INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
M sum@sum.dk
W ism.dk

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

Dato: 23-05-2025
Enhed: Innovation, Life Science og Digitalisering
Sagsbeh.: Ann Cecilie Stemann Nielsen
Koordineret med: Sundhedsdatastyrelsen
Sagsnr.: 2025 - 2494

Indenrigs- og sundhedsministerens redegørelse til beretning nr. 9/2024 om regionernes beskyttelse af sundhedsdata mod cyberangreb

Statsrevisorerne afgav den 21. januar 2025 bemærkninger til Rigsrevisionens beretning nr. 9/2024 om regionernes beskyttelse af sundhedsdata mod cyberangreb.

Statsrevisorerne har på den baggrund anmodet om en redegørelse for de foranstaltninger og overvejelser, som beretningen giver anledning til i Indenrigs- og Sundhedsministeriet, jf. § 18, stk. 2, i lov om revision af statens regnskaber m.m.

I den forbindelse har jeg indhentet udtalelser fra regionsrådene, jf. § 18, stk. 3, i lov om revisionen af statens regnskaber m.v. I udtalelserne beskriver hver region de initiativer, som de har iværksat for at imødekomme kritikpunkter fra Rigsrevisionen. Derudover har regionerne beskrevet, hvornår de enkelte initiativer vurderes at være gennemført. Indenrigs- og Sundhedsministeriet vurderer som udgangspunkt, at oplysningerne i regionernes redegørelse om håndtering af de sikkerhedsspørgsmål, som Rigsrevisionens beretning peger på, kan være af fortrolig karakter, og derfor er de beskrevet overordnet og anonymiseret i denne ministerredegørelse, så initiativerne ikke refererer til navngivne regioner. Sundhedsdatastyrelsen har også haft redegørelsen i høring og har ikke haft bemærkninger til redegørelsen.

Indledende bemærkninger
Rigsrevisionens undersøgelse har haft til formål at undersøge, hvad regionerne gør for at beskytte hospitalernes sundhedsdata mod cyberangreb. Da det er regionernes ansvarsområde, har jeg indhentet udtalelser fra hvert enkelt regionsråd.

Gode digitale løsninger og brug af sundhedsdata er en afgørende forudsætning for at fremtidssikre vores sundhedsvæsen. Således er digital adgang til borgernes sundhedsoplysninger et vigtigt arbejdsredskab for sundhedspersonalet. Det danske sundhedsvæsen er blandt de mest digitale i verden, og der er fortsat et stort potentiale.

Digitaliseringen af sundhedsvæsenet skal naturligvis foregå i trygge og sikre rammer. Derfor er det også vigtigt at tage hånd om den risiko for cyberangreb, som følger med digitaliseringen. For regeringen er det afgørende, at sygehusene kan sikre deres systemer og data mod cyberangreb – både for at sikre, at borgeres sundhedsdata ikke havner i de forkerte hænder og for at sikre, at sundhedsvæsenet ikke sættes ud af drift. Det er essentielt, at de danske sundhedsdata er sikre, så de relevante oplysninger er tilgængelige, når de er nødvendige for behandling, og så borgerne fortsat kan stole på, at sundhedsvæsenet passer godt på de følsomme oplysninger, de betror sundhedsvæsenet.

Derfor er det vigtigt, at regionerne fortsætter deres arbejde med at styrke beskyttelsen af sundhedsdata mod cybertrusler. Det er derfor også positivt, at Rigsrevisionen har taget initiativ til denne undersøgelse af regionernes beskyttelse af sundhedsdata, som understøtter sundhedsvæsenets fokus på cybersikkerhed.
Jeg noterer mig, at Statsrevisorerne finder, at regionernes beskyttelse af sundhedsdata ikke er helt tilfredsstillende. Statsrevisorerne påpeger, at der dermed er er der risiko for, at følsomme og fortrolige sundhedsdata kommer i hænderne på uvedkommende eller ikke er pålidelige og tilgængelige, når der er brug for dem. Statsrevisorerne konstaterer endvidere, at regionerne generelt har gjort en indsats for at forhindre, at hackere opnår adgang til sundhedsdata. Alle regionerne har desuden forbedret deres cybersikkerhed i undersøgelsesperioden.

Foranstaltninger og overvejelser
Rigsrevisionen har i sin undersøgelse opstillet 15 konkrete vurderingskriterier. Alle regionerne opfylder mere end halvdelen af Rigsrevisionens opstillede vurderingskriterier for beskyttelse af sundhedsdata. Regionerne har leveret beskrivelser af de foranstaltninger, som undersøgelsen har givet anledning til for de områder, hvor de kun delvist opfylder kriterierne samt for de områder, hvor de ikke opfylder kriterierne.

På baggrund af regionsrådenes udtalelser noterer jeg mig, at alle regioner har igangsat konkrete initiativer til at imødekomme kritikpunkterne fra Rigsrevisionen, hvoraf flere initiativer allerede er gennemført. Derudover har regionerne fremlagt konkrete tidsplaner for, hvornår de initiativer som ikke allerede er gennemført, vurderes at være gennemførte. Størstedelen af disse initiativer forventes gennemført inden udgangen af 2025, mens de resterende forventes gennemført inden udgangen af 2026, og dele af et initiativ for en enkelt region inden udgangen af 2027, jf. tabel 1. Derudover har en region endnu ikke afklaret, hvordan den bedst imødekommer et af Rigsrevisionens kritikpunkter og vil indgå dialog med Rigsrevisionen herom for at sikre opfyldelse af kontrolmålet. En anden region er uenig i Rigsrevisionens vurdering vedrørende et af Rigsrevisionens kritikpunkter for den pågældende region.

Tabel 1: Tidsplan for regionernes initiativer vedr. Rigsrevisionens kritikpunkter

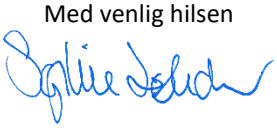
Rigsrevisionens vurderingskriterie	Tidsplan for færdiggørelse af initiativ
Har regionen tilstrækkeligt overblik over it-systemer med sundhedsdata?	Begge regioner forventes at være i mål inden udgangen af 2025.
Har regionen udført sårbarhedsscanninger?	En region har gennemført et initiativ, og den anden forventes at være i mål inden udgangen af 2025.
Har regionen opdaterede og ledelsesgodkendte risikovurderinger og handleplaner?	Den pågældende region har gennemført et initiativ.
Har regionen politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb?	Ikke relevant, da alle regioner vurderes at opfylde kriteriet i Rigsrevisionens beretning.
Har regionen sikret, at netværksudstyret er sikkerhedsopdateret?	Ikke relevant, da alle regioner vurderes at opfylde kriteriet i Rigsrevisionens beretning.

Har regionen en hensigtsmæssig brug af firewalls?	Den pågældende region har gennemført et initiativ.
Bruger regionen sikre passwords på netværksudstyret?	Ikke relevant, da alle regioner vurderes at opfylde kriteriet i Rigsrevisionens beretning.
Bruger regionen multifaktorlogin på netværksudstyret	Den pågældende region forventes at være i mål inden udgangen af 2026.
Har regionen implementeret systematisk logning og overvågning af netværkstrafikken?	Den pågældende region forventes at være i mål inden udgangen af 2025.
Har regionen segmenteret netværket	En region forventes at være i mål inden udgangen af 2025 og en i 3. kvartal 2026. En tredje region forventes at være i mål med segmentering af sine NIS-systemer inden udgangen af 2025 og med fuld implementering inden udgangen af 2027. En region er i dialog med Rigsrevisionen om opfyldelse af kontrolmålet.
Har regionen sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede?	Den ene region forventes at være i mål i 3. kvartal 2025, mens den anden region er uenig i Rigsrevisionens vurdering.
Har regionen sikret, at servere, der er kritiske for behandlingen af sundhedsdata, er sikker-hedsopdaterede?	Der er igangsat initiativer i de relevante regioner. (afrapporteres ikke med henvisning til enkelte regioner af hensyn til fortrolighed, jf. Rigsrevisionens beretning).
Har regionen en opdateret beredskabsplan for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan?	En region har gennemført et initiativ, og den anden forventes at være i mål inden udgangen af 2025.
Har regionen taget backup af de elektroniske patientjournaler?	Ikke relevant, da alle regioner vurderes at opfylde kriteriet i Rigsrevisionens beretning.
Har regionen gennemført regelmæssige restoretest af de elektroniske patientjournaler?	En region har gennemført et initiativ, og den anden forventes at være i mål i 1. halvår 2025.

Både ministeriet og regionerne anser Rigsrevisionens bemærkninger til regionernes beskyttelse af sundhedsdata mod cyberangreb som konstruktive bidrag til arbejdet med at sikre et stærkt cyberberedskab på hospitalerne. På baggrund af regionernes udtalelser, noterer jeg mig, at regionerne alle har fokus på at optimere sikkerheden med udgangspunkt i de opmærksomhedspunkter, som beretningen har fremhævet. Derudover har flere af regionerne allerede forbedret deres sikkerhed i Rigsrevisionens undersøgelsesperiode.

Ministeriet har samtidig sendt en kopi af ministerredegørelsen til Rigsrevisionen.

Med venlig hilsen



Sophie Løhde