Region Hovedstaden
Center for It, Medico og Telefoni

Årsrapport 2019/2020

Årsrapport vedr. informationssikkerhed og databeskyttelse i Region Hovedstaden

Indholdsfortegnelse

Version: 2020
Udformet af: Sektion for Informationssikkerhed
Senest opdateret: 21. september, 2020

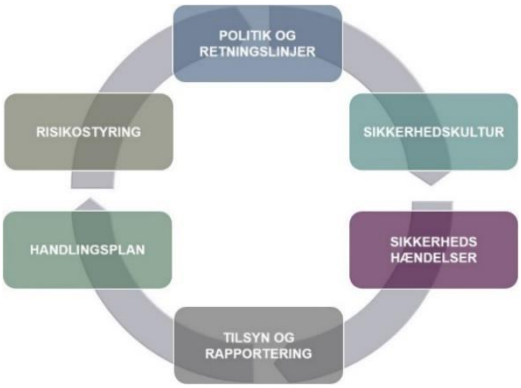
Indledning

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 lovgivningen.

Området for informationssikkerhed og databeskyttelse i regionen dækker over organisatoriske, tekniske og compliancemæssige perspektiver. Det handler om beskyttelse af data og sker indenfor rammerne af fællesregionale såvel som nationale strategier og aftaler, herunder strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022.

Arbejdet med udvikling af området er struktureret indenfor et overordnet rammeværk med seks fokusområder:

- Risikostyring
- Politik og retningslinjer
- Sikkerhedskultur
- Beredskab og håndtering af sikkerhedshændelser
- Tilsyn og rapportering
- Handlingsplan.



Til at styre, tilrettelægge og drive udviklingen af området for informationssikkerhed og databeskyttelse på tværs af regionen har regionen etableret en central Sektion for Informationssikkerhed, forankret i Center for It, Medico og Telefoni.

Til at rådgive og kvalificere udarbejdelsen af databehandleraftaler har Region Hovedstaden etableret et centralt Videnscenter for Dataanmeldelser og Databehandleraftaler (VDF). Region Hovedstaden har herudover en uafhængig DPO-funktion, som rådgiver om forpligtigelserne i forhold til databeskyttelseslovgivningen.

Kapitel 1: Resultater 19/20

Indsatsområder 19/20

Region Hovedstaden fik i 2017 udarbejdet en ekstern rapport af KMD til vurdering af it-sikkerheden i regionen. Rapporten dannede baggrund for etableringen af Sektion for Informationssikkerhed i 2018 og har sidenhen udgjort grundlaget for den overordnede udvikling af området og prioritering af nye indsatser.

Organisation
På baggrund af anbefalingerne i KMD-rapporten har regionen i de senere år arbejdet på at styrke de organisatoriske rammer og processer for arbejdet med informationssikkerhed og databeskyttelse i regionen. I 2019/2020 er der bl.a. udarbejdet nye retningslinjer målrettet medarbejdere, ledere med personaleansvar og systemejere. Der er desuden udarbejdet et nyt program for sikkerhedskultur, der skal løfte uddannelsesindsatsen og klæde medarbejderne bedre på til at agere sikkert i deres daglige arbejde.

Teknik
Regionen implementerede i 2019 et nyt system til automatisk logopfølgning i Sundhedsplatformen. Systemet sikrer en øget kontrol med uberettigede opslag i patientjournaler, og dermed en bedre beskyttelse af patienternes helbredsoplysninger.

Compliance
Regionen har fortsat stort fokus på at udmønte EU's databeskyttelsesforordning (GDPR) og løbende sikre, at regionens håndtering af persondata lever op til kravene i lovgivningen.

UDVALGTE AKTIVITETER OG PRODUKTER 19/20	Organisation	Teknik	Compliance
Automatisk logopfølgning på Sundhedsplatformen		•	•
Retningslinjer målrettet medarbejdere, ledere med personaleansvar og systemejere	•		•
Retningslinjer for anvendelse af public cloud			•
Retningslinjer for hosting af it-systemer udenfor EU/EØS			•
Modenhedsvurdering 2019	•		•
Risikostyringskoncept for Sundhedsplatformen	•		
Model for tilsyn med eksterne databehandlere			•
Proces for udarbejdelse af konsekvensanalyser (DPIA)			•
Styrket implementering af oplysningspligten			•
Program for sikkerhedskultur inkl. materialepakke, intranetunivers, rejsehold for ledergrupper og udvikling af e-læringskursus til medarbejdere	•		•
Koncept for ledelsesrapportering	•		
Opdatering af informationssikkerhedspolitik og styringsmodel	•		•
Opdatering af persondatapolitik	•		•

Nationalt og fællesregionalt samarbejde 19/20

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 2019/2020 haft fokus på at færdiggøre en række produkter, der bl.a. skal sikre, at regionerne har et fælles udgangspunkt i forbindelse med udarbejdelse af konsekvensanalyser, behandlingssikkerhed, regionernes anvendelse af cookies på hjemmesider og anvendelse af den fællesregionale databehandleraftaleskabelon.

Under TSI er der ligeledes nedsat erfaringsudvekslingsgrupper, der efter behov løbende er i dialog og vidensdeler om bl.a. uddannelsesindsatser, regionernes håndtering af brud på persondatasikkerheden, ISO27001-implementering og regionernes arbejde med automatiseret log og logopfølgning.

STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED I SUNDHEDSSEKTOREN 2019-2022

I 2019 påbegyndte Region Hovedstaden implementeringen af initiativerne fra den nye strategi for cyber- og informationssikkerhed i sundhedssektoren. Region Hovedstaden er repræsenteret i styregruppen for strategien og deltager aktivt i en række arbejdsgrupper med fokus på bl.a. at skabe fælles rammer for risikovurderinger, beredskab og sikkerhedsarkitektur.

I forbindelse med ØA2021 blev der indgået en aftale om, at det videre arbejde med etablering af overvågnings- og analysekapacitet for sundhedssektoren - med henblik på at styrke det fælles forsvar mod cyberangreb og andre digitale trusler – skal videreføres på nationalt niveau og indgå i den forestående opdatering af den nationale strategi for cyber- og informationssikkerhed.

Tilsyn 19/20

Til at føre kontrol med, at regionen lever op til gældende lovkrav, standarder og regionens egne politikker og retningslinjer, laves der løbende tilsyn på det sikkerhedsmæssige såvel som det databeskyttelsesretlige område. Regionens revisionsfirma foretager i forbindelse med it-sporet i den finansielle revision årligt eksternt tilsyn med regionens informationssikkerhed, og Sektion for Informationssikkerhed foretager årligt en række interne tilsyn. På det databeskyttelsesretlige område fører Region Hovedstadens uafhængige DPO-funktion løbende tilsyn med regionens udmøntning af databeskyttelseslovgivningen.

Foruden den løbende kontrol har regionen i 2019/2020 været underlagt eksterne tilsyn og revision fra tilsynsmyndigheder på udvalgte områder. Sundhedsdatastyrelsen har ført tilsyn med regionens arbejde med NIS-direktivet, og Rigsrevisionen har netop igangsat en it-revision som opfølgning på et tilsyn i 2017 vedr. beretning 4/2017 om ”3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata.” I nov. 2018 gennemførte Datatilsynet et fysisk tilsyn med fokus på Sundhedsplatformen. Regionen afventer fortsat den endelige rapport fra tilsynet.

Sektion for Informationssikkerhed følger systematisk op på alle revisions- og tilsynsanbefalinger og bruger dem aktivt i udviklingsarbejdet.

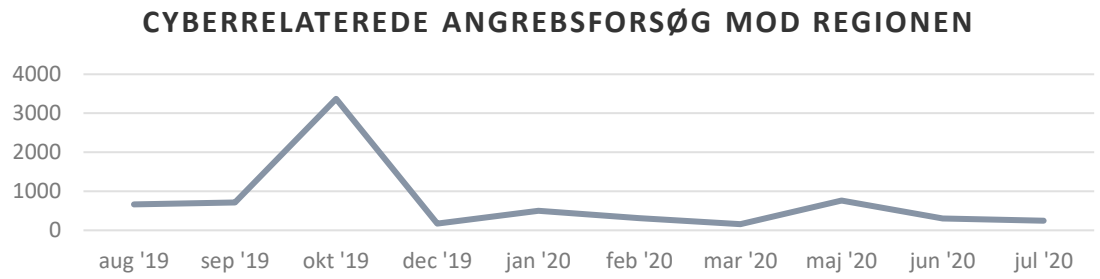
Kapitel 2: Nøgletal 19/20

Regionens cyberværn

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

Cyber- og informationssikkerhed i sundhedssektoren er udsat for en række forskellige *trusler og sårbarheder*. Center for Cybersikkerhed offentliggjorde i juli 2018 den første og hidtil eneste sektorspecifikke trusselsvurdering for sundhedssektoren. Her vurderede de, at truslen mod sundhedssektoren kan komme fra en række forskellige aktører og i mange forskellige former. Nogle trusler har potentiale til at påvirke regionens evne til at løfte kerneopgaver og indfri målsætninger, mens andre er uvæsentlige for regionens virke.

Et samlet overblik over cyberrelaterede angrebsforsøg mod regionen[1] viser, at antallet varierer betragteligt fra måned til måned. Langt de fleste cyberrelaterede angrebsforsøg håndteres af regionens tekniske sikkerhedsværn, og ingen cyberrelaterede angrebsforsøg har medført væsentlige sikkerhedsrisici.



Konsekvensanalyser / DPIA

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 beskyttelse af borgerens rettigheder skal analysen bidrage til beskyttelse af personoplysninger ved ansvarlig ibrugtagning af ny teknologi.

Region Hovedstaden har siden sommeren 2018 screenet alle projekter i regionens IT-projektportefølje samt særligt udvalgte kritiske projekter udenfor projektporteføljen, med henblik på at vurdere, om der skal udarbejdes konsekvensanalyser for de enkelte projekter. Dette arbejde har indtil videre ført til beslutning om at udarbejde fire konsekvensanalyser –

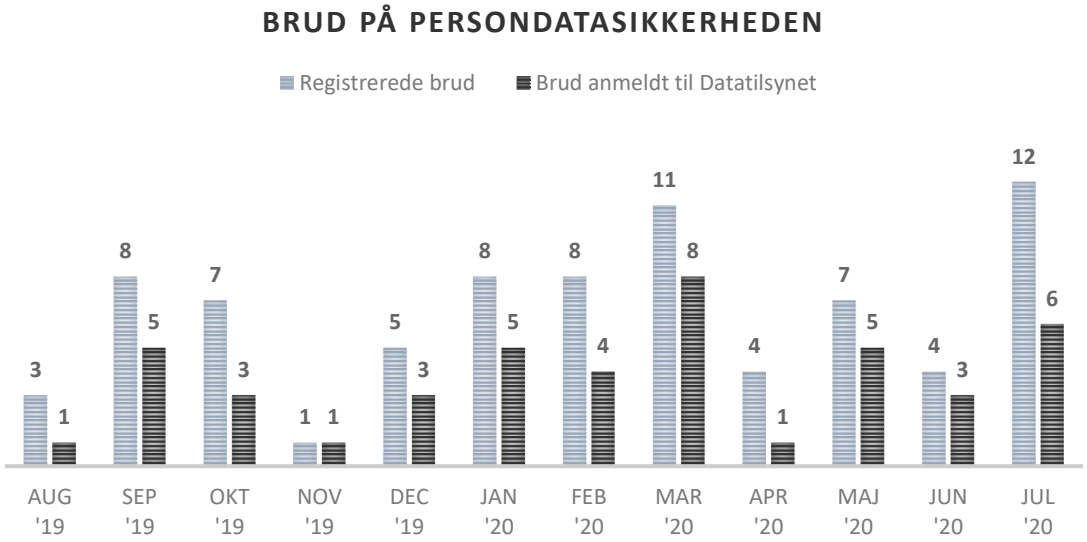
[1] Cyberrelaterede angrebsforsøg defineres her som hændelser, der forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester.

alle sammen relateret til Sundhedsplatformen, hvoraf to af de fire på nuværende tidspunkt er gennemført.

Brud på persondatasikkerheden

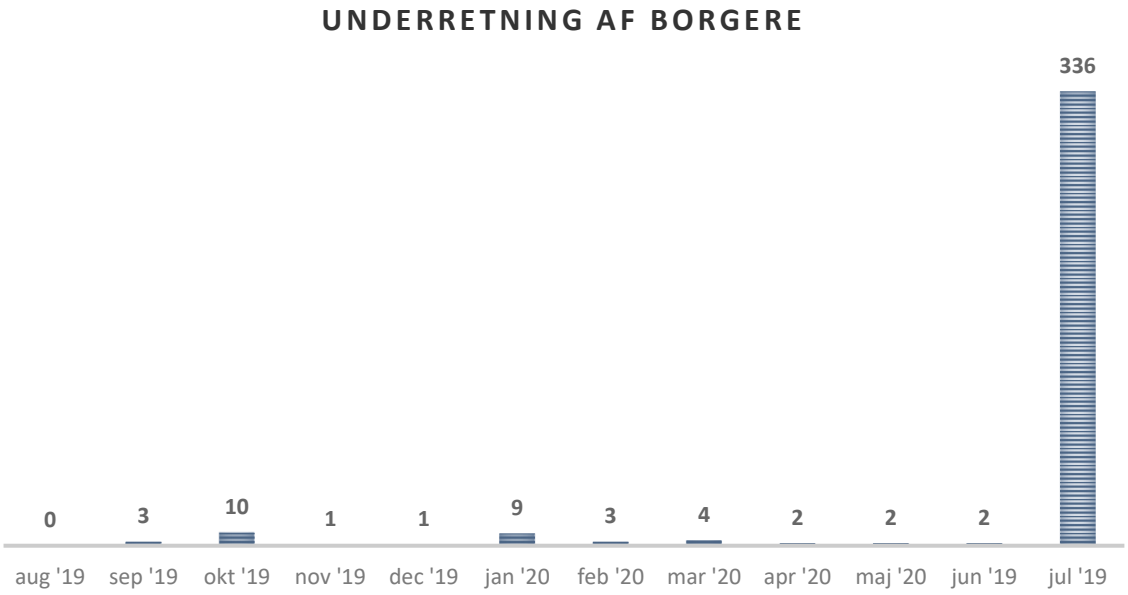
Siden Databeskyttelsesforordningen fik virkning d. 25. maj 2018, har det været et krav, at alle brud på persondatasikkerheden risikovurderes. Erfaringerne fra håndteringen af brud på persondatasikkerheden anvendes aktivt i regionens arbejde med sikkerhedskultur og i det løbende arbejde med udvikling 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 brudlog, mens øvrige brud med antagelig risiko for borgerens rettigheder også anmeldes til Datatilsynet. I perioden fra august 2019 til juli 2020 er der registreret i alt 78 brud, hvoraf 45 er anmeldt til Datatilsynet:



Antallet af brud på persondatasikkerheden i perioden fra august 2019 til juni 2020 er en stigning i antallet af brud på 44 pct. i forhold til den foregående periode, hvor der blev registreret 54 brud på persondatasikkerheden. Det forventes, at antallet af brud, der registreres og håndteres i regionen, fortsat vil være stigende i takt med øget opmærksomhed på de organisatoriske processer, der er sat op omkring denne hændelsestype.

Underretning af 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, som borgeren skal orienteres om. I perioden fra august 2019 til juli 2020 har regionen underrettet i alt 373 borgere.



Konkrete brud på persondatasikkerheden
I juli 2020 blev regionen ramt af det hidtil største og mest alvorlige tilfælde af uberettigede opslag, hvor en sygeplejerske over en årrække havde foretaget uberettigede opslag i 215 borgeres patientjournaler. Det systematiske misbrug er anmeldt til Københavns Politi, med hvem der fortsat pågår dialog. Sagen har givet anledning til at drøfte, hvordan vi kan lære af sagen og forbedre de indsatser, regionen allerede har på området. Konklusionerne fra dette arbejde forventes fremlagt for regionens politiske ledelse i oktober 2020.

Uberettigede opslag i Sundhedsplatformen udgør en fortsat stigende andel af de brud på persondatasikkerheden, som registreres og håndteres i regionen. Stigningen skyldes blandt andet, at regionen har implementeret en skærpet kontrol med opslag i Sundheds-platformen.

Andre eksempler på brud på persondatasikkerheden er:

- Tastefejl ved indtastning af cpr.nr. eller modtager
- Fejludlevering af indkaldelsesbreve
- Interne forsendelser med forkert modtager
- Offentliggørelse af screendumps med personoplysninger
- Tekniske fejl

Kapitel 3: Indsatsområder 20/21

Organisation
Region Hovedstaden har i de senere år haft stort fokus på at opbygge stærke organisatoriske rammer og processer til at kunne styre og drive arbejdet med informationssikkerhed og databeskyttelse på tværs af regionen. Disse er nu på plads. Derfor vil indsatsen i det kommende år i stigende grad centrere sig om den lokale implementering på hospitaler, virksomheder og centre og på dialogen med medarbejdere og ledere omkring den praktiske udmøntning af politikker og retningslinjer i det daglige arbejde.

Herudover vil der være fokus på at de organisatoriske områder, hvor det fortsat udestår at formalisere regionens rammer og tilgang, dette bl.a. i forhold til regionens arbejde med risikostyring.

Teknik
I 2020 er der sket en budgetmæssig tilpasning til aktiviteterne på cybersikkerhedsområdet i regionen, idet der er tilført midler til reinvestering i infrastruktur i den kommende årrække samt for 2020 tilført midler og årsværk til styrkelse af den operationelle sikkerhedsindsats. I forlængelse heraf er der etableret en ny selvstændig sektion for operationel sikkerhed i Center for It, Medico og Telefoni, som skal styrke regionens drifts- og beredskabshåndtering ift. cyberangreb og andre sikkerhedshændelser bl.a. igennem etableringen af overvågnings- og analysefunktioner (SOC/SAC) såvel lokalt som i regi af den nationale og sektorspecifikke strategi for cyber- og informationssikkerhed. Der blev i foråret 2020 indgået en foreløbig aftale om eksterne SAC ydelser, bl.a. for at imødegå det øgede trusselsbillede under COVID-19 perioden.

Til at understøtte udviklingen af den operationelle sikkerhed og opbygningen af den nye sektion er der igangsat en CIS20 analyse, som skal vurdere regionens aktuelle sikkerhedskontroller og hermed også inddrage KMD-rapporten fra 2017.

Compliance
Justitsministeriet har i juni 2020 igangsat en national evaluering af databeskyttelsesreglerne, som regionen bidrager til i regi af Danske Regioner. Region Hovedstaden oplever en række udfordringer i forhold til fortolkningen og udmøntningen af databeskyttelseslovgivningen, som regionen vil løfte i denne sammenhæng. Herudover vil regionen arbejde på at spille en mere aktiv rolle i dialogen på nationalt niveau for herigennem at sætte fokus på dilemmaer og løsninger i forhold til samspillet mellem på den ene side databeskyttelseslovgivningen og på den anden side visioner og strømninger i tiden omkring øget tværsektorielt samarbejde, øget digitalisering og bedre adgang til og anvendelse af sundhedsdata.

Region
Hovedstaden

Region Hovedstaden
Center for It, Medico og Telefoni