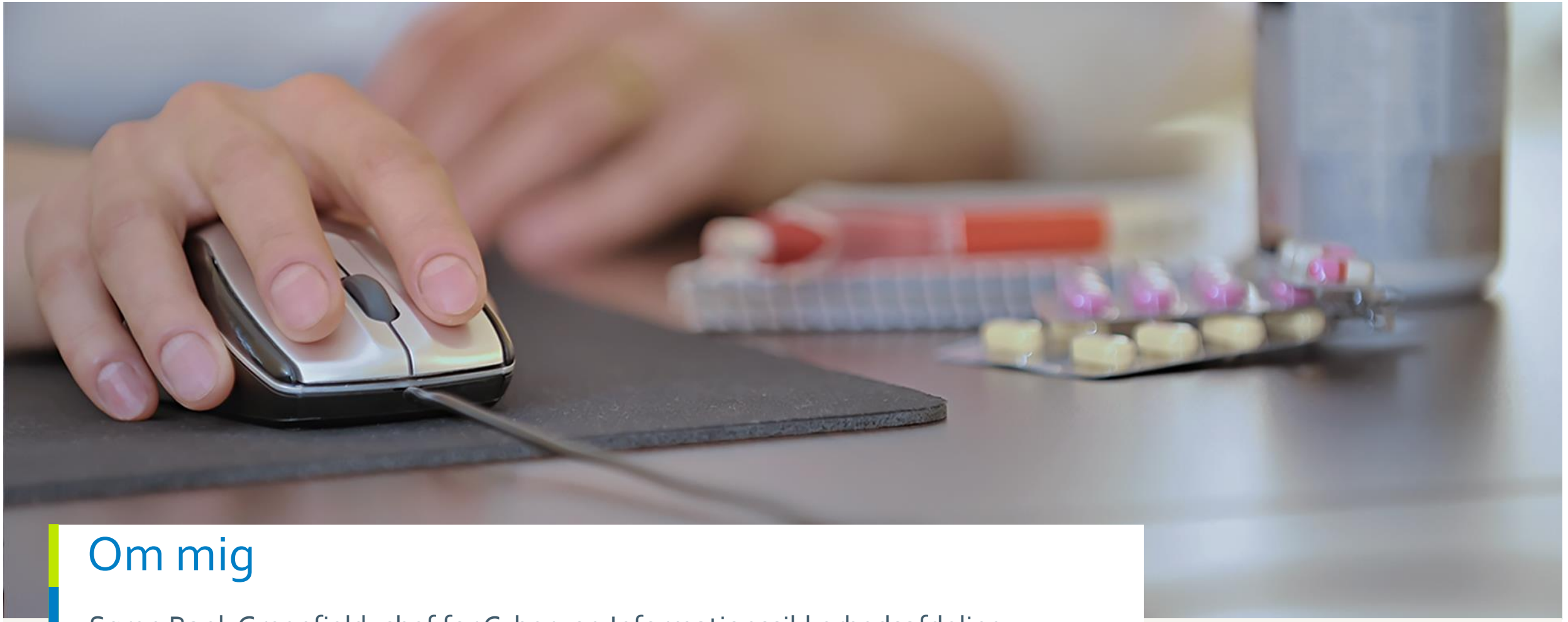
Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2021

Udmøntning og hvorfor dog sådan en strategi ☺

SUNDHEDSDATA-
STYRELSEN



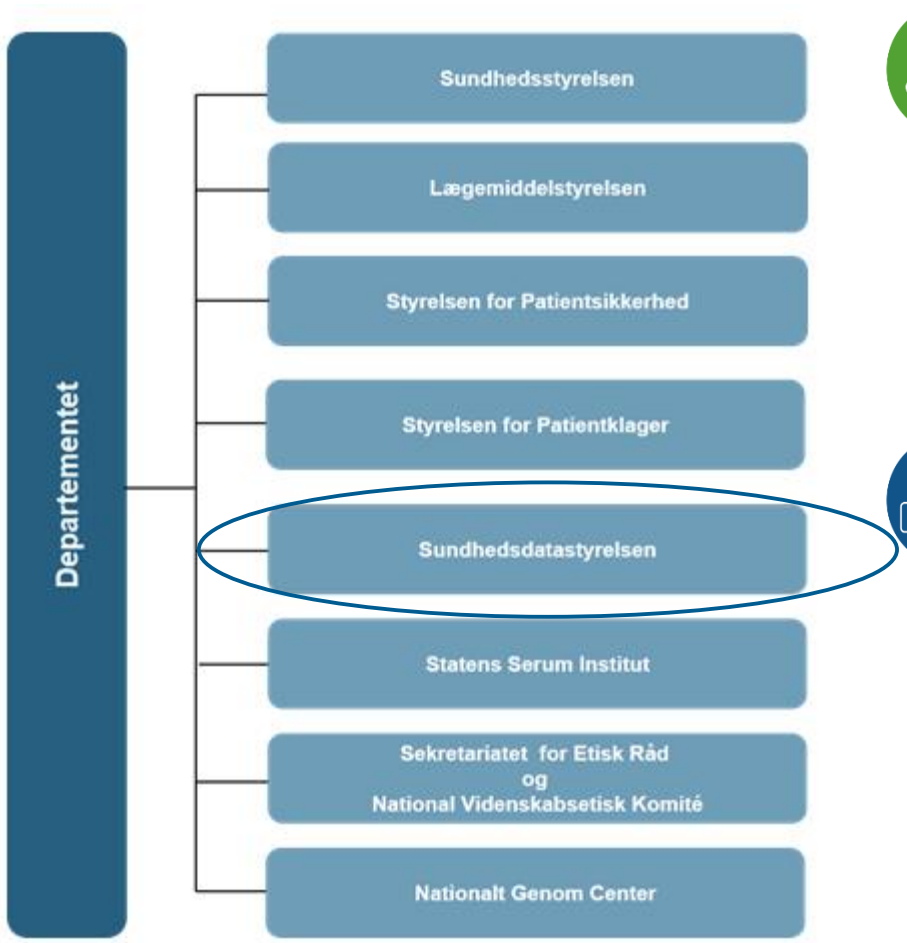
Om mig

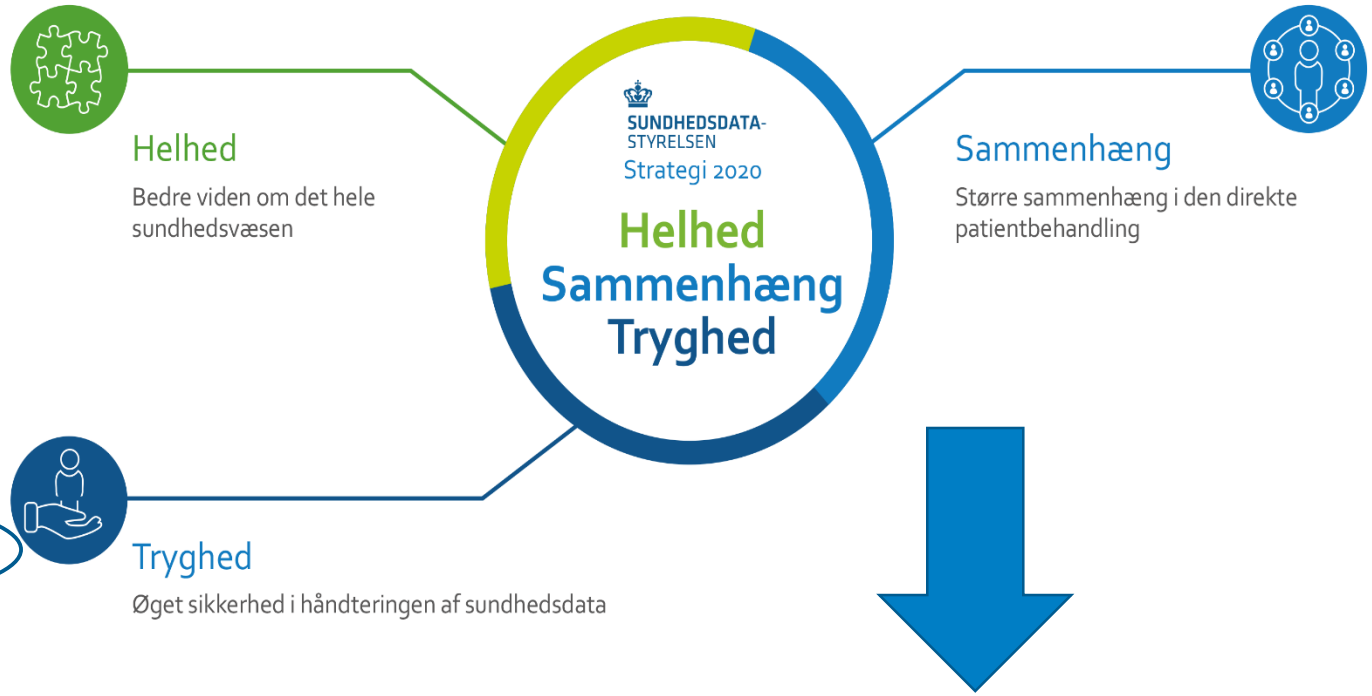
Søren Bank Greenfield, chef for Cyber- og Informationssikkerhedsafdeling.

Faglig baggrund som operationel sikkerhedschef, CISO og viden inden for brugervendt infrastruktur, brugerstyring og cybersikkerhed.
Har før været i KBH Amt, Glostrup hospital og Region H (CIMT).

SUNDHEDSDATA-
STYRELSEN

Sundheds- og Ældreministeriet



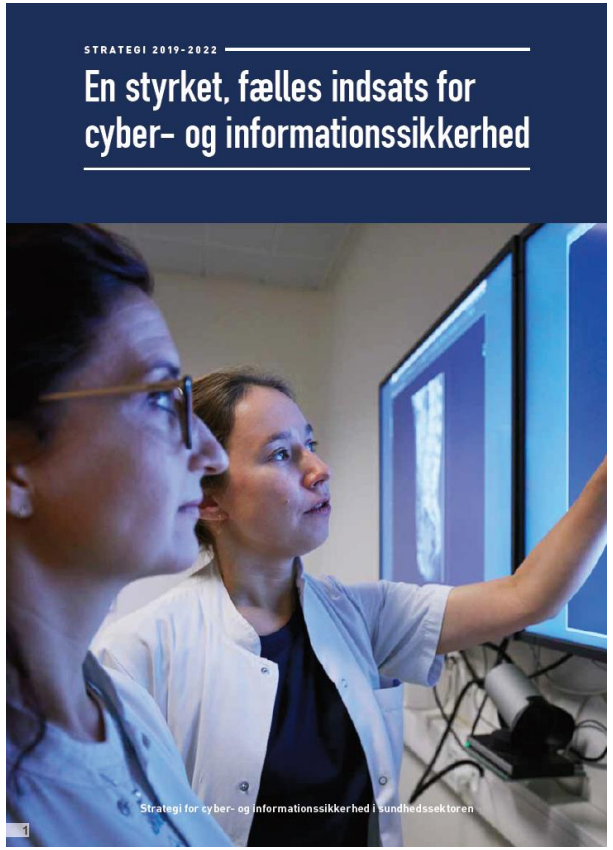


Afdelingen har til opgave at facilitere og koordinere den fælles indsat for at **styrke og øge** kapabiliteten og kapaciteten indenfor Cyber- og Informationssikkerhed i Sundhedsdatastyrelsen, Sundheds- og Ældreministeriet og **på tværs af sundhedsvæsenet**

Vi vil styrke den langsigtede opbygning af kapacitet og den fælles koordinerede indsats

Den nationale strategi for cyber- og informationssikkerhed fra maj 2018

Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022



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

SUNDHEDSDATA-STYRELSEN

National cyber- og informationssikkerhedsstrategi

- Udpeger finans, tele, energi, søfart, transport og sundhed som samfundskritiske sektorer

- Fokus på opbygning af en stærkere decentral kapabilitet på cyber- og informationssikkerhedsområdet gennem:

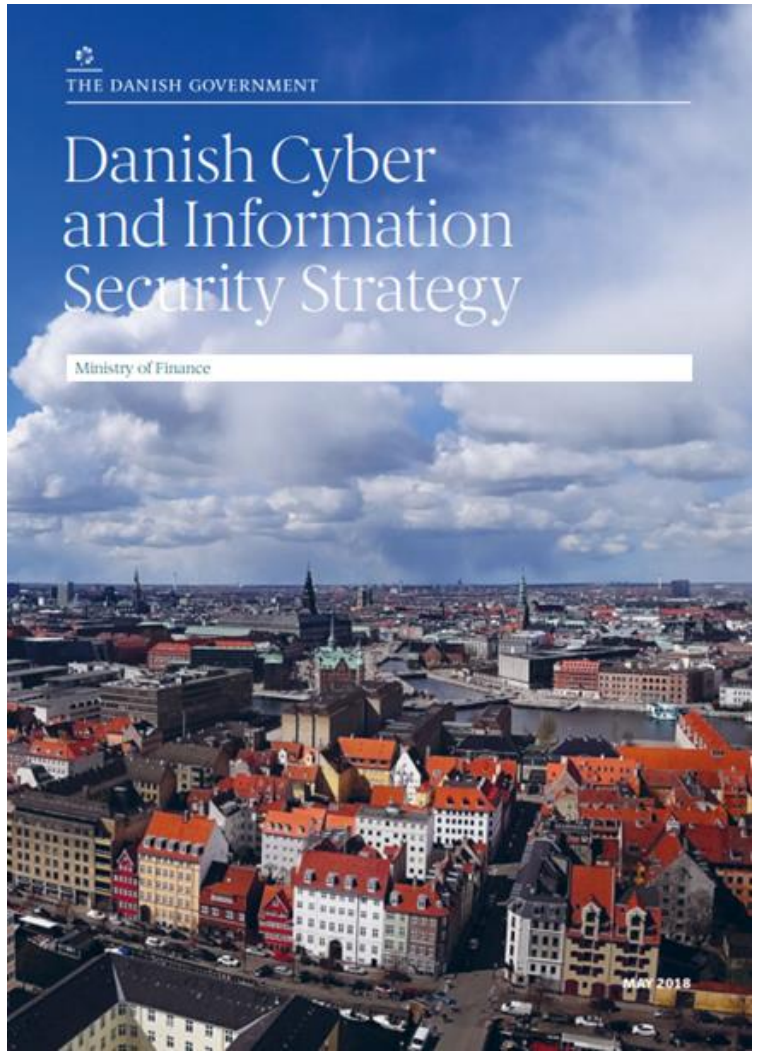
  - Oprettelse af sektorenheder "der kan bidrage til gennemførelsen af sektorvise trusselsvurderinger, overvågning, beredskabsøvelser, sikkerhedsopbygning, vidensdeling, vejledning mv."

  - Udarbejdelse af delstrategier, som skal "sikre et forsvarligt informationssikkerhedsmæssigt beredskab inden for egen sektor"

Hvad med vand og spildevand?

Forsyning og fødevare?

Sektoransvarsprincippet:
"Den myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret under cyber- og informationssikkerhedshændelser. Ansvaret for cyber- og informationssikkerhed i sundhedssektoren ligger således hos sundhedssektorens aktører."



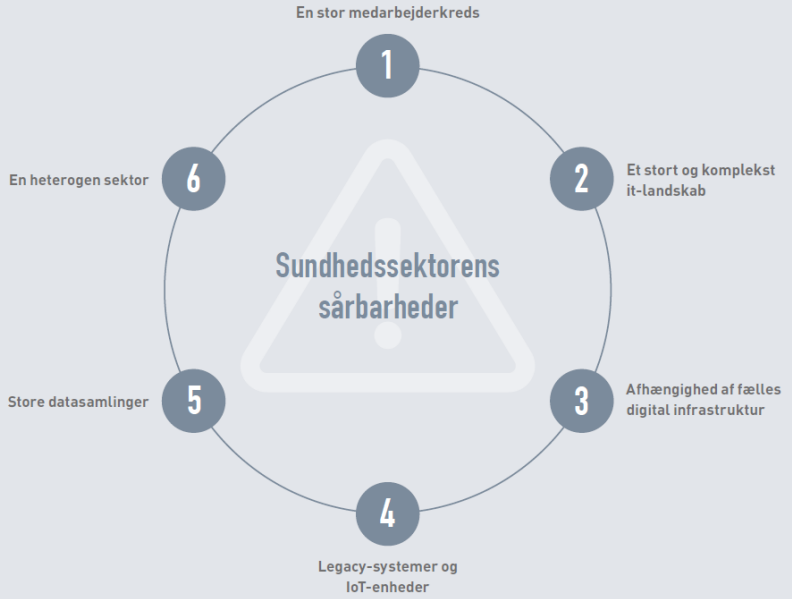
Strategiens formål

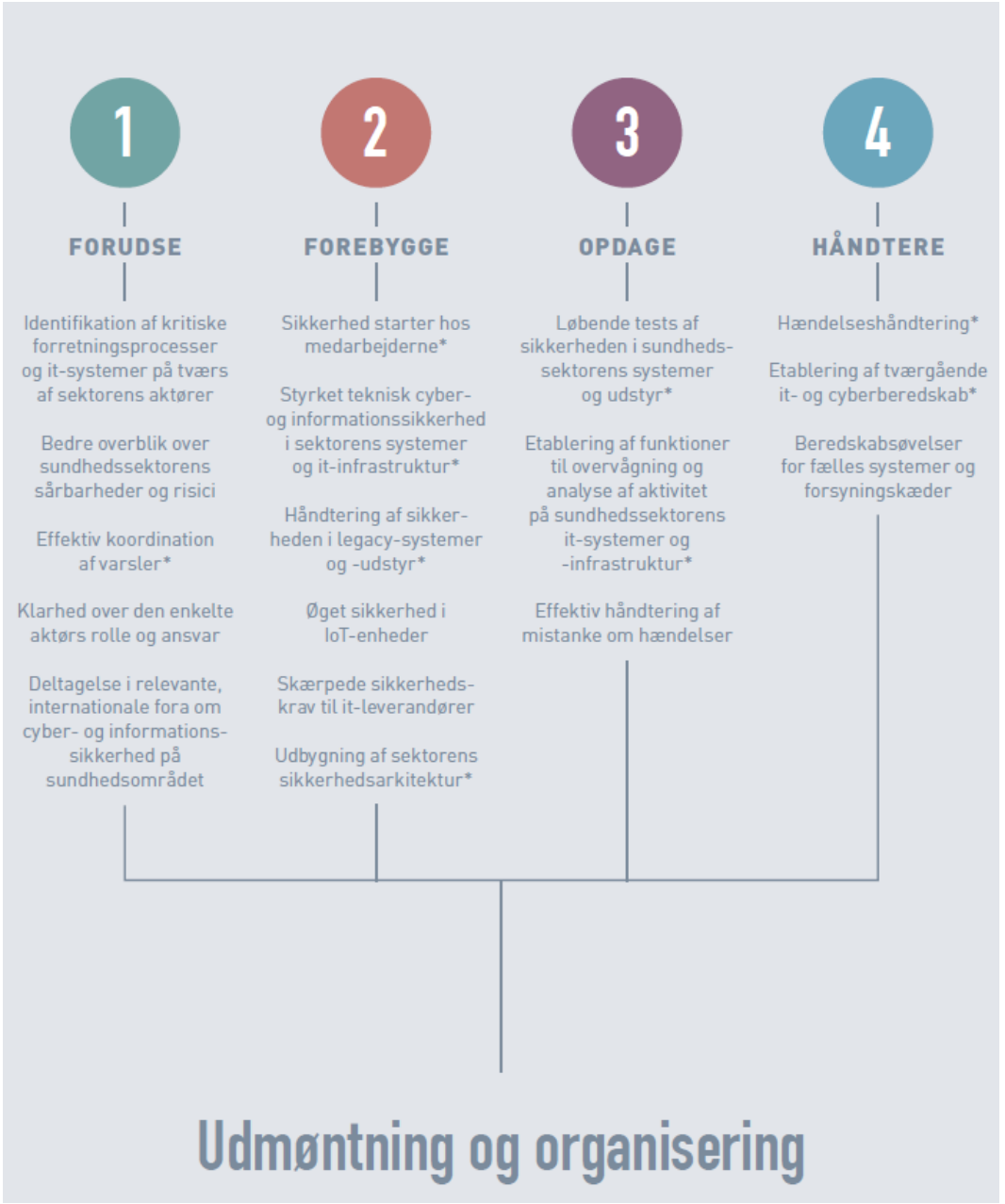
- At sikre en helhedsorienteret og risiko-baseret tilgang til cyber- og informationssikkerhed

- At styrke sektorens samlede, fælles evne til at forebygge, forudse, opdage og håndtere cyber- og informationssikkerhedshændelser

FIGUR

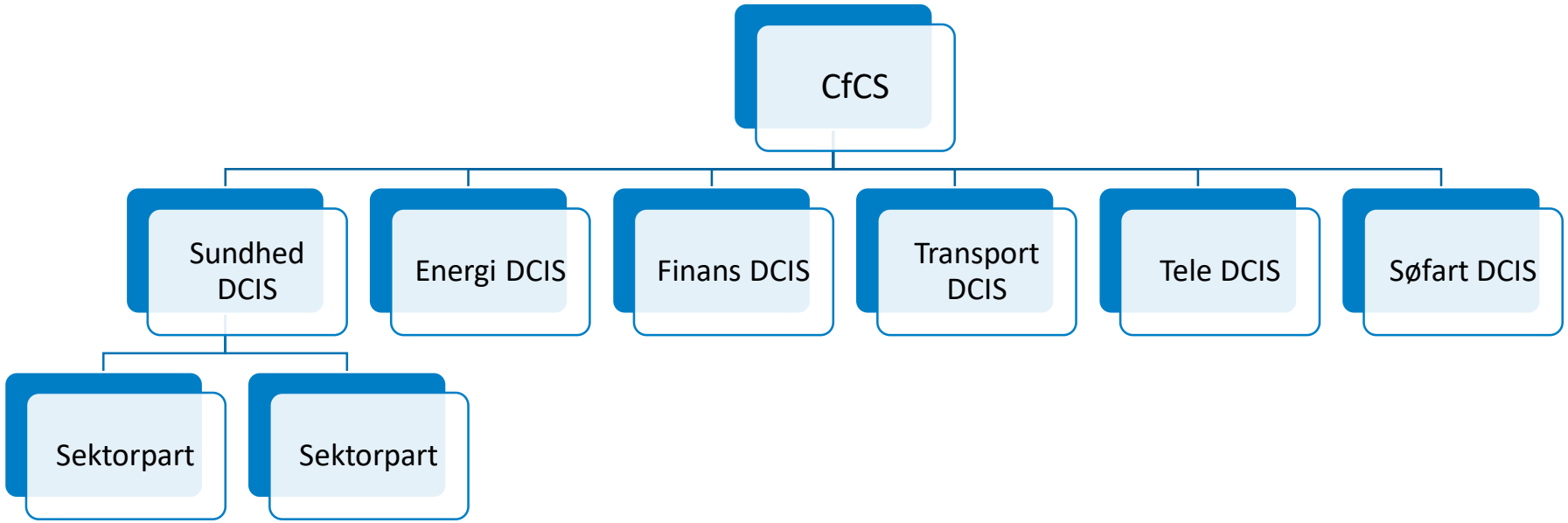
Seks overordnede sårbarheder





Decentral Cyber- og Informationssikkerhedsenhed (DCIS)

- Samlende kommunikationspunkt for sektoren (myndigheder, virksomheder og organisationer) og for CfCS
- Vedligeholder kontaktliste for sektoren til brug for hændelseshåndtering
- Vedligeholder oversigt over sektorens kritiske infrastrukturelementer og tjenester
- Indgår i operative arbejdsgrupper ved tværgående hændelser
- Formidler varsler fra CfCS



Organisationen

Styregruppe

Sundhedsdatastyrelsen

Sundheds- og Ældreministeriet, Danske Regioner, Region Midt, Region Nord, Region Hovedstaden, KL, Digitaliseringsstyrelsen, Center for Cybersikkerhed, MedCom, Sundhed.dk, PLO, Sundhedsstyrelsen

DCIS

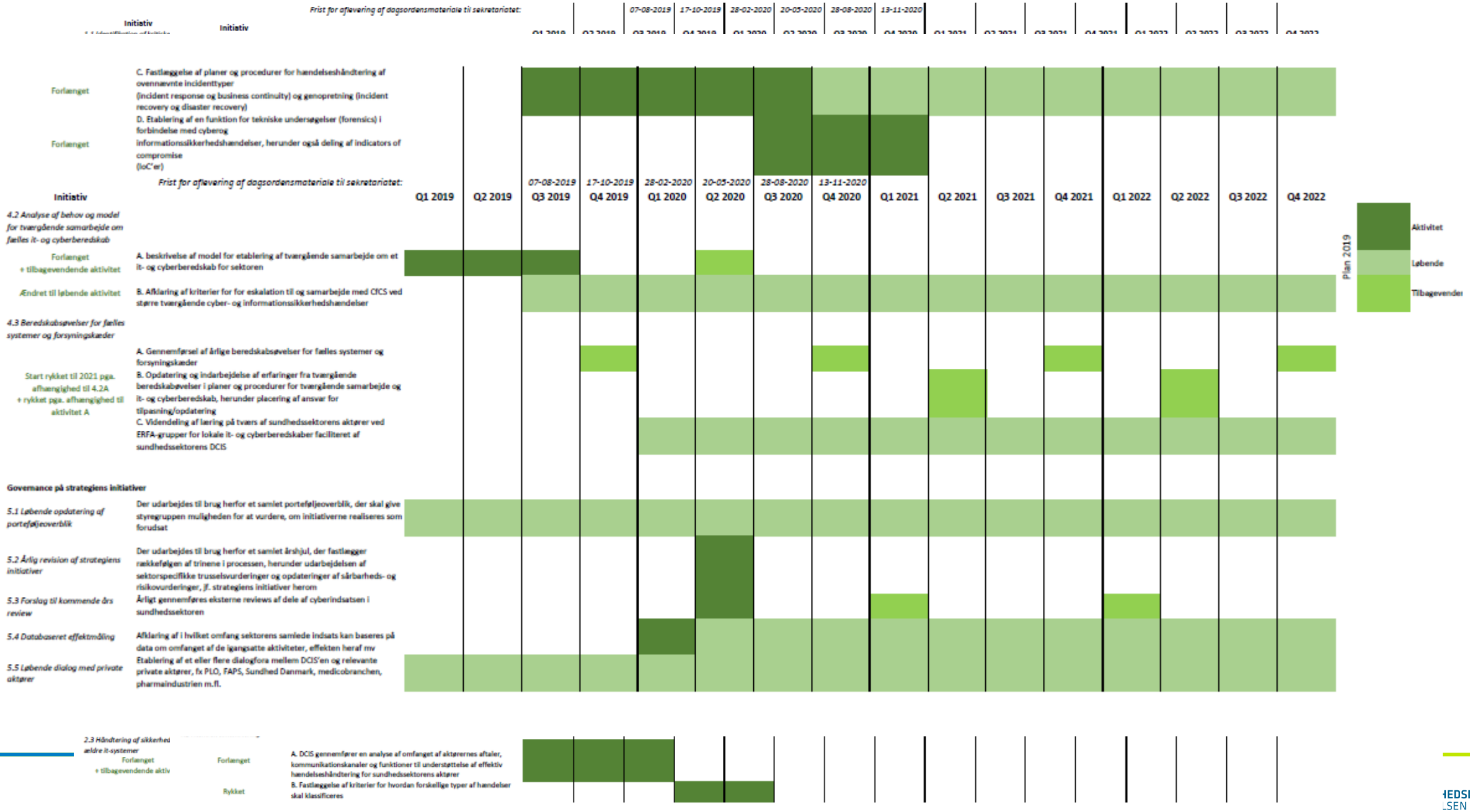
Programledelse

Sekretariat

Hovedinitiativerne

1. Forudse hændelser	2. Forebygge hændelser	3. Opdage hændelser	4. Håndtere hændelser	5. Styring og effekt
1.1 Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører 1.2 Bedre overblik over sundheds-sektorens sårbarheder og risici 1.3 Effektiv koordination af varsler 1.4 Klarhed over den enkelte aktørs rolle og ansvar 1.5 Deltagelse i relevante internationale fora om cyber- og informationssikkerhed på sundhedsområdet	2.1 Sikkerhed starter med medarbejderne 2.2 Styrket teknisk sikkerhed i sektorens løsninger og it-infrastruktur 2.3 Håndtering af sikkerheden i ældre it-systemer og –udstyr 2.4 Øget sikkerhed i online medicinsk udstyr 2.5 Skærpede sikkerhedskrav til it-leverandører 2.6 Udbygning af sektorens sikkerhedsarkitektur	3.1 Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr 3.2 Etablering af overvågnings- og analysefunktioner 3.3 Effektiv håndtering af mistanke om hændelser	4.1 Hændelseshåndtering 4.2 Tværgående samarbejde om fælles it- og cyberberedskab 4.3 Beredskabsøvelser for fælles systemer og forsyningskæder	5A løbende opdatering af porteføljeoverblik 5B Årshjul cyklus 5C Forslag til kommende års review 5D Databaseret effektmåling 5E Løbende dialog med private aktører

Tidsplan for udmøntning



Organisationen

Styregruppe

Sundhedsdatastyrelsen

Sundheds- og Ældreministeriet, Danske Regioner, Region Midt, Region Nord, Region Hovedstaden, KL, Digitaliseringsstyrelsen, Center for Cybersikkerhed, MedCom, Sundhed.dk, PLO, Sundhedsstyrelsen

Programledelse

Sekretariat

Hovedinitiativerne

1. Forudse hændelser

1.1 Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører
1.2 Bedre overblik over sundheds-sektorens sårbarheder og risici
1.3 Effektiv koordination af varsler
1.4 Klarhed over den enkelte aktørs rolle og ansvar
1.5 Deltagelse i relevante internationale fora om cyber- og informationssikkerhed på sundhedsområdet

2. Forebygge hændelser

2.1 Sikkerhed starter med medarbejderne
2.2 Styrket teknisk sikkerhed i sektorens løsninger og it-infrastruktur
2.3 Håndtering af sikkerheden i ældre it-systemer og –udstyr
2.4 Øget sikkerhed i online medicinsk udstyr
2.5 Skærpede sikkerhedskrav til it-leverandører
2.6 Udbygning af sektorens sikkerhedsarkitektur

3. Opdage hændelser

3.1 Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr
3.2 Etablering af overvågnings- og analysefunktioner
3.3 Effektiv håndtering af mistanke om hændelser

4. Håndtere hændelser

4.1 Hændelseshåndtering
4.2 Tværgående samarbejde om fælles it- og cyberberedskab
4.3 Beredskabsøvelser for fælles systemer og forsyningskæder

5. Styring og effekt

5A løbende opdatering af porteføljeoverblik
5B Årshjul cyklus
5C Forslag til kommende års review
5D Databaseret effektmåling
5E Løbende dialog med private aktører

1.3 Effektiv koordination af varsler

- Sektorens evne til at forudsige mulige angreb og sikkerhedshændelser skal styrkes ved, at DCIS etablerer en samlet model for effektiv koordination af varsler om mulige angreb og sikkerhedshændelser.

- Besvares:
  - Hvorledes sorteres der i varsler og advarsler?
  - Hvem skal have hvilke informationer?
  - Hvorledes kommer man bedst i kontakt?
  - Hvilket system skal benyttes til at dele informationer?
  - Hvad når man skal kontakte aktører akut?
  - Hvad gør man hvis der ingen internet eller email er? Eller hvad hvis der ikke er nogen telefoner?
  - Skal der oprettes en Cyberhotline? Hvem skal kunne ringe og om hvad?

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.

- Besvares:
  - Hvilke sikkerhedskrav stilles der samlet på sundhedsområdet i Danmark?
  - Hvilke krav er der stillet fra EU? Og hvilke er på vej?
  - Hvilke standarder bliver aktørerne enige om at lægge sig op ad?
  - Hvem betaler den forøgede omkostning, når sikkerheden skal højnes eller bare overholdes?
  - Hvor lang tid skal der gives, før et sikkerhedskrav skal overholdes?
  - Hvordan kan det implementeres på tværs af hele sektoren?

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.

- Besvares:
  - Hvad skal overvåges?
  - Hvem skal analysere?
  - Hvordan får en eventuel central funktion adgang til data fra aktørerne? Skal det være på samme måde?
  - Hvad er DCIS's SAC/SOC's mandat i forhold til fundne sårbarheder og risici?
  - Hvordan skal funktionen bemandes? Skal den være 24/7-365 bemandet?
  - Hvilke services skal funktionen understøtte?
  - Skal der være et "cyberrejsehold"?

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.

- Besvares:
  - Hvem er med i beredskabet?
  - Hvad skal der til for at starte et sådant beredskab?
  - Hvorledes starter man et beredskab for sundhedsvæsenet?
  - Hvordan arbejder dette sammen med de eksisterende beredskaber? Og det sundhedsfaglige?
  - Hvem kan initiere et sundhedssektorbredt beredskab?
  - Hvem er beredskabsleder?
  - Hvordan kommer man i kontakt med hinanden?
  - Hvor bundet er aktørernes ressourcer af beredskabet?

Hvorfor er det relevant for mig?

Klarer DCIS det ikke bare?

SUNDHEDSDATA-
STYRELSEN

Cyber strategien i sundhedssektoren

JANUAR 2018

UNCLASSIFIED

Healthcare Data

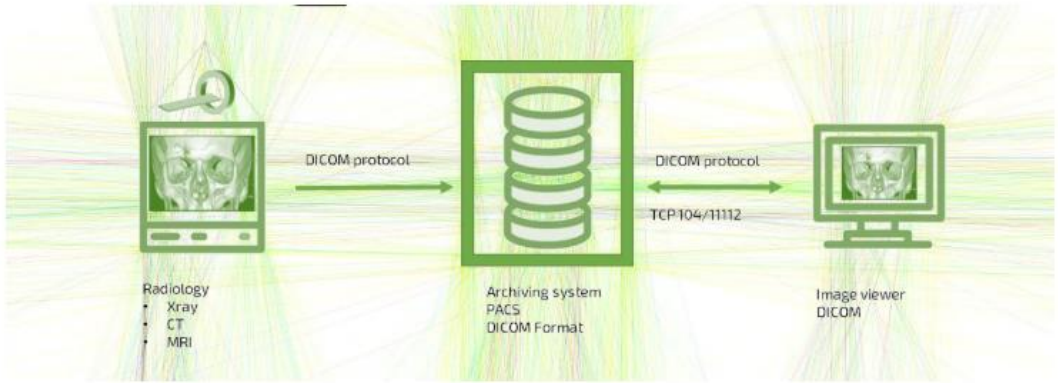
TLP:WHITE

- Research indicates healthcare records attract some of the highest prices on the dark web
  - Estimated mean value of healthcare record on criminal markets: **$250** (up to $1000)

- Mere og mere nuanceret og kompleks trusselsbillede
- Sundhedsdata er i høj kurs hos cyberkriminelle

400 Million Medical Radiological Images Exposed on the Internet

By Ionut Ilascu September 18, 2019 02:28 AM 0



An analysis of medical image storage systems exposed to the public web reveals that almost 600 servers in 52 countries are completely unprotected against unauthorized access.

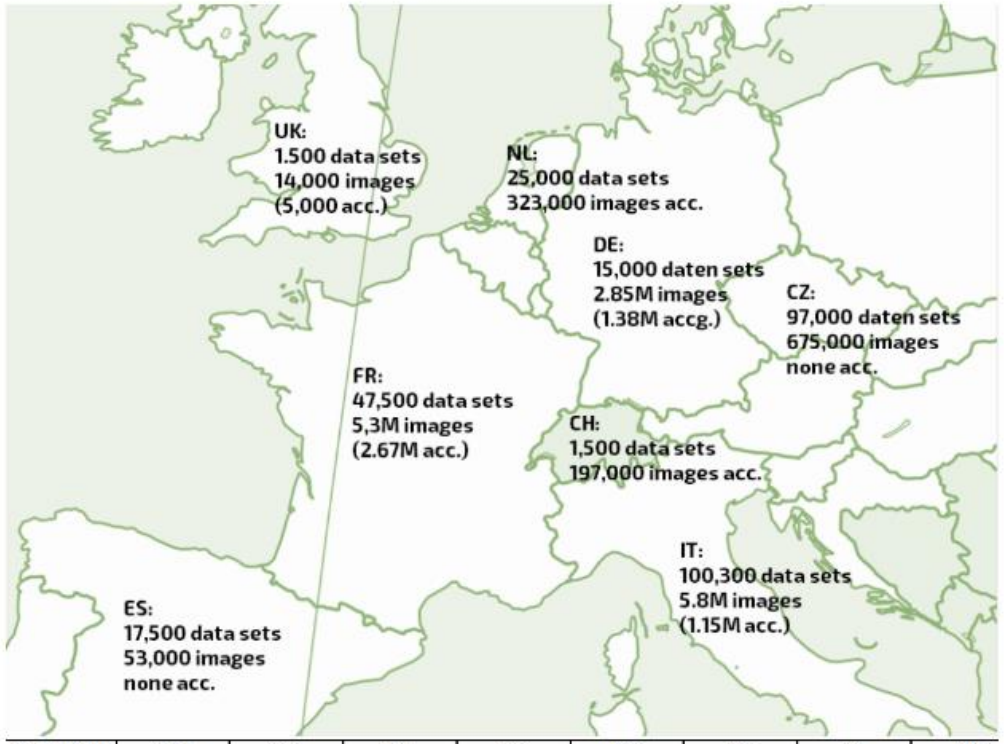
Audited systems were unpatched against thousands of vulnerabilities, more than 500 of them having the highest severity score.

Huge, worrying numbers

Greenbone Networks, a German-based vulnerability analysis and management company, looked at about 2,300 Picture Archiving and Communication System (PACS) systems connected to the public internet and found significant issues that expose confidential information.

https://www.bleepingcomputer.com/news/security/400-million-medical-radiological-images-exposed-on-the-internet/

In Europe, Italy has the highest number of affected systems, 10, and is also the country with the largest number of leaked medical information.



Country	CH	CZ	DE	ES	FR	IT	NL	UK
Systems	2	2	6	1	7	10	4	5

Digitaliserings skyggeside

45,1 % betalte .....

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,164)

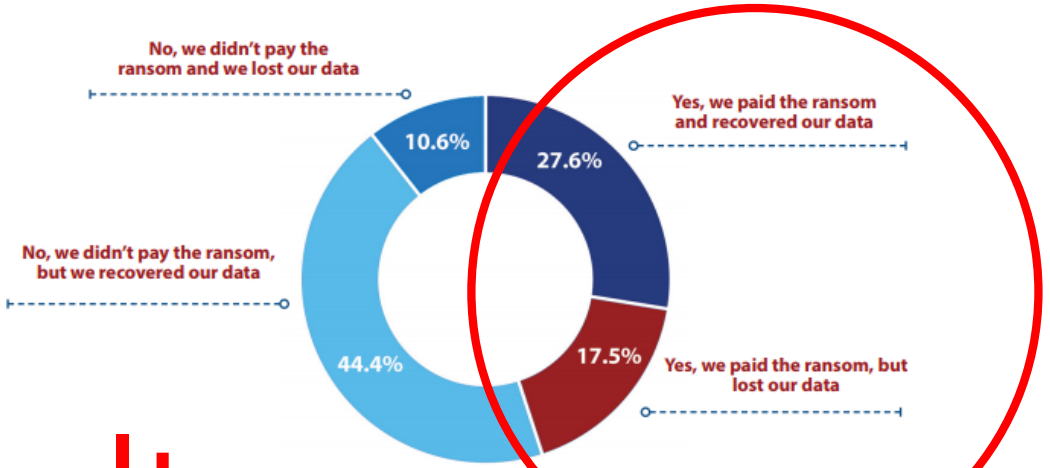


Figure 12: How victims responded to ransomware.

Despite diminishing press coverage on WannaCry, NotPetya, and Bad Rabbit, ransomware is still alive and well. Once again, we asked our research participants whether their employers were victimized by ransomware last year and, if so, whether they paid the associated ransoms. And, if they did pay the ransom, whether they got their data back.

Figure 12 and Table 1 depict the key results. Unfortunately, most of it is bad news.

To summarize:

- The percentage of organizations victimized by ransomware ticked up this year, from 55.1% to 56.1%.
- The percentage of victimized organizations that paid associated ransoms rose considerably this year, from 38.7% to 45.0%.
- The percentage of victimized organizations that refused the ransoms and subsequently lost their data increased this year, from 13.1% to 19.2%.

	2018	2019
Percentage of organizations victimized by ransomware	55.1%	56.1% ↑
Percentage of victimized organizations that paid ransom(s)	38.7%	45.0% ↑
Percentage of victimized organizations that refused ransom(s) and lost their data	13.1%	19.2% ↑
Percentage of victimized organizations that paid ransom(s) but lost their data	50.6%	38.8% ↓

https://www.computerworld.dk/art/247842/it-kriminalitet-er-nu-verdens-13-stoerste-oekonomi-saa-mange-penge-tjener-hackerne

https://komputer.dk/it-og-samfund/skraemmende-cyberkriminalitet-naar-rekordhoejt-niveau

Digitaliseringens skyggesider

(iStock) (JohnnyGreig/(iStock))

By **Kim Zetter**
April 3

When Hillary Clinton stumbled and coughed through public appearances during her 2016 presidential run, she faced critics who said that she might not be well enough to perform the top job in the country. To quell rumors about her medical condition, her doctor revealed that a CT scan of her lungs showed that she just had pneumonia.

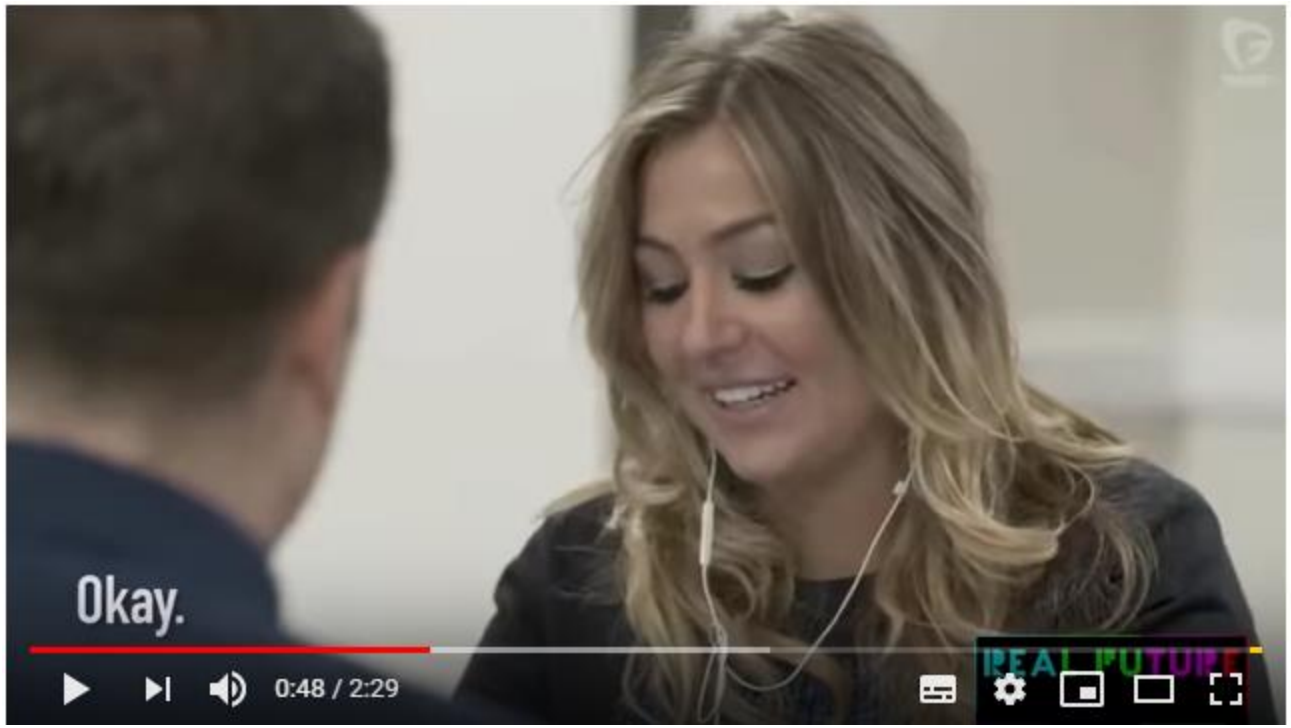
But what if the scan had shown faked cancerous nodules, placed there by malware exploiting vulnerabilities in widely used CT and MRI scanning equipment? Researchers in Israel say they have developed such malware to draw attention to serious security weaknesses in critical medical imaging equipment used for diagnosing conditions and the networks that transmit those images — vulnerabilities that could have potentially life-altering consequences if unaddressed.

The malware they created would let attackers automatically add realistic, malignant-seeming growths to CT or MRI scans before radiologists and doctors examine them. Or it could remove real cancerous nodules and lesions without detection, leading to misdiagnosis and possibly a failure to treat patients who need critical and timely care.

https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?utm_term=.4c47b32727f5

Digitaliseringens skyggesider - Vishing

Hackere kan bruge overtalelses evner og simple midler til at nå langt, bare fordi vi gerne vil hjælpe hinanden.



https://www.youtube.com/watch?v=lc7scxvKQOo

Digitaliseringens skyggesider – Social Engineering

Nøgletal, der viser, hvorfor it-sikkerhed skal fokusere på mennesker frem for infrastruktur

- Over 90% af de cyberangreb, som lykkes i øjeblikket, skyldes menneskelige faktorer. Det kan være nogen, der klikker på et skadeligt link i en e-mail eller giver sine brugeroplysninger til en forkert person.
- I tredjekvartal 2018 steg antallet af forsøg på at stjæle brugeroplysninger via phishing med 400% sammenlignet med samme periode i 2017.
- Antallet af forsøg på bedrageri via e-mail mod virksomheder, som er mål for cyberkriminalitet, steg med 80% i samme periode.
- Generelt steg personligt rettede angreb, såkaldt social engineering, med 233%.

https://it-kanalen.dk/10-noegletal-der-viser-hvorfor-it-sikkerhed-skal-fokusere-paa-mennesker-frem-for-infrastruktur/

Spørgsmål ☺

SUNDHEDSDATA-
STYRELSEN

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.