Region Hovedstaden
Center for IT og Medicoteknologi

Årsrapport 2023/2024

Årsrapport vedr. informationssikkerhed og databeskyttelse i Region Hovedstaden

Indholdsfortegnelse

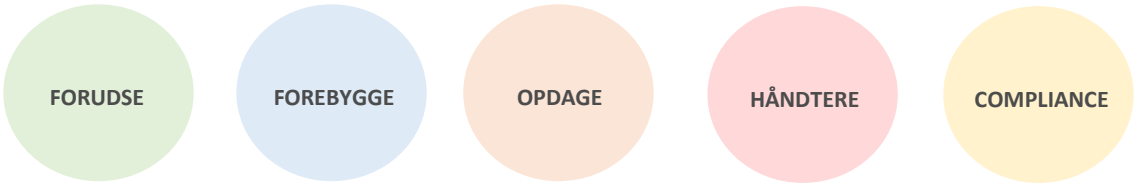
Version:	2023/2024
Udformet af:	Sektion for Informationssikkerhed
Senest opdateret:	10. januar, 2024

Indledning

Digitale løsninger spiller en stadig større rolle i sundhedssektoren, der som samfundskritisk sektor er særligt sårbar, hvis cyberangreb rammer. Samtidig har regionen ansvar for mange følsomme oplysninger og sundhedsdata, som patienter og borgere fortsat skal have tillid til, at regionen passer godt på og behandler i overensstemmelse med databeskyttelseslovgivningen og GDPR.

Området for informationssikkerhed og databeskyttelse dækker i Region Hovedstaden over både de organisatoriske, tekniske og databeskyttelsesretlige perspektiver. Det handler om den samlede beskyttelse af data og sker indenfor de lovivningsmæssige rammer, samt indenfor rammerne af fællesregionale såvel som nationale strategier og aftaler, herunder sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025.

Regionens Center for IT og Medicoteknologi er ansvarlig for at styre, tilrettelægge og drive udviklingen af området for informationssikkerhed og databeskyttelse på tværs af regionens organisationer. Arbejdet følger fem overordnede indsatsområder, som tager udgangspunkt i de nyeste internationale standarder inden for informationssikkerhed (ISO/IEC 27002):



Forudse potentielle angreb og hændelser gennem overblik over aktiver og trusselstyper, sårbarheder og risici.	Forebygge angreb og hændelser gennem risikostyring, governance og opbygning af kompetencer.	Opdage angreb og hændelser gennem opbygning af kapacitet til overvågning og analyse.	Håndtere angreb og hændelser gennem kapaciteter til hændelseshåndtering.	Udvikling af kapaciteter til efterlevelse af databeskyttelseslovgivningen og GDPR.

Kapitel 1: Resultater 2023

I dette kapitel ser vi tilbage på året der gik. Indledningsvist fremhæves relevante nedslagspunkter og aktiviteter indenfor de fem overordnede indsatsområder, hvorefter der gives et indblik i det nationale og fællesregionale samarbejde om informationssikkerhed og databeskyttelse. Afslutningsvist følger en kort orientering om årets tilsynsaktiviteter.

Indsatsområder

I 2023 blev der gennemført en ny CIS20-analyse af regionens modenhedsniveau på sikkerhedsområdet. CIS20 er et internationalt rammeværk for cyber- og informationssikkerhed, der opstiller en række konkrete sikkerhedstiltag, som organisationer kan implementere for at højne deres sikkerhed. Ved den første måling (2021) scorede Region Hovedstaden 2,23 og i den seneste måling (2023) er scoren løftet til 3,07. Regionerne har fastsat 3,5 som en fælles målsætning for arbejdet CIS20 rammeværket.

I 2023 er der i arbejdet med opdatering og vedligehold af regionens politikker og retningslinjer. Samtidig er regionens geoblokering og øvrige tekniske værn (eks. antivirus) løbende opdateret. Herudover er der på baggrund af anbefalinger fra Center for Cybersikkerhed implementeret teknisk blokering af først TikTok (Q1) og siden Snapchat (Q4).

I 2023 har Region Hovedstaden etableret en lokal overvågningsfunktion (SOC), som er opkoblet til den centrale analysefunktion (SAC) i Sundhedsdatastyrelsens DCIS SUND. Formålet er at øge kapaciteten til at opdage potentielle sikkerhedshændelser og minimere risikoen for, at aktører i sundhedssektoren bliver alvorligt ramt af cyberangreb og anden IT-kriminalitet.

Region Hovedstaden arbejder kontinuerligt med at styrke regionens IT-beredskab. Målet er at sikre, at regionen er bedst muligt rustet til at håndtere alvorlige cyberangreb. I 2023 har Region Hovedstaden haft et særligt fokus på beredskabsøvelser, hvor hospitalerne og regionens sundhedsberedskab er involveret.

I 2023 har regionen haft fokus på at håndtere en række eksterne tilsyn vedrørende det databeskyttelsesretlige område. Herunder blandt andet vedrørende regionens brug af public cloud baserede tredjelandsoverførsler. Herudover er der udarbejdet en ny retningslinje, som beskriver de overordnede principper for regionens tilgang til anonymisering af personoplysninger.

Nationalt og fællesregionalt samarbejde

I regi af Regionernes Sundheds-IT (RSI) og den tværregionale styregruppe for informationssikkerhed (TSI) samarbejder regionerne om at styrke regionernes sikkerhedsindsats og varetage regionernes interesser.

I 2023 har TSI bl.a. haft fokus på regionernes samarbejde om øget modenhed ift. CIS20-rammeværket, den danske implementering af EU's nye cybersikkerhedsdirektiv NIS2, samt opdatering af den fællesregionale persondatapolitik og regionernes politiske linje for informationssikkerhed. Herudover afholdt TSI i november 2023 en fælles temadag med fokus på beredskab, hvor regionerne udvekslede erfaringer om håndteringen af større sikkerhedshændelser i lyset af det skærpede trusselsbillede for sundhedssektoren.

I 2023 blev der lanceret en ny strategi for cyber- og informationssikkerhed i sundhedssektoren 2023-2025. Strategien er blevet til i et samarbejde mellem DCIS SUND i Sundhedsdatastyrelsen og de centrale aktører i sundhedssektoren, herunder regioner, kommuner, praktiserende læger (PLO) m.fl. Strategien har fokus på de dele af sikkerhedsarbejdet, som aktørerne løser i fællesskab og bygger videre på det fundament, der er blevet skabt med den forudgående sektorstrategi. Initiativer omfatter bl.a. kortlægning af kritisk infrastruktur, cyber- og informationssikkerhed på de sundhedsfaglige uddannelser, cybersikkerhed for de mindre aktører i sundhedssektoren, løsningskatalog for sikkerheden i borgernært udstyr, fælles beredskabsøvelser og øget udbredelse af overvågnings- og analysefunktioner (SOC/SAC). Regio-

nerne står bag et nyt initiativ i strategien vedr. bedre samarbejde om databeskyttelse ift. digitalisering i sundhedssektoren. Formålet med initiativet er at styrke dialogen om, hvordan komplekse, tværoffentlige samarbejdskonstruktioner rent databeskyttelsesretligt kan håndteres mere smidigt i praksis bl.a. i forhold til databehandleraftaler, tilsyn, kontrol og håndtering af brud på persondatasikkerheden.

Tilsyn

I Region Hovedstaden gennemføres både eksterne og interne tilsyn. Begge indgår som elementer i Region Hovedstadens samlede kontrolmiljø. Formålet med tilsynene er løbende at vurdere, om regionens udvikling og styring af området for informationssikkerhed og databeskyttelse er hensigtsmæssigt tilrettelagt. Med tilsynene testes informationssikkerhedsniveauet og det efterprøves, om regionens politikker og retningslinjer efterleves. I praksis bevirker tilsynene ofte, at sårbarheder bliver afdækket, så regionen kan agere rettidigt på dem.

Alle anbefalinger afgivet af såvel eksterne som interne tilsyn risikovurderes og omsættes til aktiviteter i det omfang det skønnes nødvendigt. Aktiviteter kan være afgrænsede opgaver, der styres via regionens centrale aktivitetslog eller tilbagevendende kontrolopgaver. Begge dele styres via regionens ISMS (Informations Security Management System) og har til formål at nedbringe de risici, der blotlægges i forbindelse med tilsynene. Både eksterne og interne tilsyn bidrager således effektivt til at målrette regionens aktiviteter i forhold til informationssikkerhed og databeskyttelse.

Eksterne tilsyn

De eksterne tilsyn udføres af en række forskellige aktører. Nogle tilsyn udføres som en fast tilbagevendende aktivitet, mens andre gennemføres ad hoc. De faste eksterne tilsyn gennemføres af henholdsvis Sundhedsdatastyrelsen og det eksterne revisionsselskab BDO. Sidstnævnte som led i den årlige finansielle revision.

Følgende eksterne tilsyn er blevet afsluttet i 2023:

Opstart	Eksterne tilsyn (afsluttet)
Oktober 2018	Datatilsynet: Fysisk tilsynsbesøg målrettet Sundhedsplatformen
Maj 2022	Rigsrevisionen: Opfølgning på Beretning om beskyttelse af adgangen til IT-systemer og sundhedsdata
August 2022	BDO: Finansiel revision 2022, IT-sporet
September 2022	Datatilsynet: Tilsyn med organisationens modenhed på databeskyttelsesområdet 2022

Rigsrevisionens tilsyn er helt afsluttet og giver ikke anledning til yderligere opfølgning. De øvrige tilsyn er afsluttet med enkelte anbefalinger men uden kritiske bemærkninger. Alle anbefalinger følges op med relevante aktivitetsopgaver.

Følgende eksterne tilsyn har været i proces i 2023 og er fortsat igangværende:

Opstart	Eksterne tilsyn (igangværende)
Juni 2022	Datatilsynet: Tilsyn med regionens brug af cloud i regi af patientbehandlingen
Juni 2023	Datatilsynet: Tilsyn med offentlige aktørers brug af AI-løsninger
August 2023	BDO: Finansiel revision 2023, IT-sporet
September 2023	Datatilsynet: Tilsyn vedr. videregivelse af personoplysninger
September 2023	Datatilsynet: Fysisk tilsyn med TV-overvågning på bostedet Sølager
September 2023	Datatilsynet: Fysisk tilsyn hos RBGB
November 2023	Sundhedsdatastyrelsen: NIS-tilsyn 2023

Interne tilsyn

De årlige interne tilsyn vedrørende regionens informationssikkerhed og databeskyttelse planlægges og gennemføres af Sektion for Informationssikkerhed og rapporteres til relevante ledelsesfora. De seks interne tilsyn i 2023 er blevet gennemført som planlagt.

Kapitel 2: Nøgletal 2023

Regionens cyberværn

Sundhedssektoren er udsat for en række forskellige *trusler og sårbarheder*. Siden 2018 har Center for Cybersikkerhed (CFCS) løbende offentliggjort sektorspecifikke trusselsvurderinger for sundhedssektoren. Den seneste er opdateret i februar 2023.

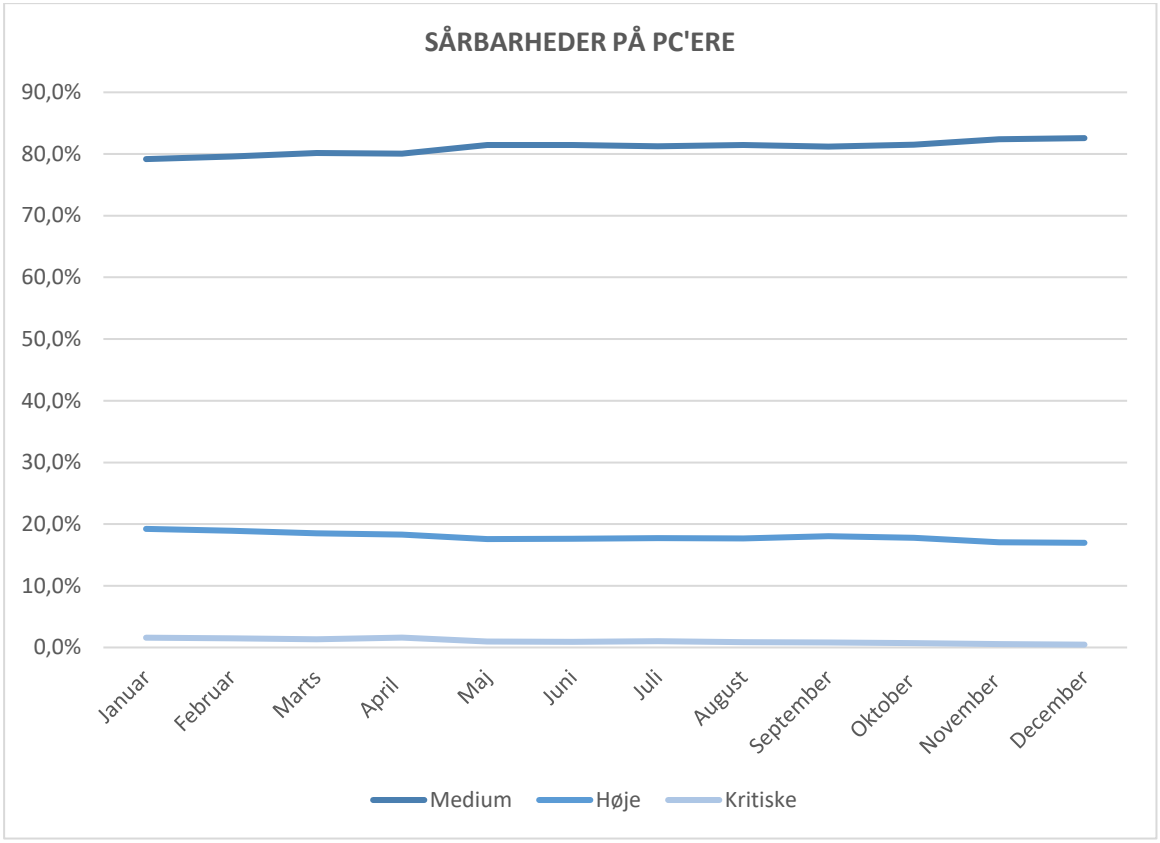
- RISIKO FOR CYBERSPIONAGE ER **MEGET HØJ**
- RISIKO FOR CYBERKRIMINALITET ER **MEGET HØJ**
- RISIKO FOR CYBERANGREB ER **MIDDEL**
- RISIKO FOR CYBERAKTIVISME ER **HØJ**
- RISIKO FOR CYBERTERRORISME ER **INGEN**

Infoboks 1: Trusselsniveauer jf. CFCS, februar 2023

I årsrapporten for 2022 rapporterede vi for sikkerhedshændelser på regionens PC'ere. Måden at arbejde med disse tal er under omlægning, da man arbejder for at få en mere detaljeret oversigt. I år rapporteres der derfor i stedet på antallet af sårbarheder på regionens PC'ere. Generelt skal alle sårbarheder så vidt muligt undgås, men i praksis er det særligt de kritiske sårbarheder, som udgør en sikkerhedsrisiko.

Fra januar til december 2023 er både de høje og kritiske sårbarheder faldende. De høje sårbarheder er faldet fra 19,2% til 17%, mens de kritiske sårbarheder er faldet fra 1,6% til 0,5%. Det betyder, at de høje sårbarheder per december 2023 udgør 17 %, mens de kritiske udgør 0,5 % af regionens samlede sårbarheder. I samme periode er den procentuelle andel af medium sårbarheder steget fra 79,6 % til 82,6 %

Figur 1 herunder viser mængden af sårbarheder på PC'ere.



Figur 1 - Sårbarheder fordelt på PC'ere i 2023.

Cyberhændelser

I Q1 2023 var Region Hovedstaden udsat for et såkaldt ”DDoS” angreb”, som medførte, at en række af regionens hjemmesider var ude af drift. Et DDoS angreb betyder, at der sendes enorme mængder trafik hen imod en eller flere hjemmesider. I langt de fleste tilfælde kan de almindelige tekniske sikkerhedsværn (firewalls og såkaldte DDoS-filtre) håndtere angrebene, og filtrerer automatisk trafikken væk. Men i nogle tilfælde lykkes det at få tilstrækkelig trafik igennem de tekniske sikkerhedsværn til at overbelaste de servere, som kører hjemmesiderne. Når det sker, går hjemmesiderne ned. Der er efterfølgende etableret relevante forebyggende foranstaltninger, herunder blandt andet i forhold til at justere regionens DDoS-filter.

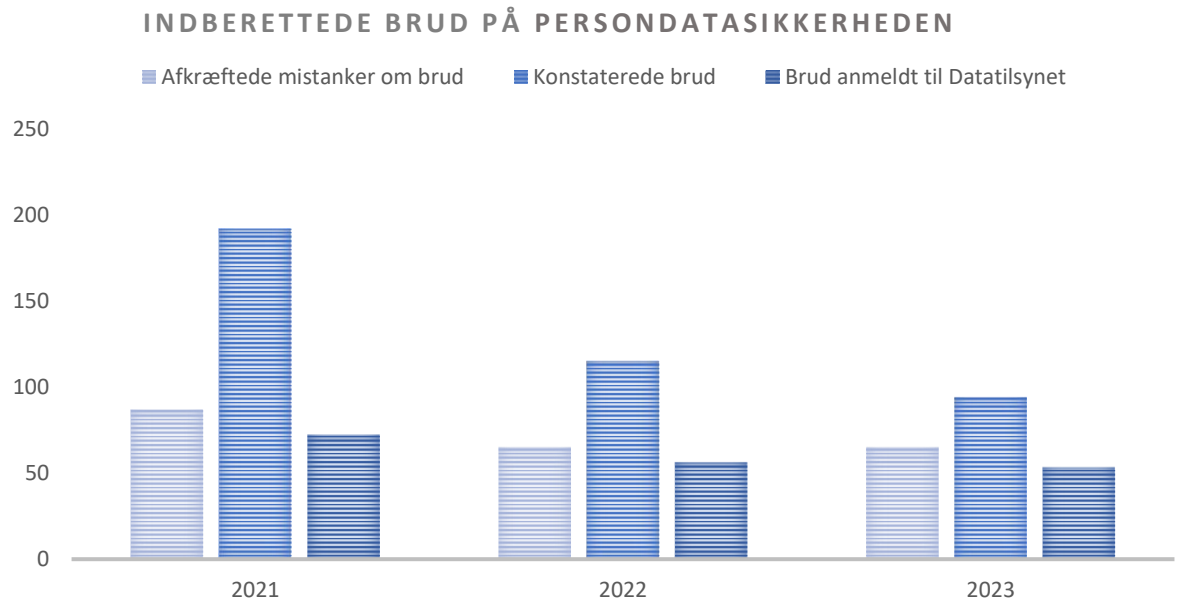
Brud på persondatasikkerheden

Siden Databeskyttelsesforordningen trådte i kraft d. 25. maj 2018, er der stillet særlige krav til, hvordan sikkerhedshændelser, som omfatter personoplysninger, skal håndteres og registreres. Denne type hændelser omtales som brud på persondatasikkerheden. Regionens procedure for håndtering af brud på persondatasikkerheden er forankret i Sektion for Informationssikkerhed, som i samarbejde med den lokale ledelse og GDPR-ambassadør håndterer alle brud på persondatasikkerheden i regionen. Regionens DPO-funktion orienteres løbende om verserende brud på persondatasikkerheden. Erfaringerne fra håndteringen af brud på persondatasikkerheden anvendes aktivt i regionens arbejde med sikkerhedskultur og i det løbende arbejde med udvikling af regionens informationssikkerhed og databeskyttelse.

Indberettede brud på persondatasikkerheden

Alle brud på persondatasikkerheden skal vurderes i forhold til de risici, der potentielt kan opstå for den registreredes rettigheder. Er der tale om et brud med lav risiko for borgerens rettigheder, bliver det alene registreret i regionens interne log over brud på persondatasikkerheden, mens øvrige brud på persondatasikkerheden, der kan medføre risiko for borgerens rettigheder, også anmeldes til Datatilsynet. I 2023 er der registreret i alt 159 henvendelser, som har ledt til mistanke om brud på persondatasikkerheden, hvoraf 94 blev konstateret som brud på persondatasikkerheden. Af de 94 brud vurderedes det, at der forelå en højere risiko for registreredes rettigheder i 53 tilfælde, hvor bruddet således også blev anmeldt til Datatilsynet.

Nedenstående figur viser udviklingen i antallet af indberettede brud på persondatasikkerheden fra 2021 til 2023.



Figur 2 - Oversigt over antallet af brud på persondatasikkerheden på årsbasis fra 2021 til 2023.

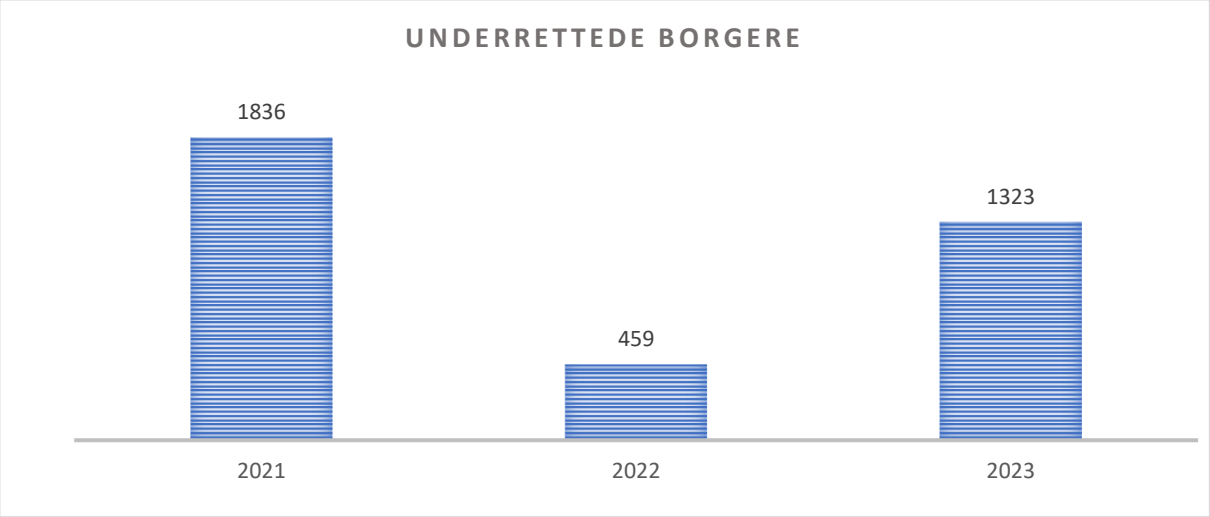
Mulige forklaringer på et fald i udviklingen i antallet af brud siden 2021 kan være regionens awareness-kampagner vedrørende brud på persondatasikkerheden, som har haft en præventiv effekt og ledt til en større bevågenhed blandt medarbejderne. Faldet skal også ses i lyset af, at regionen i forbindelse med håndteringen af covid-19 oplevede et større antal brud på persondatasikkerheden relateret til uberettigede opslag på covid-prøvesvar. Denne type hændelse er aftaget i takt med udfasning af testindsatsen.

Ca. 90% af alle brud på persondatasikkerheden skyldes menneskelige årsager. Det kan være uberettigede opslag i IT-systemer eller afsendelse af personoplysninger til forkert modtager.

Underrettede borgere

I særlige tilfælde underretter regionen borgere om, at der er sket et brud på persondatasikkerheden. Det sker i sager, hvor det vurderes at være en væsentlig risiko for borgerens rettigheder. I 2023 kan det høje antal underrettede borgere bl.a. forklares ved en større sag om en medarbejder der i en periode fra 2017 til 2022 har foretaget mere end 1200 uberettigede opslag i SP. De personer, hvor det har været muligt at underrette, er blevet underrettet i marts måned 2023.

Nedenstående figur viser udviklingen i antallet af underrettede borgere fra 2021 til 2023.



Figur 3 - Antallet af underrettede borgere på årsbasis fra 2021 til 2023.

Kapitel 3: Indsatsområder 2024

Indsatsområder

I dette kapitel ser vi på regionens indsatsområder på området for informationssikkerhed og databeskyttelse i det kommende år.

I 2024 vil der være fokus på at formulere en samlet strategi for udvikling af regionens cyber- og Informationssikkerhed. Strategien skal sætte retningen for udvikling af regionens CIS20-score og samle trådene fra ny lovgivning og initiativer på området, herunder blandt andet NIS2-direktivet samt sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025.

I forhold til politikker og retningslinjer vil regionen i 2024 have et særligt fokus på de IT-specifikke fagområder, eksempelvis backup og restore.

På sikkerhedskulturområdet vil fokus i 2024 være på implementering af et nyt e-læringskoncept (iSikkerhedstræning), som skal sikre en årlig og tilbagevende sikkerhedstræning af regionens medarbejdere og ledere.

I 2024 vil der også være fokus på at øge segmenteringen af regionens netværk for derved i endnu højere grad at kunne understøtte den digitale udvikling på hospitalerne på en sikker og målrettet måde.

I 2024 vil fokus fortsat være på at nedbringe antallet af sårbarheder. Det vil blandt andet ske ved fortsat optimere overblikket over sårbarheder for derved at kunne målrette risikominimeringsindsatser.

Videreudviklingen af den lokale overvågningsfunktion (SOC) vil også være et indsatsområde i 2024. Et væsentligt element i optimering af området vil være automatisering af SOC-funktionen.

HÅNDTERE

I 2024 vil den fokuserede indsats i forhold til at styrke regionens IT-beredskab fortsætte. Som en del af regionernes samarbejde om beredskab skal Region Hovedstaden i 2024 være vært for en tværregional beredskabsdag.

I forhold til håndtering af brud på persondatasikkerheden vil regionen fortsætte den løbende opdatering af procedurer og vejledningsmaterialer, herunder også for at sikre opsamling af erfaring og læring fra de konkrete sager.

COMPLIANCE

Regionens fremadrettede fokus i forhold til arbejdet med compliance i forhold til GDPR vil blive fastlagt med den samlede strategi for cyber- og informationssikkerhed. Herudover vil der blive igangsat en samlet opdatering af regionens retningslinje for tredjelandsoverførsler og public cloud.