Region Hovedstaden
Center for IT og Medicoteknologi

Årsrapport 2022/2023

Årsrapport vedr. informationssikkerhed og databeskyttelse i Region Hovedstaden

Indholdsfortegnelse

Version: 2022/2023

Udformet af: Sektion for Informationssikkerhed

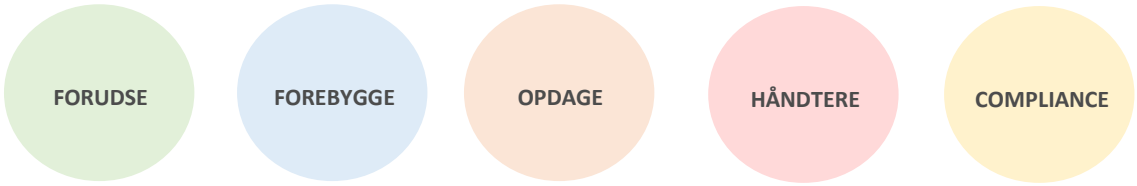
Senest opdateret: 07. februar 2023

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):



FORUDSE	FOREBYGGE	OPDAGE	HÅNDTERE	COMPLIANCE
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.	Udmøntning af regler for databeskyttelse gennem udvikling af kapaciteter til efterlevelse af databeskyttelseslovgivningen og GDPR.

Kapitel 1: Resultater 2022

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

FORUDSE

I 2022 er regionens evne til at forudse trusselstyper blevet udvidet på en række områder. I forbindelse med Ruslands invasion af Ukraine skulle regionen handle hurtigt for at mitigere potentielle sikkerhedsrisici og etablerede blandt andet et geoblokeringsfilter, så der fra en række konkrete lande ikke er adgang til regionen netværk. Herudover er det tekniske værn blevet hærdet, bl.a. i forhold til anti-virus på regionens servere og beskyttelse mod DDoS-angreb.

I forhold til at vurdere risici og sårbarheder i regionens IT-systemer og software har regionen fortsat udviklingen med den nuværende ramme for risikovurderinger af konkrete IT-systemer og software. I forbindelse med regionens forpligtigelser under NIS-direktivet er der i 2022 gennemført risikovurderinger af regionens mest kritiske IT-systemer.

FOREBYGGE

I den forebyggende indsats udgør regionens medarbejdere et centralt og værdifuldt element. I 2022 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. Ved udgangen af 2022 var gennemførelsesprocenten løftet til 75%. Regionens målsætning er, at 90% af alle medarbejdere har gennemført det obligatoriske e-læringskursus. I regi af regionens program for sikkerhedskultur er der herudover kørt en spotkampagne med temaet ”Send sikkert/Sikker Kommunikation” (andet kvartal) samt en kampagne med fokus på identitetstyveri (oktober).

Med henblik på at forebygge sikkerhedshændelser har regionen i 2022 også øget sikkerheden omkring brugere med udvidede rettigheder til regionens infrastruktur gennem implementeringen af "Privileged Access Management" (PAM) og udarbejdelsen af en retningslinje målrettet privilegerede brugere.

OPDAGE

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

I 2022 har regionens haft fokus på at forberede tilslutning til sundhedssektorens fælles overvågnings- og analysefunktion (SOC/SAC), som er under-etablering i regi af Sundhedsdatastyrelsens DCIS. Parallelt hermed er den løbende scanning og overvågning af regionens IT-miljø blevet styrket. Det gælder både generelt i forhold til sårbarhedsscanning af regionens netværk og konkret i forhold til bestemte typer af hændelser.

Som opfølgning på et konkret brud på persondatasikkerheden er der i 2022 herudover implementeret et nyt kontrolfilter i regionens automatiske logkontrol i Sundhedsplatformen. Med det nye kontrolfilter adresserer regionen den særlige risiko for uberettigede opslag, som relaterer sig til borgere med en offentlig profil.

HÅNDTERE

I 2022 er regionens evne til at håndtere angreb og hændelser styrket gennem et vedvarende fokus på de tekniske og organisatoriske forudsætninger for håndtering af konkrete sikkerhedshændelser. Dette ses i forhold til regionens IT- og cyberberedskab, hvor der både centralt i regionens IT-organisation og lokalt på regionens hospitaler, virksomheder og centre er gennemført beredskabsøvelser med fokus på cyberangreb. Det ses også i regionens Sektion for Operationel Sikkerhed, hvor der er etableret procedurer for central opfølgning på og bistand til håndteringen af sikkerhedshændelser med en vis kritikalitet. Derudover er der implementeret et værn mod DDoS-angreb for at styrke regionens tekniske håndtering af ondsindede aktører, der bevidst prøver at gøre regionens tjenester og ydelser utilgængelige ved overbelastning.

COMPLIANCE

I 2022 har regionens arbejde med compliance haft et 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 har været et selvstændigt tema i dette arbejde. Herudover er der implementeret organisatoriske ændringer ift. den centrale rådgivning om databeskyttelseslovgivningen med henblik på at optimere rammerne for understøttelse af henholdsvis regionens forskningsprojekter og regionens samlede portefølje IT-systemer og software.

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 2022 har TSI bl.a. haft fokus på at styrke samarbejdet omkring teknisk sikkerhed, regionernes fælles målsætning om at øge modenhedsniveauet i forhold til CIS20/CIS18 rammeværket, fælles indspil til økonomiforhandlinger samt igangsættelse af en række nye initiativer, herunder opdatering af regionernes politiske linje for informationssikkerhed.

Region Hovedstaden deltager aktivt i arbejdet med at udarbejde en ny strategi for cyber- og informationssikkerhed i sundhedssektoren i samarbejde med de centrale aktører i sektoren. I den forbindelse har regionerne i fællesskab foreslået et nyt initiativ, som har til formål at forenkle aktørernes arbejde med databeskyttelse i relation til de tværoffentlige digitaliseringsprojekter. Den nye strategi forventes at ligge klar i første halve år af 2023.

Som udløber af ØA21 og ØA22 indgår Region Hovedstaden i arbejdet med at etablere en fælles over-

STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED I SUNDHEDSSEKTOREN 2019-2022

Region Hovedstaden har i 2022 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.

vågnings- og analysefunktion i sundhedssektoren (SOC/SAC). 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 i starten af 2023.

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 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 årlige finansielle revision.

Følgende eksterne tilsyn vedrørende informationssikkerhed og databeskyttelse har været i proces i 2022:

Opstart	Eksterne tilsyn
Oktober 2018	Datatilsynet: Fysisk tilsynsbesøg målrettet Sundhedsplatformen
Oktober 2020	Datatilsynet: Skriftligt tilsyn i henhold til Region Hovedstadens behandling af personoplysninger til forskningsbrug
Juni 2021	Datatilsynet: Procedure for udstedelse af adgangskort
Oktober 2021	BDO: Finansiel revision 2021, IT-sporet
November 2021	Datatilsynet: Skriftligt tilsyn vedrørende fysiske materialer med personoplysninger (Øjenafdelingen på Rigshospitalet). Aflyst.

Maj 2022	Rigsrevisionen: Opfølgning på beretning om beskyttelse af adgangen til IT-systemer og sundhedsdata
Juni 2022	Datatilsynet: Tilsyn med regionens brug af cloud i regi af patientbehandlingen.
August 2022	BDO: Finansiel revision 2022, IT-sporet
September 2022	Datatilsynet: Tilsyn med organisationens modenhed på databeskyttelsesområdet 2022

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).

De interne tilsyn i 2022 blev aflyst for at håndtere forsinkelser omkring IT-sporet i den finansielle revision for 2021. Tilsynsemner fra 2022 vil i relevant omfang blive indarbejdet med de interne tilsyn for 2023.

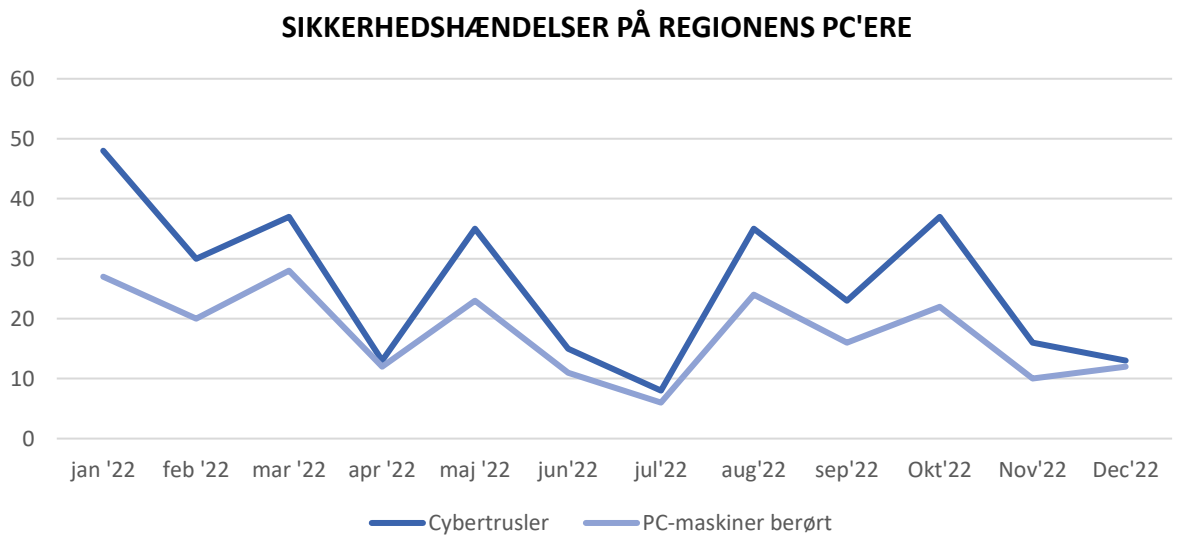
Kapitel 2: Nøgletal 2022

Regionens cyberværn

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

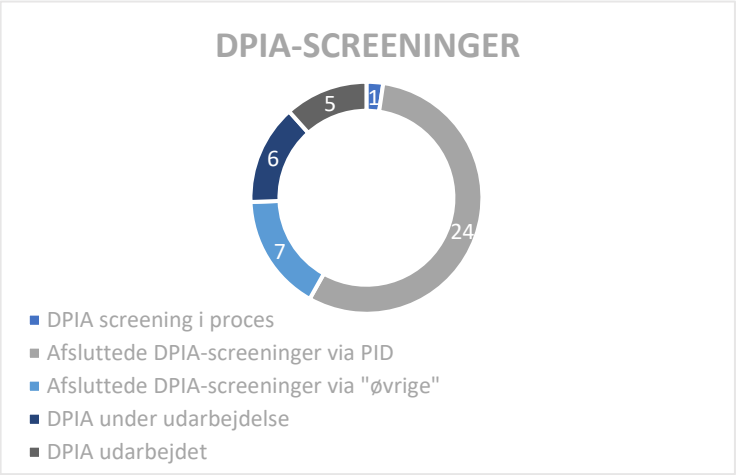
Infoboks 1: Trusselsniveauer for sundhedssektoren.

Center for Cybersikkerhed (CFCS) offentliggjorde i juni 2022 en opdateret version af den sektorspecifikke trusselsvurdering for sundhedssektoren. I opdateringen hæves risikoen for cyberaktivisme i sundhedssektoren fra lav til middel. Trusselsniveauet for sundhedssektoren er hævet i forlængelse af CFCS's samlede trusselsvurdering for Danmark og som følge af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine.



Figur 1: Unikke cyber-trusler rettet mod regionens PC'ere.

DPIA



Figur 2: DPIA-screeninger siden år 2018.

En DPIA (Data Protection Impact Assessment) er en omfattende databeskyttelsesretlig analyse målrettet beskyttelsen af personoplysninger. Analysen har til formål at beskrive behandlingen af personoplysninger, vurdere behandlingens nødvendighed og proportionalitet samt bidrage til at håndtere de (eventuelle) risici, behandlingen medfører for de registrerede. Der skal udarbejdes en DPIA i de situationer, hvor ibrugtagningen af ny teknologi sandsynligvis indebærer en høj risiko for de registrerede. En DPIA kaldes også for en ”konsekvensanalyse”.

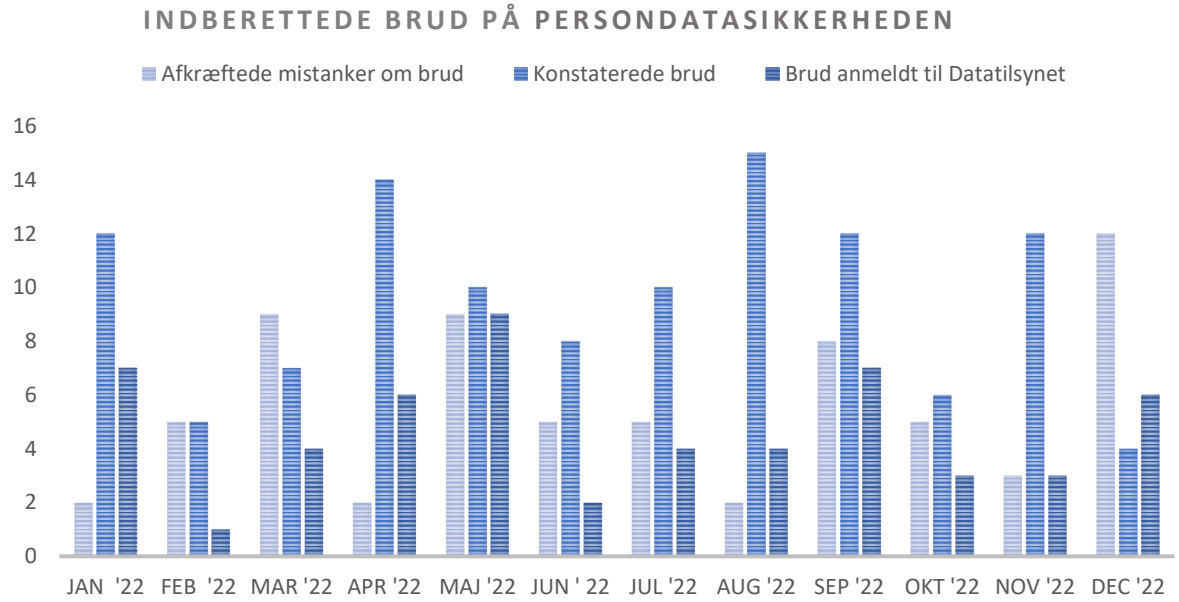
Region Hovedstaden har siden sommeren 2018 screenet alle projekter i regionens IT-projekt-portefølje med henblik på at vurdere, om der skal udarbejdes DPIA. Screening af øvrige behandlingsaktiviteter gennemføres på anmodning. Både screening samt udarbejdelse af DPIA'er varetages af Sektion for Informationssikkerhed. Regionens DPO-funktion orienteres om samtlige vurderinger og har mulighed for at kommentere udfaldet.

Brud på persondatasikkerheden

Siden Databeskyttelsesforordningen fik virkning d. 25. maj 2018, er der stillet særlige krav til, hvordan sikkerhedshændelser der 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.

Alle brud på persondatasikkerheden skal vurderes i forhold til de risici der potentielt kan opstå for den registrerede. Er der tale om et brud, hvor det er usandsynligt, at der er en risiko for borgeren, bliver det alene registreret i regionens interne log over brud på persondatasikkerheden, mens brud på persondatasikkerheden, der kan medføre en risiko for borgeren

også anmeldes til Datatilsynet. I 2022 er der registreret i alt 186 henvendelser der har ledt til mistanke om brud på persondatasikkerheden. Heraf er 115 blevet konstateret (bekræftet) som brud på persondatasikkerheden. Af de 115 brud på persondatasikkerheden er de 51 anmeldt til Datatilsynet.



Figur 3 - Oversigt over antallet af brud på persondatasikkerheden.

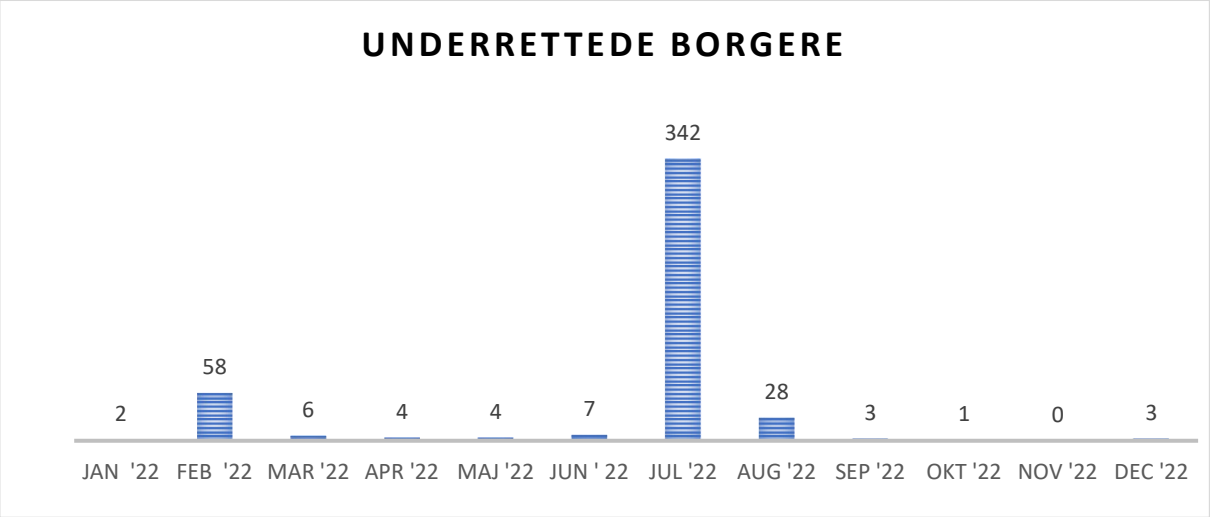
Det samlede antal af brud på persondatasikkerheden var i 2021 i alt 191, mens det i 2022 var 115. Det er første gang siden databeskyttelsesforordningens virke i 2018, at regionen oplever et fald i udviklingen af antal konstaterede brud på persondatasikkerheden. Mulige forklaringer herpå kan være regionens awareness-kampagner vedrørende brud på persondatasikkerheden har haft en præventiv effekt og ledt til en større bevågenhed blandt medarbejderne. Derudover registrerede regionen i forbindelse med håndteringen af covid-19 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 de tilfælde, hvor der vurderes at være en høj risiko for borgeren, bliver borgeren underrettet om, at der er sket et brud på persondatasikkerheden, som omfatter borgerens oplysninger. I

2022 underrettede regionen i alt 458 borgere. Til sammenligning underrettede regionen i 2021 i alt 1876 borgere. Figur 6 viser en oversigt over underretning af borgere fordelt på måneder.



Figur 4 - Antallet af underrettede borgere i år 2022.

Kapitel 3: Indsatsområder 2023

Indsatsområder

I dette kapitel ser vi på regionens indsatsområder på området for informationssikkerhed og databeskyttelse i år 2023.

I 2023 vil der være fokus på at videreudvikle regionens koncept for risikovurdering af IT-systemer og software, samt at gennemføre formaliserede risikovurderinger på en større andel af regionens IT-systemer. Der vil i 2023 blive gennemført en ny CIS20-analyse af regionens modenhedsniveau på sikkerhedsområdet, som vil følge op på udviklingen fra den sidst gennemførte måling i 2021.

I 2023 vil der være fokus på opdatering og vedligehold af regionens politikker og retningslinjer for informationssikkerhed og databeskyttelse. Bl.a. vil den fællesregionale persondatapolitik og regionens egne retningslinjer for kommunikation, brug af billeder og samtykke blive opdateret. Herudover arbejdes der på nye regionale retningslinjer vedrørende anonymisering og brug af overvågningskamera. Med hensyn til sikkerhedskultur og uddannelse af medarbejdere vil der blive lanceret et nyt årligt tilbagevendende e-læringskursus om informationssikkerhed og databeskyttelse til medarbejdere, som skal supplere det grundlæggende obligatoriske e-læringskursus alle nye medarbejdere i regionen skal tage, når de begynder at arbejde i regionen.

I 2023 vil tilslutningen til sundhedssektorens fælles overvågnings- og analysefunktion (SOC/SAC), forankret i, forankret i Sundhedsdatastyrelsens DCIS, være helt central i udviklingen af regionens evne til at opdage angreb og hændelser. I denne forbindelse opbygger regionen blandt andet et lokalt Security Operations Center (SOC) som vil styrke regionens evne til tidligt at

opdage angreb og sikkerhedshændelser og sikre fundamentet for et godt sammenspil med Sundhedsdatastyrelsens DCIS.

HÅNDTERE

I 2023 vil den fokuserede indsats i forhold til at styrke regionens IT-beredskab fortsætte. Målet er at sikre, at regionen er bedst muligt rustet til at håndtere alvorlige cyberangreb. I 2023 vil der bl.a. være fokus på de lokale nødberedskaber og samarbejdet mellem IT-beredskabet og sundhedsberedskabet. Herudover vil der blive arbejdet på at forbedre regionens backup-løsning, så regionen kan undgå datatab og hurtigere reetablere driften ved større nedbrud.

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

I 2023 vil der være fokus på opdatering af regionens model for tilsyn med eksterne databehandlere, herunder blandt andet med henblik på at justere spørgeramme og vejledende skabelon til brug for dokumentation. Desuden skal regionens retningslinje for tredjelandsoverførsler opdateres. I forhold til den databeskyttelsesretlige vurdering af regionens IT-systemer og software, vil der være særligt fokus på de IT-systemer og software, der forvaltes lokalt på regionens hospitaler, virksomheder og centre. I løbet af 2023 vil regionens rammer for udmøntning af NIS2-direktivet (Net- og Informationssikkerhedsdirektivet) også være et selvstændigt tema. Direktivet skal være udmøntet i efteråret 2024.