvor og til hvem de skal henvende sig, og hvad der kan gøres lokalt i tilfælde af en hændelse. Som led heri skal sektorens aktører såvel som deres medarbejdere have en fælles forståelse af opgave- og ansvarsfordeling samt konkrete og veletablerede aftaler for håndtering af cyber- og informationssikkerhedshændelser.

Det er afgørende at sikre læring, så sektorens hændelseshåndtering og beredskab løbende styrkes og følger med udviklingen i trusler og risici. Læring bør ske både i tilfælde af en hændelse, således at alle relevante parter kan få gavn af erfaringerne fra håndteringen af hændelsen, og gennem tilbagevendende tests af det fælles beredskab. Læringen skal dermed bidrage til, at sektoren løbende styrker sin samlede kapacitet til at forudsige, forebygge og opdage og håndtere cyber- og informationssikkerhedshændelser.

→ Indberetning af hændelser

I tilfælde af en cyber- og informationssikkerhedshændelse har sundhedssektorens aktører i mange tilfælde pligt til at indberette hændelsen til de relevante myndigheder:

- I regi af NIS-direktivet skal operatører af væsentlige tjenester i sundhedssektoren hurtigst muligt indberette hændelser, der har væsentlige konsekvenser for kontinuiteten af den væsentlige tjeneste, til Sundhedsdatastyrelsen og Center for Cybersikkerhed.
- I tilfælde af et brud på persondatasikkerheden skal sundhedssektorens aktører i regi af EU's databeskyttelsesforordning indberette bruddet til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer efter den dataansvarlige er blevet bekendt med bruddet.

Indberetning af cyber- og informationssikkerhedshændelser skal ske via Den Fælles Løsning til Indberetning af It-sikkerhedshændelser (FLIIS) på www.virk.dk.

Varsling af udlandet om cyberangreb: Når der konstateres et cyberangreb mod den danske sundhedssektor, er det afgørende, at de rette udenlandske myndigheder orienteres rettidigt om angrebet, således at sundhedsmyndighederne i de pågældende lande kan træffe de rette foranstaltninger for at imødegå, at angrebet også rammer der.

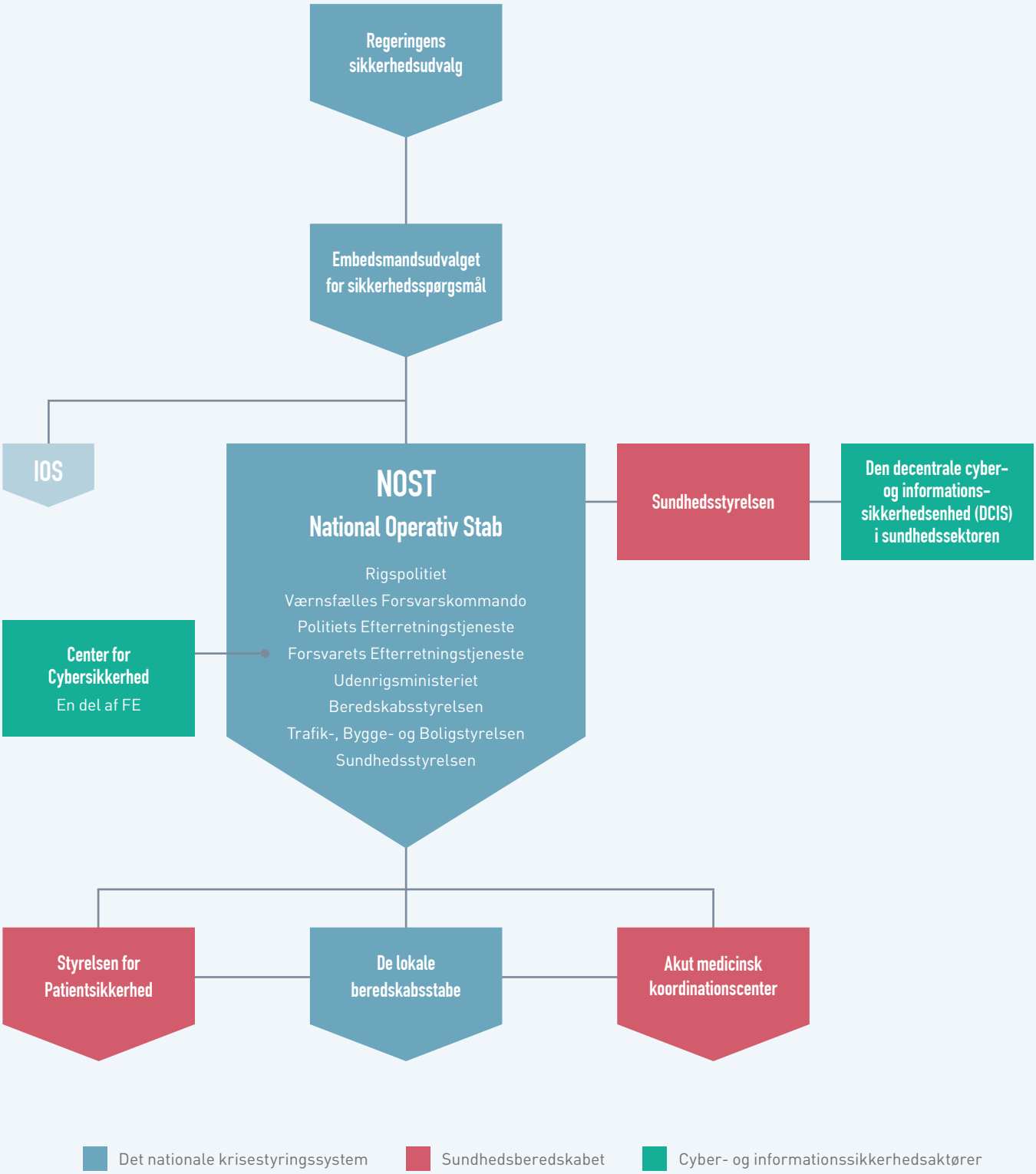
SPOR 4 – HÅNDTERE

→ Initiativer

- **Hændelseshåndtering**
- **Etablering af tværgående it- og cyberberedskab**
- **Beredskabsøvelser for fælles systemer og forsyningskæder**

FIGUR

National krisestyring og sundhedsberedskab, inkl. cyber- og informationssikkerhedsaktører



Roller og ansvar

Regeringens sikkerhedsudvalg
Det øverste sikkerhedspolitiske organ: Statsministeren (formand), udenrigsministeren, justitsministeren og forsvarsministeren.

Embedsmandsudvalget
Rådgiver Regeringens sikkerhedsudvalg: Relevante departementschefer og chefer for Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste.

International Operativ Stab (IOS)
Koordinerer indsatsen over for danskere ved større hændelser i udlandet.

National Operativ Stab (NOST)
Koordinerer ved større hændelser i Danmark og sikrer information til regeringen, offentligheden og relevante myndigheder. NOST består af Rigspolitiet, Værnsfælles Forsvarskommando, Udenrigsministeriet samt en række andre myndigheder (se model). Øvrige myndigheder kan indkaldes ved behov.

De lokale beredskabsstabe
Koordinerer den lokale indsats ved ekstraordinære hændelser. I de lokale beredskabsstabe indgår politiet, totalforsvarsregionen, Beredskabsstyrelsens regionale beredskabscenter, regionens sundhedsberedskab samt de kommunale beredskaber. Styrelsen for Patientsikkerhed er ad hoc-medlem.

Sundhedsstyrelsen
Sundhedsstyrelsen har det faglige sektoransvar for sundhedsberedskabet i Danmark. Det indebærer blandt andet rådgivning af Sundheds- og Ældreministeriet, kommuner og regioner om sundhedsberedskab. Sundhedsstyrelsen vil ved en konkret hændelse koordinere indsatsen inden for sundhedssektoren med andre sektorer.

Styrelsen for Patientsikkerhed
Rådgiver lokale myndigheder om sundhedsforhold og varetager beredskabsopgaver i samarbejde med Sundhedsstyrelsen.

Akut Medicinsk Koordinationscenter (AMK)
Leder sundhedsindsatsen inden for regionen ved en større hændelse. AMK står for kommunikationen mellem sundhedsmyndighederne og skadestedet.

Center for Cybersikkerhed
Center for Cybersikkerhed vil som en del af Forsvarets Efterretningstjeneste deltage i NOST i tilfælde af større, tværgående cyber- og informationssikkerhedshændelser af national betydning.

Den decentrale cyber- og informationssikkerhedsenhed (DCIS) i sundhedssektoren
I tilfælde af en cyber- og informationshændelse i sundhedssektoren, hvor der er behov for at aktivere beredskabet, vil Sundhedsstyrelsen og DCIS samarbejde om beredskabet.

INITIATIV 4.1.

Hændelseshåndtering

I tilfælde af en cyber- og informationssikkerhedshændelse skal sundhedssektoren være i stand til hurtigt og sikkert at håndtere hændelsen og genoprette almindelig drift. Alle aktører i sektoren skal derfor have relevante funktioner og procedurer til håndtering af cyber- og informationssikkerhedshændelser i eget systemlandskab på plads. For at bidrage til dette gennemfører DCIS i første halvår 2019 en analyse af sundhedssektorens eksisterende aftaler og funktioner til håndtering af hændelser lokalt såvel som ved tværgående hændelser. DCIS skal desuden i samarbejde med sektorens aktører fastlægge hændelsesklassifikationer som udgangspunkt for en afklaring af behovet for, at der i sektoren etableres fælles funktioner til håndtering af avancerede hændelser (forensics). Etablering heraf forudsætter særskilt aftale.

INITIATIV 4.2.

Etablering af tværgående it- og cyberberedskab

For at sikre at sektoren hurtigst muligt formår at overkomme effekten af en større, tværgående cyber- og informationssikkerhedshændelse, er der behov for tværgående processer for effektiv og koordineret hændelseshåndtering. Derfor igangsætter DCIS i samarbejde med sektorens aktører i første halvår af 2019 et arbejde med at beskrive en model for etableringen af et tværgående samarbejde om et it- og cyberberedskab for sektorens fælles systemer og forsyningskæder. Arbejdet bygger oven på og koordineres med de eksisterende lokale it- og cyberberedskaber ved sektorens aktører, det generelle sundhedsberedskab samt den nationale krisestyringsorganisation.

INITIATIV 4.3.

Beredskabsøvelser for fælles systemer og forsyningskæder

Sundhedssektorens skal være i stand til på effektiv og koordineret vis at håndtere cyber- og informationssikkerhedshændelser, når de indtræffer. For at sikre dette skal samarbejdet i sektorens tværgående it- og cyberberedskab kontinuerligt efterprøves, og læring herfra skal videndeles og indarbejdes i processer for hændelseshåndtering på tværgående såvel som lokalt plan. De tværgående it- og cyberberedskabsøvelser skal omfatte hændelser, som rammer tværgående it-systemer og it-infrastrukturkomponenter, der leverer forretningskritiske it-tjenester til én eller flere af sundhedssektorens aktører. Aktørernes deltagelse i øvelserne sker inden for egne budgetter.

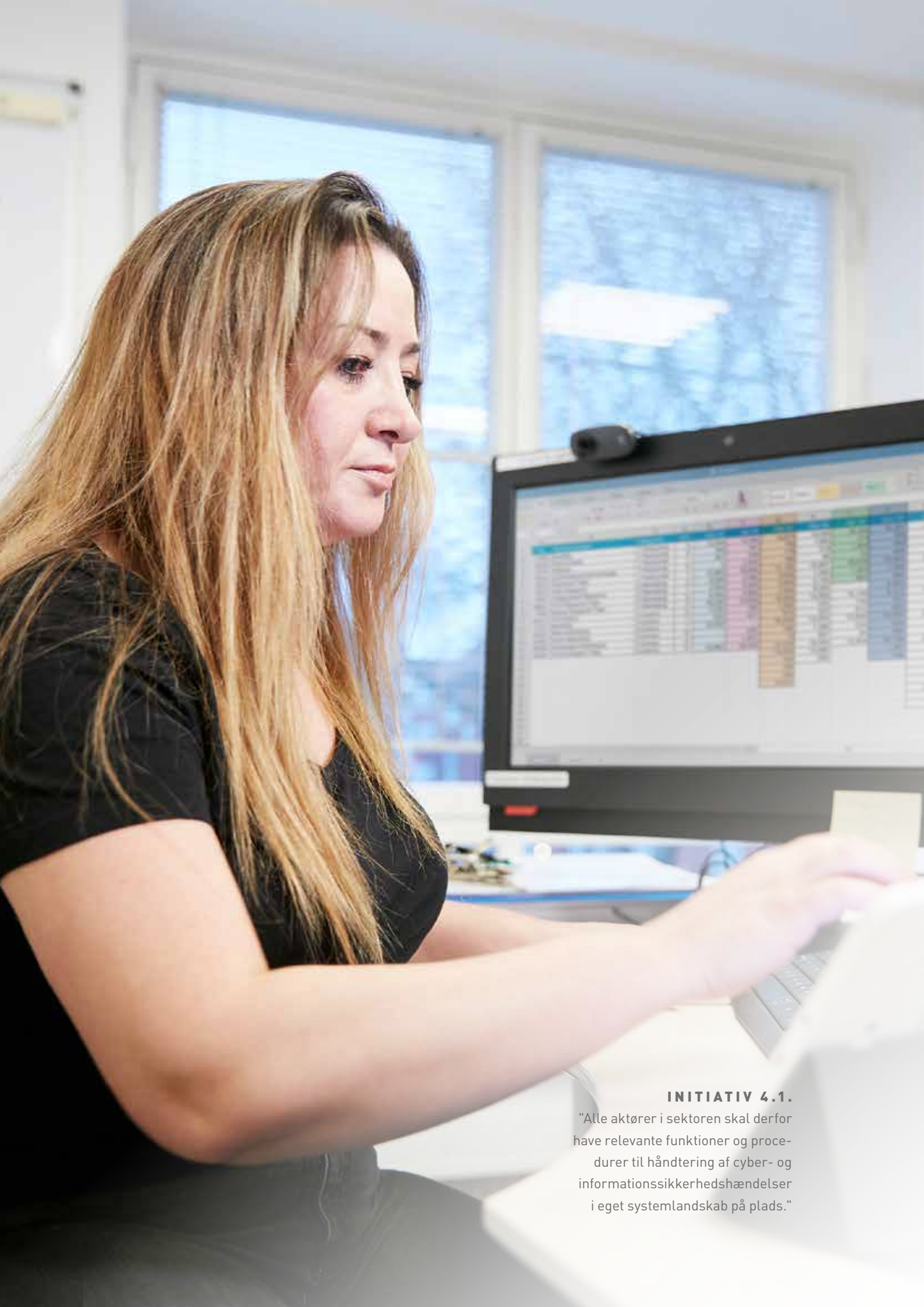
→ Beredskabets aktiveringstrin

Såvel det nationale som sundhedssektorens beredskab anvender tre trin for aktivering:

Trin 1 – Informationsberedskab: Der vurderes endnu ikke at være behov for at aktivere og etablere en krisestab. Chefer og nøglepersoner bør være opmærksomme. Det kan fx være relevant at foretage skærpet overvågning, informere relevante medarbejdere og gennemgå procedurerne i beredskabsplanen.

Trin 2 – Stabsberedskab: En hændelse eller trussel kan medføre, at krisestabe skal kunne mødes inden for 2 timer for at koordinere myndighedernes opgaver. Det kan fx være relevant at mødes jævnligt i en kreds af ledere og medarbejdere, dog stadig uden at etablere en egentlig krisestab og kriseledelse.

Trin 3 – Operationsberedskab: Etablering af en krisestab, som samles for at varetage samtlige krisestyringsrelevante opgaver.



INITIATIV 4.1.

"Alle aktører i sektoren skal derfor have relevante funktioner og procedurer til håndtering af cyber- og informationssikkerhedshændelser i eget systemlandskab på plads."

Udmøntning og løbende evaluering, prioritering og udvikling

Strategien sætter en ambitiøs retning for at styrke sundhedssektorens samlede kapacitet i forhold til cyber- og informationssikkerhed og dermed bidrage til at fremtidssikre det danske sundhedsvæsen. Det er en krævende opgave, der kræver, at der løbende følges op på udmøntningen af strategien og dens initiativer.

Strategien er politisk aftalt mellem Sundheds- og Ældreministeriet, KL og Danske Regioner. Arbejdet med at følge op på strategien og dens initiativer forankres i styregruppen for udarbejdelsen af strategien, som videreføres med enkelte justeringer af sammensætningen; herunder at styregruppen udvides med et medlem fra Sundhedsstyrelsens sundhedsberedskab og et medlem fra Praktiserende Lægers Organisation. Styregruppen mødes fire gange årligt og drøfter udmøntningen af strategien og afrapporterer to gange om året til Den nationale bestyrelse for sundheds-it om fremdriften i dette arbejde.

Strategien sætter en ambitiøs retning for at styrke sundhedssektorens samlede kapacitet i forhold til cyber- og informationssikkerhed og dermed bidrage til at fremtidssikre det danske sundhedsvæsen.

Cyber- og informationssikkerhed er et område under konstant udvikling, og nye udfordringer og trusler såvel som nye muligheder kan opstå, som ikke fandtes ved strategiens lancering. Derudover ændrer sektoren sig også løbende. Derfor skal strategiens retning og initiativer evalueres årligt baseret på opdaterede trussels-, sårbarheds- og risikovurderinger af sundhedssektoren. Til det brug udarbejdes et samlet årshjul, der fastlægger rækkefølgen af trinene i processen. På den baggrund gennemføres den endelige vurdering af, om strategien og de eksisterende initiativer er dækkende.

Med henblik på at sikre gennemsigtighed og fremdrift i arbejdet med at styrke sundhedssektorens kapacitet i forhold til cyber- og informationssikkerhed skal der årligt gennemføres et antal eksterne reviews af dele af sektorens cyber- og informationssikkerhedsindsats. Ved at benytte en ekstern part sikres der uafhængighed

→ Snitflade mellem Center for Cybersikkerhed og sundhedssektorens aktører

Center for Cybersikkerhed spiller primært en rolle i forhold til indsatsen i sundhedssektoren gennem rådgivning og bistand. Center for Cybersikkerhed udarbejder trusselsvurderinger – såvel nationale som specifikt for sundhedssektoren – et nationalt cybersituationsbillede, formidler varsler om løbende trends og aktuelle sikkerhedshændelser både til og fra sundhedssektoren i forhold til de øvrige sektorer og centrets internationale samarbejdspartnere. Som følge af sektoransvarsprincippet påhviler ansvaret for cyber- og informationssikkerhed i sundhedssektoren sundhedssektorens aktører – også i forbindelse med håndtering af konkrete cyber- og informationssikkerhedshændelser. Center for Cybersikkerhed bistår udelukkende med egentlig hændelseshåndtering i de tilfælde, hvor centret vurderer, at en hændelse har tværsektoriel og national relevans; og i disse tilfælde skal Center for Cybersikkerheds bistand ses som et supplement til sektorens egen håndtering og indsats.

DCIS er en ny enhed, der samler trådene, koordinerer analyser og monitorerer indsatser

Som led i arbejdet med at styrke den samlede cybersikkerhedsindsats i sektoren er der den 1. november 2018 oprettet en decentral cyber- og informationssikkerhedsenhed (DCIS) i Sundhedsdatastyrelsen. Enheden vil udgøres af 12 14 ansatte og får til opgave at samle og koordinere arbejdet i sektoren og skal bl.a. fungere som sektorens bindeled til Center for Cybersikkerhed. Herudover har enheden til ansvar at understøtte sektorens implementering af strategien, herunder være tovholder på gennemførelsen af de aftalte analyser, koordinere varsler, udarbejde vejledninger og informationsmateriale, facilitere videndeling mv.

i forhold til den decentrale cyber- og informationssikkerhedsenhed (DCIS), da opgaverne i denne enhed også vil være omfattet af de eksterne reviews.

Endelig skal den decentrale cyber- og informationssikkerhedsenhed (DCIS) stå for, at der etableres en metode til indsamling af viden i hele sektoren om antallet af cyber- og informationssikkerhedshændelser og karakteren heraf med henblik på at måle effekten af sektorens samlede indsats. Opgørelserne skal bl.a. danne baggrund for vurderinger af, om cyber- og informationssikkerhedsindsatsen i sektoren er tilstrækkelig. Der skal i den forbindelse tages hensyn til, at oplysninger om antallet af angreb og sikkerhedshændelser skal håndteres fortroligt.

En række af strategiens aktiviteter baserer sig på indsatser, som allerede løftes hos de enkelte aktører, og de finansieres og tilrettelægges derfor lokalt inden for aktørernes egne budgetter. Det gælder fx udarbejdelsen af sårbarheds- og risikovurderinger, awareness- og kompetenceudvikling for relevante faggrupper mv. Tilsvarende afholdes aktiviteter i den decentrale cyber- og informationssikkerhed (DCIS) for sundhedssektoren, herunder gennemførsel af analyser, udarbejdelse af vejledninger, facilitering af videndeling mv. inden for enhedens budget.

Med strategien lægger sundhedssektorens parter samtidig op til en række nye, fælles aktiviteter, som beror på en afdækning af sektorens konkrete behov og afsøgning af finansiering. Det indebærer, at sundhedssektorens parter på et senere tidspunkt kan aftale finansiering af de nye, fælles aktiviteter. Finansiering af de nye, fælles aktiviteter indgår dermed i den løbende prioritering og justering af sektorens indsats – i takt med udviklingen af nye teknologier, i trusselsbilledet og i sektoren selv.

Strategien sætter en fælles dagsorden for cyber- og informationssikkerhed i sundhedssektoren. Snarere end et definitivt katalog af aktiviteter er strategien derfor tænkt som et dynamisk dokument med retningsgivende, strategiske initiativer, der skal bidrage til, at sundhedssektorens parter i fælleskab fortsat kan udvikle og styrke sektorens samlede cyber- og informationssikkerhedsindsats.

MIX
Paper from responsible sources
FSC® C134744
FSC
www.fsc.org

Tak til Region Nordjylland, Aalborg Universitetshospital, hjemmeplejen i Københavns Kommune samt alle deltagere i fotograferingen.

SUNDHEDS- OG ÆLDREMINISTERIET

KL

DANSKE REGIONER

Strategi for cyber- og informationssikkerhed i sundhedssektoren

2019 2022