Kort fortalt

Regionernes beskyttelse af sundhedsdata mod cyberangreb

Konklusion

Regionernes indsats for at beskytte sundhedsdata er ikke helt tilfredsstillende. Regionerne har beskyttet sundhedsdata mod cyberangreb, men alle regioner kan forbedre deres beskyttelse. Regionerne har generelt gjort en indsats for at forhindre, at hackere opnår adgang til sundhedsdata, men har ikke gjort nok for at begrænse skaderne af cyberangreb i de tilfælde, hvor hackere er lykkedes med at opnå adgang til sundhedsdata. Konsekvensen er, at hackere har lettere ved at sprede deres angreb og potentielt sætte større dele af hospitalsvæsenet ud af drift.

Statsrevisorerne udtaler

"Statsrevisorerne finder, 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 konstaterer, 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".

Væsentligste resultater af undersøgelsen

- Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb varierer.
- Regionerne har iværksat flere relevante tiltag til at beskytte sundhedsdata mod cyberangreb, men har ikke gjort nok for at begrænse skaderne af succesfulde cyberangreb.
- Regionernes beredskab i forhold til de elektroniske patientjournaler varierer.

Baggrund og formål med undersøgelsen

Formålet med undersøgelsen er at vurdere, om regionerne i tilstrækkeligt omfang beskytter sundhedsdata i hospitalsvæsenet mod cyberangreb.

Center for Cybersikkerhed vurderede i maj 2024, at truslen fra cyberkriminalitet og cyberspionage mod den danske sundhedssektor er meget høj.

Et succesfuldt cyberangreb kan sætte hospitalernes kritiske it-infrastruktur ud af drift med den konsekvens, at patienter ikke kan få den nødvendige behandling. Det kan også betyde, at borgeres personlige helbredsoplysninger bliver ændret, slettet eller videregivet til uvedkommende.

Det danske sundhedsvæsen er blandt de mest digitale sundhedsvæsener i verden. Sundhedsdata, som før fandtes i fysiske papirjournaler, findes nu som digitale sundhedsdata, bl.a. i de elektroniske patientjournaler, som er et af sundhedspersonalets vigtigste værktøjer i hverdagen.

Den udbredte digitalisering betyder, at det danske sundhedsvæsen er sårbart over for cyberangreb.

Regionerne har ansvaret for de offentlige hospitalers it-systemer, der opbevarer og giver sundhedspersonalet adgang til sundhedsdata. Regionerne skal have dækkende viden om sårbarhederne i regionernes netværk og i de it-systemer, der indeholder sundhedsdata, ligesom regionerne skal tage de nødvendige skridt til løbende at beskytte sundhedsdata mod cyberangreb. Derudover skal regionerne have et beredskab til at håndtere konsekvenserne af cyberangreb, der rammer it-systemer med sundhedsdata.

Rigsrevisionen har opstillet en række konkrete vurderingskriterier, som følger af kravene i ISO 27001 og af anbefalingerne fra Center for Cybersikkerhed.

Figuren nedenfor viser, hvor mange af vurderingskriterierne de 5 regioner har opfyldt.

Læs hele rapporten på www.rigsrevisionen.dk. Kontakt Rigsrevisionens pressechef Lisbeth Sørensen på tlf. 33 92 85 06/ls@rigsrevisionen.dk eller Statsrevisorernes sekretariatschef Michala Krakauer på tlf. 33 37 59 89/michala.krakauer@ft.dk for yderligere information.

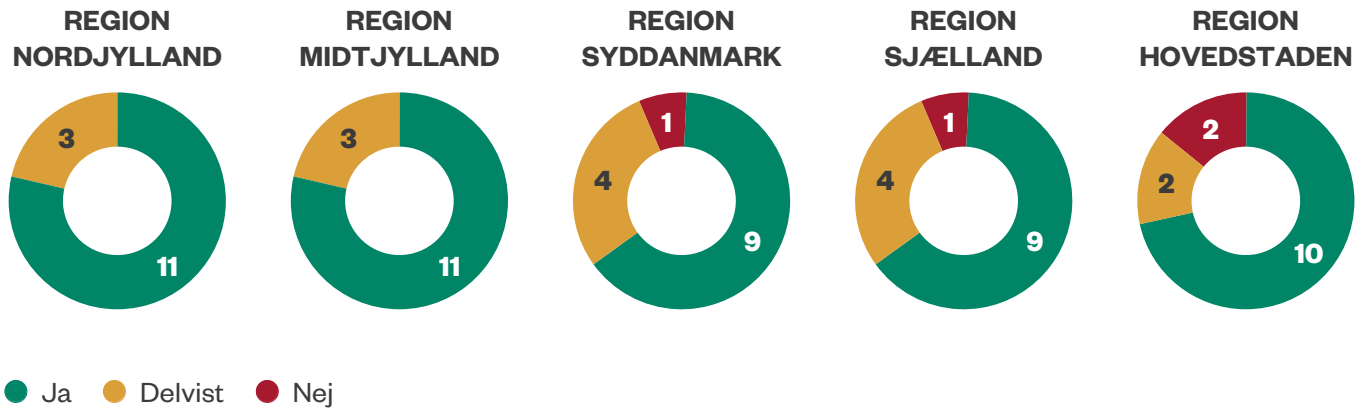
FOLKETINGET STATSREVISORERNE

FOLKETINGET RIGSREVISIONEN

Kort fortalt

Regionernes beskyttelse af sundhedsdata mod cyberangreb

Opfylder regionerne Rigsrevisionens vurderingskriterier?



Læs hele rapporten på www.rigsrevisionen.dk. Kontakt Rigsrevisionens pressechef Lisbeth Sørensen på tlf. 33 92 85 06/ls@rigsrevisionen.dk eller Statsrevisorernes sekretariatschef Michala Krakauer på tlf. 33 37 59 89/michala.krakauer@ft.dk for yderligere information.

FOLKETINGET STATSREVISORERNE

FOLKETINGET RIGSREVISIONEN