Region Hovedstaden
Center for IT og Medicoteknologi

REGION

Årsrapport 2021/2022

Årsrapport vedr. informationssikkerhed og databeskyttelse i Region Hovedstaden

Indholdsfortegnelse

Indledning **2**

Kapitel 1: Resultater 2021 ..... **3**

Indsatsområder 3

Nationalt og fællesregionalt samarbejde 5

Tilsyn 6

Kapitel 2: Nøgletal 2021 ..... **8**

Regionens cyberværn 8

Konsekvensanalyser / DPIA 9

Brud på persondatasikkerheden 9

Kapitel 3: Indsatsområder 2022 ..... **13**

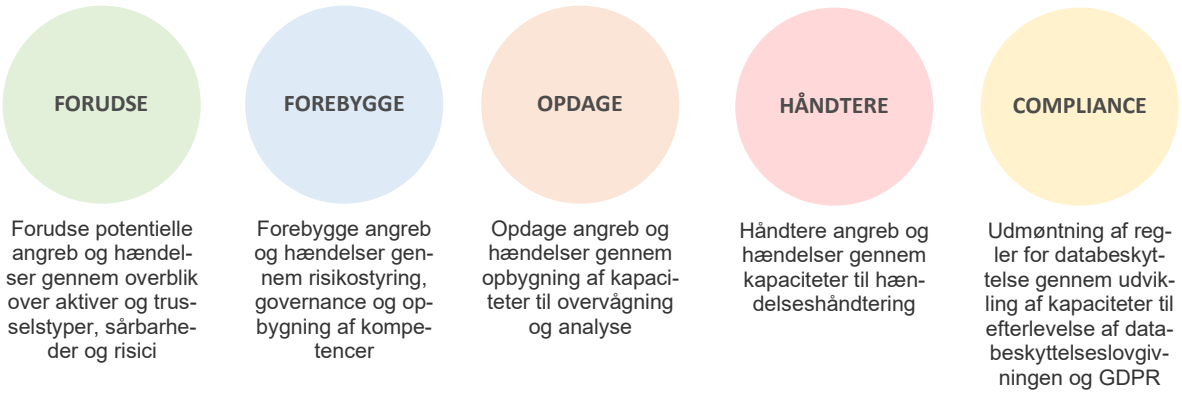
Version: 2021/2022
Udformet af: Sektion for Informationssikkerhed
Senest opdateret: 15. januar, 2022

Indledning

I Region Hovedstaden er adgang til data og stabil drift af regionens digitale infrastruktur en forudsætning for, at regionen kan give patienter og borgere en tryg og sikker behandling. Digitale løsninger spiller en stadig større rolle i sundhedssektoren, der som samfundskritisk sektor derfor 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 rammerne af databeskyttelseslovgivningen og GDPR samt indenfor rammerne af fællesregionale såvel som nationale strategier og aftaler, herunder strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022.

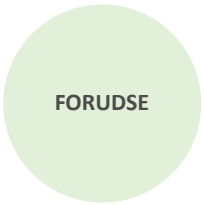
Sektion for Informationssikkerhed, der er forankret i Center for IT og Medicoteknologi, er ansvarlig for at styre, tilrettelægge og drive udviklingen af området for informationssikkerhed og databeskyttelse på tværs af regionens organisationer. Arbejdet følger fem overordnede indsatsområder, som tager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



Kapitel 1: Resultater 2021

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 2021 er regionens evne til at forudse trusselstyper blevet udviklet ved et generelt skærpet fokus på den operationelle sikkerhed. Blandt andet har de øgede ressourcer til regionens sektion for Operationel sikkerhed bidraget til løfte den samlede viden om aktuelle trusselstyper, herunder også via et styrket samarbejde med de øvrige regioner og med Sundhedsdatastyrelsens decentrale cyber- og informationssikkerhedsenhed i sundhedssektoren (DCIS-Sund). Samtidig er der skabt øget fokus på at sikre en struktureret opfølgning på kritiske sårbarheder i regionens systemer og udstyr.

I forhold til at forudse risici og sårbarheder i regionens systemer og software er rammerne styrket gennem udvikling af et samlet koncept til risikovurdering af konkrete systemer og software. I forbindelse med regionens forpligtigelser under NIS-direktivet er der desuden gennemført risikovurderinger af regionens mest kritiske systemer og tjenester.

I den forebyggende indsats udgør regionens medarbejdere et centralt og værdifuldt element. I 2021 har regionens indsatser i forhold til medarbejdere og sikkerhedskultur været koncentreret om udrulningen af det obligatoriske e-læringskursus om informationssikkerhed og databeskyttelse til alle medarbejdere i regionen. Herudover blev der afviklet en spotkampagne på regionens intranet med fokus på brud på persondatasikkerheden (juni) og under overskriften ”Hvem lukker du ind?” blev der afviklet en adfærdsorienteret kampagne med fokus på, hvad medarbejdere kan gøre for at undgå, at uvedkommende får adgang til regionens data både fysisk og digitalt (oktober).

I forhold til forebyggelse er regionen samtidig styrket gennem implementering af Privileged Acces Management (PAM) på brugere med kritiske adgange og rettigheder til regionens it-miljø. Derudover er der igangsat en omfattende opdatering af regionens retningslinjer for tredjelandsoverførsler gennemført i forlængelse af "Schrems II dommen" og EDBP's vejledning om supplerende foranstaltninger.

Kapaciteter til overvågning og analyse omfatter både det organisatoriske arbejde med tilsyn og revision og de mere tekniske foranstaltninger i form af værktøjer til overvågning af regionens IT-miljø.

I 2021 er regionens evne til at opdage angreb og hændelser væsentligt styrket gennem et generelt opbygningen af en operationel sikkerhedsfunktion, som løbende overvåger og følger op på kritiske alarmer vedrørende regionens it-miljø.

Herudover er regionens kontrol af opslag i den elektroniske patientjournal (Sundhedsplatormen) styrket gennem løbende revision og implementering af relevante supplerende kontrolfiltre. Det er eksempelvis sket ved implementering af et nyt "offentlighedsfilteret", der adresserer den særlige risiko for uberettigede opslag på borgere med en offenlig profil, som blev identificeret i forbindelse med evalueringen af et konkret brud på persondatasikkerheden i sommeren 2020.

I 2021 er regionens evne til at håndtere angreb og hændelser særligt styrket gennem en større opdatering af regionens IT-beredskabsplan. Opdateringen har taget udgangspunkt i konkrete beredskabsøvelser med bred deltagelse fra både IT-organisation, hospitaler, Sundhedsberedskabsorganisationen samt Sundhedsdatastyrelsens DCIS. Håndteringen af et alvorligt og omfattende cyberangreb har været det centrale i fokus for opdateringen. Arbejdet med udvikling og optimering af regionens IT-beredskabsplan i forhold til cyber vil fortsætte i 2022.

Regionens håndtering af hændelser vedr. brud på persondatasikkerheden er i 2021 styrket gennem opdatering af regionens procedure for brud på persondatasikkerheden samt fokus på identifikation og rapportering af brud på persondatasikkerheden i regi af aktiviteterne i regionens program sikkerhedskultur.

COMPLIANCE

I 2021 har regionens arbejde med compliance haft et markant fokus på håndteringen af EU-Domstolens "Schrems II dom" (juni 2020), som har skærpet kravene til overførsel af personoplysninger til lande udenfor EU/EØS. Anvendelsen af public cloud baseret software er et selvstændigt tema i dette arbejde. Derudover er der implementeret organisatoriske ændringer ift. den centrale rådgivning om databeskyttelseslovgivningen – herunder blandt andet for at skabe bedre rammer for understøttelse af forskningsområdet.

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. TSI har i 2021 bl.a. arbejdet med at opdatere den fællesregionale databehandleraftaleskabelon og fastlægge rammerne for et øget tværregionalt samarbejde om den mere operationelle del af sikkerhedsarbejdet, der vedrører cybersikkerhed og håndtering af truslen fra cyberangreb.

Regionerne blev i 2021 enige om at anvende det internationalt anerkendte rammeværktøj CIS20 som fælles ramme for styrkelse af sikkerheden i regionerne. Danske Regioners bestyrelse besluttede samtidig at fastsætte 3,5 på CIS20-modenhedsskalaen som et fælles ambitionsniveau for regionerne. PwC udarbejdede i 2020-2021 en CIS20 analyse for Region Hovedstaden, som viste, at regionens aktuelle modenhedsscore ligger på 2,23. På baggrund af anbefalingerne i CIS20-analysen arbejder regionen målrettet på at løfte modenheden bl.a. via en række konkrete tekniske sikkerhedstiltag.

STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED I SUNDHEDSSEKTOREN 2019-2022

Region Hovedstaden har i 2021 fortsat arbejdet med at implementere initiativerne i strategi for cyber- og informationssikkerhed i sundhedssektoren.

I december 2021 lancerede Regeringen en ny national strategi for cyber- og informationssikkerhed 2022-2024 med fokus på de statslige myndigheder. I forlængelse af den nationale strategi, arbejdes der på en ny strategi målrettet sundhedssektoren, som forventes at være klar, når den nuværende strategi udløber med udgangen af 2022. Regionen deltager aktivt i udarbejdelsen af den nye strategi, som bliver til i et samarbejde mellem Sundhedsdatastyrelsen, regionerne, kommunerne og andre centrale aktører i sundhedssektoren.

Som udløber af ØA21 og ØA22 indgår Region Hovedstaden i arbejdet med at etablere en fælles overvågnings- og analysefunktion i sundhedssektoren. Aftalerne indebærer, at der etableres en central analyse- og overvågningsenhed (SAC) forankret i Sundhedsdatastyrelsen og lokale overvågningsfunktioner (SOC) ved regioner, kommuner, praksissektoren og øvrige aktører. Formålet er at øge kapaciteten til at opdage potentielle sikkerhedshændelser og dermed minimere risikoen for, at aktører i sundhedssektoren bliver alvorligt ramt af cyberangreb og anden it-kriminalitet. Region Hovedstaden forventer at blive opkoblet til den centrale SAC-funktion ultimo 2022/primo 2023.

Tilsyn

Grundlæggende opereres der i Region Hovedstaden med hhv. eksterne og interne tilsyn. Begge indgår som elementer i Region Hovedstadens samlede kontrolmiljø. Formålet med tilsynene er løbende at vurdere om styringen af informationssikkerheden på hospitaler, virksomheder og centre er hensigtsmæssigt tilrettelagt. Med tilsynene testes informationssikkerhedsniveauet og det efterprøves om regionens egne politikker og retningslinjer efterleves. I praksis bevirker tilsynene ofte, at sårbarheder afdækkes og at 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 disciplin, mens andre gennemføres ad hoc. De faste eksterne tilsyn gennemføres af henholdsvis Sundhedsdatastyrelsen og det eksterne revisionsselskab BDO. Sidstnævnte som led i den Finansielle Revision.

Følgende eksterne tilsyn vedrørende informationssikkerhed og databeskyttelse har været i proces i 2021:

- Med opstart medio 2020: Rigsrevisionen igangsætter opfølgning på tilsyn med ”tre regioners IT-sikkerhed”. Afgørelsen fra Rigsrevisionen blev modtaget i januar 2021. Med afgørelsen bemærkede Rigsrevisionen, at der er sket en markant forbedring af beskyttelsen af sundhedsdata.

- Med opstart ultimo 2020: Datatilsynet gennemfører generelt tilsyn på forskningsområdet. Uddybende høringer i 2021. Der er netop kommet afgørelse på tilsynet. Med afgørelsen udtales kritik af manglende tilsyn med eksterne databehandlere i to konkrete forskningsprojekter.

- Med opstart september 2021: Sundhedsdatastyrelsen gennemfører tilsyn vedr. NIS-direktivet. Tilbagemelding afventes.

- Med opstart oktober 2021: BDO gennemfører den finansielle revision af regionen, heri indgår et IT-spor med fokus på cyber- og informationssikkerhed. Tilsynet er fortsat i proces og forventes afsluttet til april.

Interne tilsyn

De interne tilsyn planlægges og gennemføres af Sektion for Informationssikkerhed. Tilsynene rapporteres til relevante fora i forlængelse af regionens governance, herunder blandt andet den øverste administrative informationssikkerhedsledelse i Digital Styregruppe (DS).

I 2021 er der som en del af den interne tilsynsplan 2021 gennemført 10 konkrete tilsyn, der har medført i alt 7 opfølgningsaktiviteter som følges i regionens centrale aktivitetslog.

Kapitel 2: Nøgletal 2021

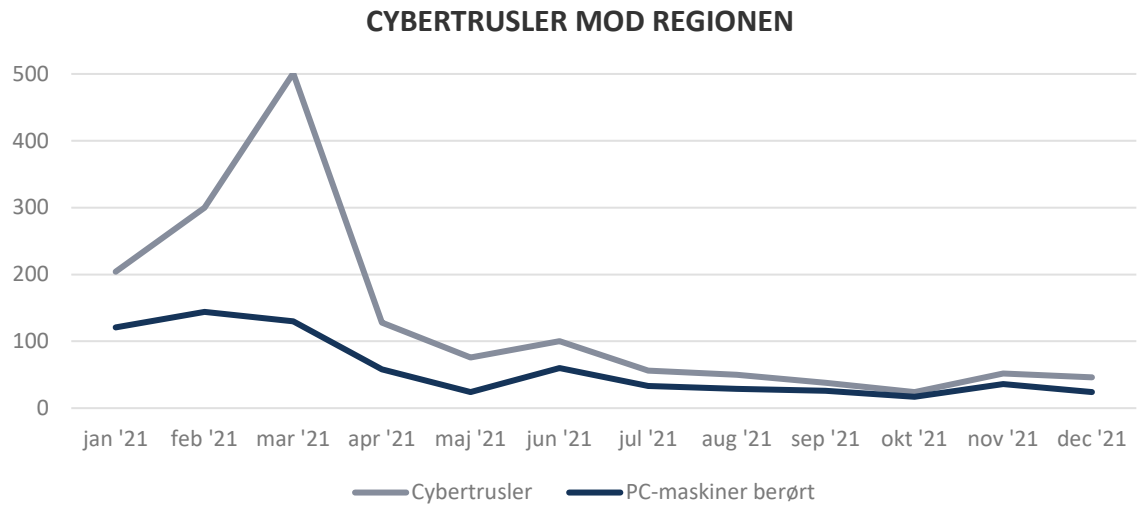
Regionens cyberværn

Cyber- og informationssikkerhed i sundhedssektoren er udsat for en række forskellige *trusler og sårbarheder*.

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

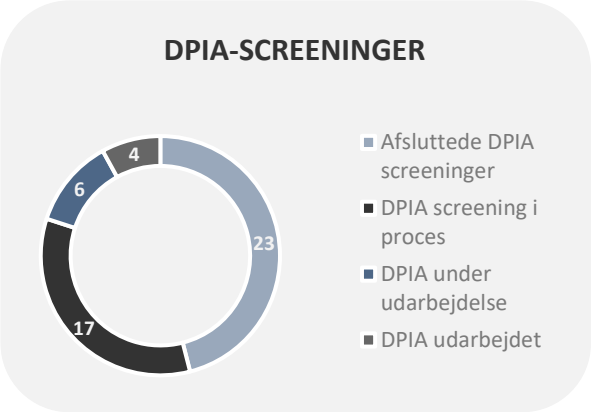
Infoboks 1 - Trusselsniveauer

Center for Cybersikkerhed offentliggjorde i juli 2018 den første og hidtil eneste sektorspecifikke trusselsvurdering for sundhedssektoren. Her vurderede de, at truslen for cyberspionage og -kriminalitet mod sundhedssektoren er meget stor, hvilket betyder at "der er en specifik trussel" og at "angrebsaktivitet er meget sandsynlig". Den seneste overordnede trusselsvurdering for Danmark, som er udgivet i juni 2021, angiver identiske trusselsniveauer og bemærker desuden, at hackere i løbet af år 2020 er begyndt på såkaldt dobbelt afpresning. For at øge presset på deres ofre, truer hackere nu dels med at fjerne tilgængeligheden til it-systemer, dels med at lække følsomme personoplysninger til offentligheden. Det ændrer ikke det overordnede trusselsniveau, men nuancerer trusselsbilledet.



Figur 1 – Unikke cybertrusler rettet mod regionens PC'ere. *Antallet af cybertrusler i marts 2021 var 7115, men af hensyn til overskueligheden er dette tal modificeret grafisk.

Konsekvensanalyser / DPIA



Figur 2 – DPIA-screeninger siden år 2018.

En konsekvensanalyse vedrørende databeskyttelse (*Data Protection Impact Assessment* eller DPIA) er en analyse, der har til formål at beskrive og vurdere nødvendigheden og proportionaliteten i at behandle personoplysninger. Med udgangspunkt i registreredes rettigheder skal analysen bidrage til beskyttelse af personoplysninger ved ansvarlig ibrugtagning af ny teknologi.

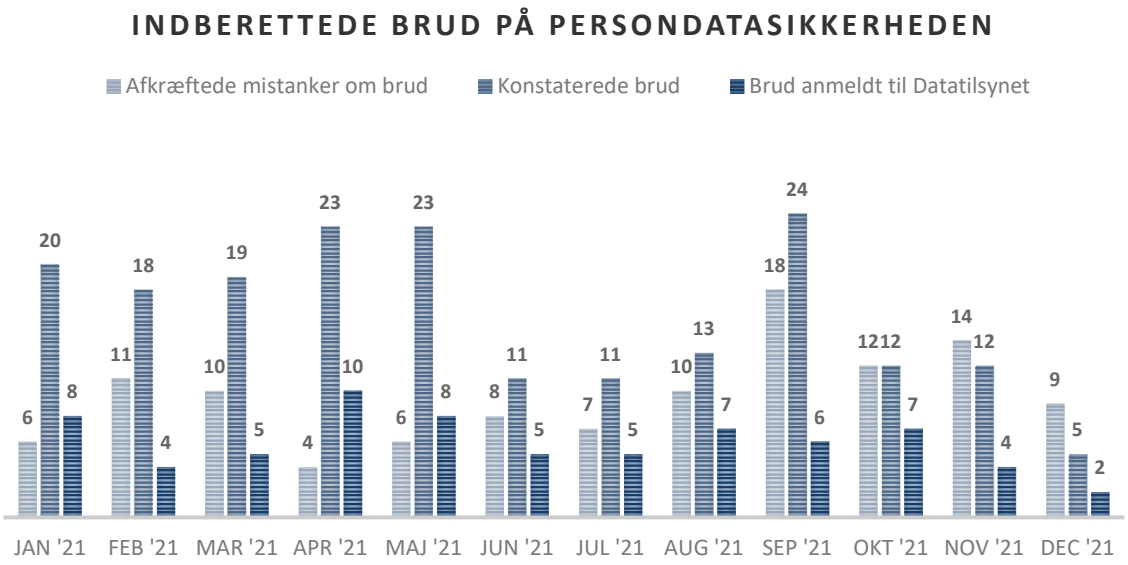
Region Hovedstaden har siden sommeren 2018 screenet alle projekter i CIMT's projektportefølje med henblik på at beslutte, om der skal udarbejdes konsekvensanalyser for de enkelte projekter. Screeningsarbejdet (en såkaldt præ-DPIA) og udarbejdelse af en egentlig konsekvensanalyse (DPIA-rapport) varetages af Sektion for Informationssikkerhed i tæt samarbejde med projektorganisationen. Regionens DPO-funktion orienteres om samtlige vurderinger og har mulighed for at kommentere udfaldet.

Brud på persondatasikkerheden

Siden Databeskyttelsesforordningen ikrafttrædelse d. 25. maj 2018, har det været et krav, at alle brud på persondatasikkerheden risikovurderes. 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.

Regionens procedure for håndtering af brud på persondatasikkerheden er forankret i Sektion for Informationssikkerhed, som i samarbejde med den lokale ledelse og GDPR-ambassadører håndterer alle brud i regionen. Regionens DPO-funktion orienteres løbende om alle brudsager.

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 med antagelig risiko for borgerens rettigheder også anmeldes til Datatilsynet. I 2021 er der registreret i alt 306 mistanker om brud på persondatasikkerheden, hvoraf 191 blev konstateret som brud. Af de 191 brud vurderede vi at der var risiko for krænkelse af de(n) registreredes rettigheder i 71 tilfælde, hvor bruddet således også blev anmeldt til Datatilsynet:



Figur 3 – Oversigt over antallet af brud på persondatasikkerheden

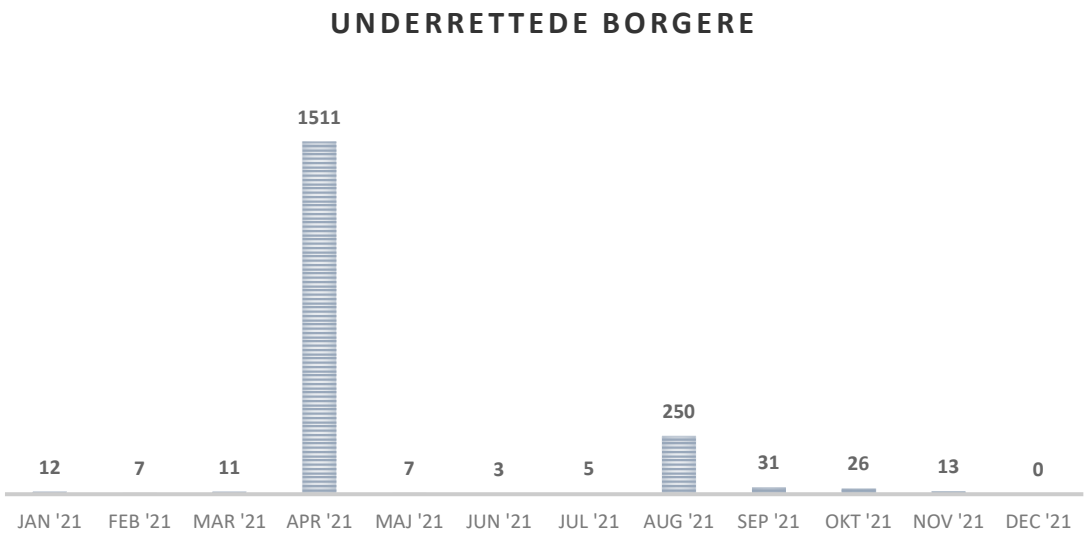
Det samlede antal af brud på persondatasikkerheden var i 2020 i alt 110, mens det i 2021 var 191. Det er en stigning på 73 procent i antallet af brud på ét år. Det forventes, at antallet af brud, der registreres og håndteres i regionen, vil være stigende i takt med øget opmærksomhed på de organisatoriske processer, der er sat op omkring denne hændelsestype.

Ca. 90% af alle brud på persondatasikkerheden skyldes menneskelige årsager. Det kan være uberettigede opslag i systemer, afsendelse af mail til forkert modtager eller manglende sløring af personoplysninger ved brug af screendumps i præsentationer.

Underrettede borgere

I særlige tilfælde underretter regionen borgere om, at der er sket et brud på persondatasikkerheden, som involverer deres helbredsoplysninger. Det sker i de sager, hvor der vurderes at være en væsentlig risiko for borgerens rettigheder. I år 2021 underrettede regionen i

alt 1876 borgere. Figur 6 viser en oversigt over underretning af borgere fordelt på måneder. Det er her værd at bemærke, at regionen i enkelte brudsager underretter mange registrerede om den samme hændelse. Det skete f.eks. i april 2021, hvor en USB-nøgle med 1499 borgeres prøvesvar for COVID-19 bortkom.



Figur 4 - Antallet af underrettede borgere i år 2021.

Brud rapporteret til det politiske niveau

Nedenfor følger en oversigt over og status på de sager om brud på persondatasikkerheden, som i 2021 er rapporteret til regionens politiske ledelse:

IT-medarbejders misbrug af adgang til Sundhedsplatformen

I sommeren 2021 blev regionen ramt af en alvorlig sag vedrørende misbrug af adgang til regionens systemer og uberettiget opslag. Sagen vedrørte en betroet IT-medarbejder, som har misbrugt sin adgang til Sundhedsplatformen til at foretage uberettigede opslag på i alt 244 borgere.

Der er igangsat en række opfølgningsaktiviteter, som skal minimere risikoen for lignede hændelser i fremtiden, ligesom den pågældende medarbejder er afskediget og politianmeldt. Københavns Politi forventer at føre straffesag mod medarbejderen for mindst ét og sandsynligvis flere lovbrud. Sagen er berammet til sommeren 2022.

FMK-sagerne

I 2021 blev regionen ramt af to sager vedrørende kodefejl i Sundhedsplatformen, som

førte til fejl i visningen af oplysninger i FMK. Fejlvisningerne vedrørte hhv. ”dobbeltvisning af ordinationer” og ”uoverensstemmelse i produktbeskrivelsen vedr. ordinationsstyrke”.

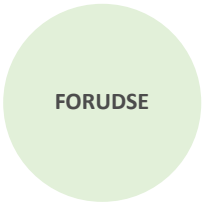
Begge fejl var afgrænset til *visningen* i FMK og har ikke haft konsekvenser for patientsikkerheden. Hændelsen vedr. ”dobbeltvisning af ordinationer” er grundigt rapporteret til Styrelsen for Patientsikkerhed, som ikke har fundet anledning til bemærkninger ift. regionens håndtering.

Sundhedsdatastyrelsen, som er dataansvarlig for FMK, anmeldte i sommeren 2021 hændelserne til Datatilsynet som brud på persondatasikkerheden. Datatilsynet har for nyligt truffet afgørelse i sagen. Med afgørelsen udtaler Datatilsynet henholdsvis påbud, advarsel og alvorlig kritik af regionen, hvilket til dato er den mest alvorlige kritik, regionen har modtaget.

Regionen Hovedstaden tager Datatilsynets afgørelse meget alvorligt og er i proces med at håndtere det konkrete indhold. Datatilsynets afgørelse indebærer dog også nogle meget principielle implikationer, som har givet anledning til bred bekymring hos regionerne. De principielle implikationer vedrører blandt andet risikoen for unødvendigt bureaukrati og dobbeltsagsbehandling i forholdet mellem Datatilsynets og Styrelsen for Patientsikkerheds ressortområder. I regi af Danske Regioner, herunder konkret Regionernes Sundheds IT (RSI), har regionerne derfor besluttet at sende et fælles brev til Datatilsynet, der udtrykker regionernes bekymringer i forhold til de principielle implikationer af afgørelsen.

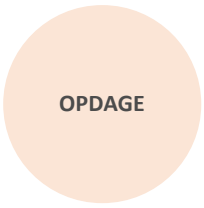
Kapitel 3: Indsatsområder 2022

I dette kapitel ser vi på regionens indsatsområder på området for informationssikkerhed og databeskyttelse i år 2022.



I 2022 vil der være fokus på risikovurdering af regionens kritiske systemer og udstyr – herunder både udarbejdelse af risikovurderinger samt procedurer for opfølgning og håndtering af identificerede risici. Derudover vil den øgede kapacitet i regionens Sektion for Operationel sikkerhed generelt bidrage til at forbedre regionens muligheder for at forudse nye trusselstyper, sårbarheder og risici.

I 2022 vil der være fokus på opdatering og vedligehold af regionens politikker og retningslinjer for informationssikkerhed og databeskyttelse. Herudover vil der blive arbejdet på at etablere ny en regional retningslinje, som er målrettet de problemstillinger, der knytter sig til anonymisering af personoplysninger. Desuden vil der i forhold til sikkerhedskultur og medarbejdere blive udviklet og implementeret et koncept for årlig træning og genopfriskning af regionens grunlæggende regler for informationssikkerhed og databeskyttelse.



I 2022 vil tilslutningen til den sundhedsspecifikke fælles SAC (Security Analytics Center), som er under etablering i regi af Sundhedsdatastyrelsens DCIS, være helt central i udviklingen af regionens evne til at opdage angreb og hændelser. Region Hovedstaden forventer at blive tilsluttet til SAC'en ultimo 2022/2023.

I 2022 vil regionen fastholde fokus på at styrke regionens IT-beredskab ift. håndteringen af alvorlige cyberangreb. Herudover vil regionen have fokus på forberedelse og kvalificering af de tekniske værktøjer, der vil blive anvendt i forbindelse med et alvorligt cyberangreb.

COMPLIANCE

I 2022 vil der være fokus på implementering af regionens model for tilsyn med eksterne databehandlere. Herudover vil der være fokus på arbejdet med udmøntning af Schrems II-dommen, idet alle regionens eksisterende tredjelandsoverførsler skal opdateres til det nye sæt af EU-standardkontrakter.