FOLKETINGET
RIGSREVISIONEN

August 2025

Rigsrevisionens notat om beretning om

regionernes beskyttelse af sundhedsdata mod cyberangreb

Vedrører:

Statsrevisorernes beretning nr. 9/2024 om regionernes beskyttelse af sundhedsdata mod cyberangreb

Indenrigs- og sundhedsministerens redegørelse af 23. maj 2025

23. juni 2025

RN C111/25

1. Rigsrevisionen gennemgår i dette notat de initiativer, som indenrigs- og sundhedsministeren og regionerne har iværksat som følge af Statsrevisorernes bemærkninger og beretningens konklusioner. Dette sker med henblik på at vurdere, om Indenrigs- og Sundhedsministeriets og regionernes initiativer adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning.

Konklusion

Rigsrevisionen finder, at indenrigs- og sundhedsministeren og regionerne har redegjort for, hvordan regionerne vil følge op på Statsrevisorernes bemærkninger og de væsentligste kritikpunkter i beretningen.

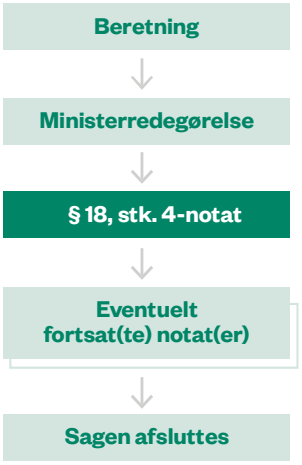
Ministeren oplyser, at alle regionerne har fokus på at optimere sikkerheden med udgangspunkt i de kritikpunkter, som fremgår af beretningen. Alle regionerne har igangsat konkrete initiativer til at imødekomme kritikpunkterne, og ministeren oplyser, at flere af initiativerne allerede er gennemført.

Derudover har regionerne fremlagt konkrete tidsplaner for, hvornår de initiativer, som ikke allerede er gennemført, vurderes at være gennemført. Størstedelen af initiativerne forventes gennemført inden udgangen af 2025. Ministeren oplyser, at regionerne vil have gennemført initiativer på alle områder ved udgangen af 2027.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Region Syddanmarks, Region Hovedstadens og Region Sjællands initiativer til at styrke grundlaget for at beskytte sundhedsdata mod cyberangreb
- regionernes tiltag til at beskytte sundhedsdata mod cyberangreb
- Region Syddanmarks, Region Midtjyllands og Region Nordjyllands initiativer til at sikre et fuldstændigt beredskab.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

I. Baggrund

2. Rigsrevisionen afgav i januar 2025 en beretning om regionenernes beskyttelse af sundhedsdata mod cyberangreb. Sundhedsdata kan fx være journaler, prøvesvar og røntgenbilleder.

3. Da Statsrevisorerne behandlede beretningen, fandt de, at regionernes beskyttelse af sundhedsdata ikke er helt tilfredsstillende. Dermed 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 konstaterede, 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.

4. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

5. Bilag 1 viser Folketingets behandling af beretningen.

II. Gennemgang af ministerens redegørelse og regionernes udtalelser

Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb

6. Statsrevisorerne bemærkede, at alle regionerne har politikker og retningslinjer for, hvordan de skal beskytte sundhedsdata. Men Region Syddanmark og Region Hovedstaden mangler at vurdere, hvor kritiske de enkelte it-systemer er for hospitalsdriften. Region Sjælland og Region Syddanmark har ikke fulgt samlet op på resultaterne af deres sårbarhedsskanninger på ledelsesniveau, og Region Sjælland mangler desuden at udarbejde risikovurderinger og handleplaner for sikkerheden omkring sundhedsdata.

7. Region Syddanmark oplyser, at de har etableret et overblik over it-systemer med sundhedsdata og har vurderet, hvor kritiske de enkelte systemer er. Region Hovedstaden oplyser, at de forventer at have fuldendt kortlægningen af en række af de mest kritiske it-systemer med sundhedsdata inden udgangen af 2025.

Region Syddanmark og Region Sjælland oplyser, at de har taget initiativ til at styrke opfølgningen på resultaterne af deres sårbarhedsskanninger. Region Sjællands initiativ er gennemført, og Region Syddanmarks initiativ vil være endeligt gennemført ved udgangen af 2025.

Endelig oplyser Region Sjælland, at de pr. marts 2025 har en ledelsesgodkendt risikovurdering af it-systemer med sundhedsdata med tilhørende handleplaner. Rigsrevisionen har ikke haft mulighed for at efterprøve regionens initiativer.

8. Rigsrevisionen vil fortsat følge Region Syddanmarks, Region Hovedstadens og Region Sjællands initiativer til at styrke grundlaget for at beskytte sundhedsdata mod cyberangreb.

Regionernes tiltag til at beskytte sundhedsdata mod cyberangreb

9. Statsrevisorerne bemærkede, at alle regionerne generelt har iværksat tiltag, der skal forhindre, at hackere kan opnå adgang til regionernes netværk med sundhedsdata. Region Hovedstaden anvender dog ikke multifaktorlogin eller har ikke segmenteret netværket for at forhindre spredning af cyberangreb.

Det fremgik af beretningen, at ingen af regionerne har foretaget en tilstrækkelig segmentering af de it-systemer med sundhedsdata, som de selv vurderer er kritiske for hospitalsdriften. Det fremgik desuden, at regionerne også på andre områder ikke har en tilstrækkelig beskyttelse af sundhedsdata mod cyberangreb. Flere af regionerne har fx mobile enheder, fx pc'er og mobiltelefoner, eller servere, der ikke er tilstrækkeligt sikkerhedsopdaterede.

10. Region Hovedstaden oplyser, at de forventer at have indført multifaktorlogin ultimo 2026. Multifaktorlogin øger sikkerheden ved login ved at sikre, at det er den korrekte bruger, der logger ind.

11. Region Sjælland oplyser, at det på grund af nogle ældre systemer ikke er muligt at udføre en fuldstændig segmentering af netværket, men at regionen har segmenteret de væsentligste kliniske it-systemer, fx Sundhedsplatformen. De øvrige regioner arbejder fortsat på at forbedre segmenteringen af deres netværk. Region Syddanmark har gennemført et længerevarende segmenteringsforløb og forventer at være færdig inden udgangen af 2025. Region Nordjylland forventer at have segmenteret alle it-systemer med sundhedsdata, der er kritiske for hospitalsdriften, inden udgangen af 2025 og de resterende systemer inden udgangen af 2027. Region Hovedstaden forventer at have segmenteret alle it-systemer med sundhedsdata ved udgangen af 3. kvartal 2026.

Region Midtjylland oplyser, at de arbejder med segmentering baseret på konkrete vurderinger ud fra en risikobaseret tilgang. Derfor arbejder regionen også med andre tiltag (fx intensiv overvågning), der kompenserer for eventuel manglende segmentering. Rigsrevisionen bemærker, at segmentering af netværk ifølge Center for Cybersikkerhed er et af de væsentligste tiltag til at forhindre spredning af cyberangreb. Rigsrevisionen har i forbindelse med undersøgelsen ikke set eksempler på tiltag i regionerne, der kan kompensere for manglende segmentering.

12. Endelig fremgår det af indenrigs- og sundhedsministerens redegørelse og regionernes udtalelser, at flere af regionerne arbejder på en række øvrige initiativer til beskyttelse af sundhedsdata mod cyberangreb. Det er fx brug af firewalls, logning og overvågning af netværkstrafikken. Regionerne vil også opdatere pc'er, mobiltelefoner og servere. Ifølge ministeren vil regionerne have implementeret initiativer på alle områder ved udgangen af 2027.

Region Hovedstaden har i deres udtalelse givet udtryk for, at de er uenige i, at de ikke i tilstrækkelig grad har sikkerhedsopdateret enheder, fx pc'er, mobiltelefoner og tablets. Rigsrevisionen skal bemærke, at det fremgår af Center for Cybersikkerheds vejledning "Cyberforsvar der virker", at al software, herunder bl.a. mobile enheder, servere og netværksudstyr, skal opdateres, når nye versioner eller sikkerhedsopdateringer frigives fra leverandøren. Dette har Region Hovedstaden ikke sikret.

13. Rigsrevisionen vil fortsat følge regionernes tiltag til at beskytte sundhedsdata mod cyberangreb.

Regionernes beredskab til at håndtere konsekvenserne af cyberangreb

14. Statsrevisorerne bemærkede, at alle regionerne har et beredskab til at håndtere konsekvenserne af cyberangreb, men dele af beredskabet er mangelfuldt i Region Midtjylland, Region Nordjylland og Region Syddanmark. Alle regionerne har beredskabsplaner til at håndtere cyberangreb, der rammer de elektroniske patientjournaler, men Region Midtjylland og Region Syddanmark har ikke testet deres beredskabsplaner regelmæssigt. Endelig har regionerne taget backup af de elektroniske patientjournaler, men Region Nordjylland og Region Syddanmark har ikke i tilstrækkeligt omfang testet, om deres backup kunne bruges til at reetablere de elektroniske patientjournaler ved nedbrud.

15. Region Syddanmark oplyser, at de har gennemført en it-beredskabsøvelse og fremadrettet vil gennemføre øvelser årligt. Regionen har også udarbejdet en reetableringsplan, som vil blive testet regelmæssigt, og gennemført en test af, om de elektroniske patientjournaler gendannes ud fra en backup ved nedbrud. Regionen vil fremadrettet foretage disse tests regelmæssigt.

Region Nordjylland oplyser, at de også årligt vil teste, om de elektroniske patientjournaler kan gendannes ud fra en backup ved nedbrud, og at resultaterne vil blive gennemgået systematisk.

Region Midtjylland oplyser, at deres it-beredskabsplan vil blive opdateret ultimo 2025. Rigsrevisionen forudsætter, at regionen også vil teste den opdaterede beredskabsplan regelmæssigt.

16. Rigsrevisionen vil fortsat følge Region Syddanmarks, Region Midtjyllands og Region Nordjyllands initiativer til at sikre et fuldstændigt beredskab.

Birgitte Hansen

Bilag 1. Folketingets behandling af beretningen

Beretning (nr.), dato for Statsrevisorernes mødebehandling og ministerredegørelse(r)	Behandlet i udvalg	Gennemgang ved Statsrevisorerne og Rigsrevisionen	Udvalgsspørgsmål (nr.)	Indkaldt til samråd	Statsrevisorerne har holdt møde med ministeren	§ 20-spørgsmål
Regionernes beskyttelse af sundhedsdata mod cyberangreb (nr. 9/2024) 20-01-2025 **Ministerredegørelse:** Indenrigs- og sundhedsministeren: 23-05-2025	Finansudvalget: 23-01-2025 Sundhedsudvalget: 28-01-2025 10-06-2025		Indenrigs- og sundhedsministeren: 30-01-2025 (253) 30-01-2025 (254)			