FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Januar 2025
– 9/2024

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

Regionernes beskyttelse af sundhedsdata mod cyberangreb

9/2024

Beretning om

regionernes beskyttelse af sundhedsdata mod cyberangreb

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2025

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Indenrigs- og sundhedsministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.

På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i august 2025.

Ministerens redegørelse, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2024, som afgives i februar 2026.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

ISSN: 2245-3008
ISBN online 978-87-7434-856-6

Statsrevisorernes bemærkning

Beretning om regionernes beskyttelse af sundhedsdata mod cyberangreb

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.

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.

Formålet med undersøgelsen er at vurdere, om regionerne i tilstrækkeligt omfang beskytter sundhedsdata i hospitalsvæsenet mod cyberangreb. Vurderingen sker på baggrund af 15 konkrete vurderingskriterier, som Rigsrevisionen har defineret på baggrund af den internationale standard for informationssikkerhed ISO 27001 og vejledningen "Cyberforsvar der virker" fra Center for Cybersikkerhed.

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.

Statsrevisorerne

20. januar 2025

Serdal Benli
Leif Lahn Jensen
Mikkel Irminger Sarbo
Lars Christian Lilleholt
Monika Rubin
Mai Mercado

Statsrevisorerne bemærker følgende:

- Alle regionerne har politikker og retningslinjer for, hvordan de skal beskytte sundhedsdata.
- 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.
- Region Sjælland mangler at udarbejde risikovurderinger og handleplaner for sikkerheden omkring sundhedsdata.
- Alle regionerne har generelt iværksat tiltag, der skal forhindre, at hackere kan opnå adgang til regionernes netværk med sundhedsdata.
- Alle regionerne på nær Region Hovedstaden anvender multifaktorlogin på netværksudstyret for at forhindre, at hackere opnår adgang til netværket.
- Region Hovedstaden har ikke segmenteret netværket for at forhindre spredning af cyberangreb.
- 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.
- Alle regionerne har taget backup af de elektroniske patientjournaler, men Region Nordjylland og Region Syddanmark har ikke i tilstrækkeligt omfang testet, om deres backup kan bruges til at reetablere de elektroniske patientjournaler ved nedbrud.

Indholdsfortegnelse

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionens mandat til at gennemføre undersøgelsen følger af § 4, stk. 1, nr. 1, jf. § 6 i rigsrevisorloven.

Beretningen vedrører finanslovens § 16. Indenrigs- og Sundhedsministeriet.

I undersøgelsesperioden 2. januar - 31. oktober 2024 har der været følgende ministre:

Sophie Løhde: december 2022 -

Beretningen har i udkast været forelagt Indenrigs- og Sundhedsministeriet, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Indledning

1.1. Formål og konklusion

1. Denne beretning handler om, hvad regionerne gør for at beskytte hospitalernes sundhedsdata mod cyberangreb. Sundhedsdata kan fx være journaler, prøvesvar og røntgenbilleder.

2. 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.

3. 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. Digitaliseringen understøtter, at sundhedspersonalet har adgang til personlige helbredsoplysninger på tværs af sundhedsvæsenet, så patienterne kan få et sammenhængende behandlingsforløb.

Den udbredte digitalisering betyder, at det danske sundhedsvæsen er sårbart over for cyberangreb. Sundhedsdata er værdifulde for cyberkriminelle og for fremmede stater, der kan opnå økonomiske eller teknologiske fordele ved cyberspionage. Cyberkriminelle kan fx bruge sundhedsdata til at afpresse borgere og organisationer.

4. Regionerne har ansvaret for de offentlige hospitalers it-systemer, der opbevarer og giver sundhedspersonalet adgang til sundhedsdata.

Regionerne har med aftalen "Fællesregional Informationssikkerhedspolitik" skullet følge kravene i den internationale standard for informationssikkerhed ISO 27001 siden januar 2017. ISO 27001 opstiller en række overordnede og generelle krav til arbejdet med informationssikkerhed. Rigsrevisionens undersøgelse tager – ligesom Rigsrevisionens øvrige undersøgelser af it- og cybersikkerhed – udgangspunkt i ISO 27001.

Center for Cybersikkerhed
Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Center for Cybersikkerhed er sat i verden for at hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

Kritisk it-infrastruktur
Ifølge Center for Cybersikkerhed er kritisk it-infrastruktur digitale elementer, som understøtter behandlingen af data, der er nødvendige for at kunne opretholde eller genoprette samfundsvigtige funktioner.

Cybersikkerhed og it-sikkerhed
Cybersikkerhed omfatter beskyttelse mod digitale angreb rettet mod data eller systemer via en ekstern forbindelse, fx gennem internettet.

It-sikkerhed omhandler mere bredt informationssikkerhed for data, der behandles i it-systemer.

Rigsrevisionen har opstillet 15 konkrete vurderingskriterier, som vi har udledt af ISO 27001 og af anbefalingerne fra Center for Cybersikkerhed. Nogle af hovedelementerne er, at 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.

5. Formålet med undersøgelsen er at vurdere, om regionerne i tilstrækkeligt omfang beskytter sundhedsdata i hospitalsvæsenet mod cyberangreb. Vi besvarer følgende spørgsmål i beretningen:

- Har regionerne et tilstrækkeligt grundlag for at beskytte sundhedsdata mod cyberangreb?
- Har regionerne iværksat tilstrækkelige tiltag til at beskytte sundhedsdata mod cyberangreb?
- Har regionerne et beredskab til at håndtere konsekvenserne af cyberangreb, der rammer de elektroniske patientjournaler?

Vi har undersøgt regionernes beskyttelse af deres netværk og de it-systemer med sundhedsdata, som regionerne vurderer som kritiske for hospitalsdriften. Hver region har 10-20 it-systemer med sundhedsdata, som er kritiske for hospitalsdriften, fx elektroniske patientjournaler, røntgensystemer og blodprøvesystemer. I det tredje spørgsmål har vi fokus på de elektroniske patientjournaler, som ifølge regionerne er de it-systemer med sundhedsdata, som er mest kritiske for hospitalsdriften.

6. Rigsrevisionen har selv taget initiativ til undersøgelsen i december 2023.

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.

Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb varierer

Alle regionerne har politikker og retningslinjer for, hvordan de skal beskytte sundhedsdata. Alle regionerne har desuden et overblik over deres it-systemer med sundhedsdata og foretager sårbarhedsskanninger. 2 af regionerne mangler dog at vurdere, hvor kritiske it-systemerne er for hospitalsdriften, og 2 af regionerne mangler at følge samlet op på sårbarhedsskanningerne på ledelsesniveau. Endelig mangler en enkelt region at udarbejde risikovurderinger og handleplaner for sikkerheden omkring sundhedsdata.

Regionerne har iværksat flere relevante tiltag til at beskytte sundhedsdata mod cyberangreb, men har ikke gjort nok for at begrænse skaderne af succesfulde cyberangreb

Alle regionerne har generelt iværksat tiltag, der skal forhindre, at hackere kan opnå adgang til regionernes netværk med sundhedsdata. Tiltagene kan fx være at bruge sikre passwords og sikkerhedsopdatere netværksudstyret. Undersøgelsen viser dog, at regionerne ikke har gjort nok for at forhindre spredning af succesfulde cyberangreb. Fx har regionerne kun i begrænset omfang arbejdet med at adskille deres kritiske it-systemer med sundhedsdata i segmenter. Desuden har flere af regionerne bl.a. ikke sikkerhedsopdateret pc'er og mobiltelefoner med adgang til sundhedsdata.

Regionernes beredskab i forhold til de elektroniske patientjournaler varierer

2 af regionerne har et beredskab til at håndtere konsekvenserne af cyberangreb, der rammer de elektroniske patientjournaler. De øvrige 3 regioner har forskellige mangler i deres beredskab. Undersøgelsen viser fx, at 2 af regionerne ikke har testet deres beredskab regelmæssigt og heller ikke har beskrivelser af, hvordan de elektroniske patientjournaler skal reetableres. Alle regionerne har taget backup af de elektroniske patientjournaler, men 2 af regionerne har ikke i tilstrækkeligt omfang testet, om deres backup kan bruges til at reetablere de elektroniske patientjournaler ved nedbrud.

Alle regionerne har forbedret deres sikkerhed i undersøgelsesperioden på baggrund af Rigsrevisionens resultater og har oplyst, at de fortsat vil arbejde med at forbedre deres beskyttelse af sundhedsdata mod cyberangreb.

1.2. Baggrund

7. Der er ifølge Center for Cybersikkerhed en alvorlig cybertrussel mod sundhedssektoren i Danmark. Truslen kommer særligt fra cyberkriminelle og fra fremmede stater i form af cyberspionage.

Flere europæiske lande har allerede været ramt af cyberangreb i sundhedsvæsenet. Boks 1 viser eksempler på cyberangreb mod sundhedsvæsenet i Irland, Tyskland og England.

Boks 1
Eksempler på cyberangreb

Cyberangreb mod sundhedsvæsenet i Irland
I maj 2021 blev det irske sundhedsvæsen ramt af et cyberangreb. Hackerne krypterede sundhedsdata og forlangte en løsesum for at genetablere adgangen. Angrebet resulterede i omfattende aflysninger af behandlinger. Desuden blev 520 patienters følsomme personoplysninger offentliggjort på internettet. Det irske sundhedsvæsen har pr. april 2023 informeret over 90.000 borgere om, at deres sundhedsdata er blevet berørt af angrebet.

Cyberangreb mod 3 hospitaler i Tyskland
Hackere udførte et cyberangreb mod 3 hospitaler i Tyskland den 24. december 2023. Ifølge hospitalerne var der tale om et angreb, hvor sundhedsdata blev krypteret. Angrebet resulterede i, at de 3 hospitaler i en periode ikke kunne bruge flere af deres it-systemer, og at akutpatienter måtte omdirigeres til andre hospitaler.

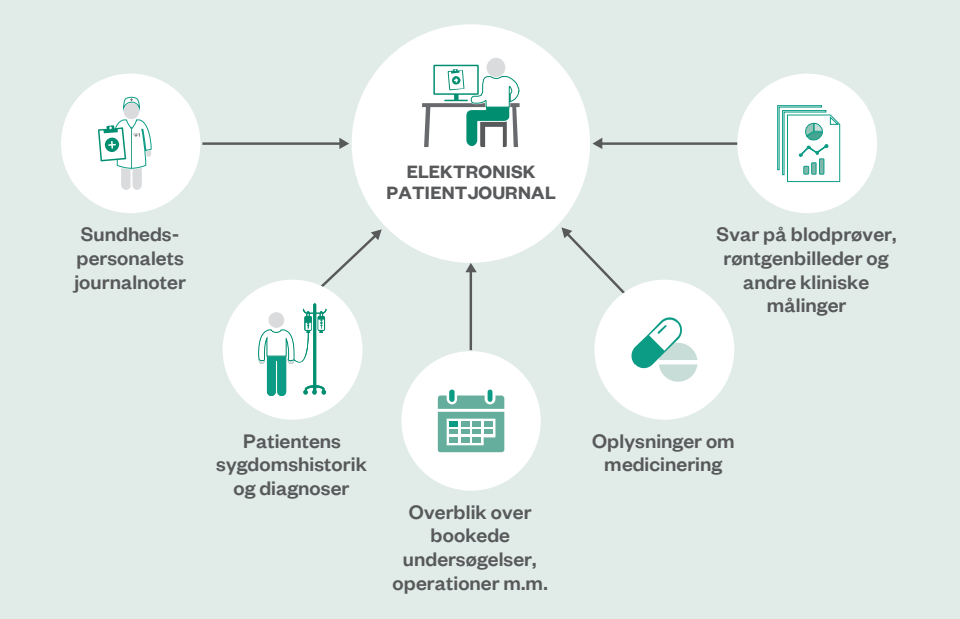
Cyberangreb mod sundhedsvæsenet i England
Den 3. juni 2024 blev det engelske sundhedsvæsen ramt af et cyberangreb. Hackerne krypterede data om over 300 millioner kontakter mellem patienter og sundhedsvæsenet og forlangte en løsesum for at genetablere adgangen. De krypterede data dækker bl.a. over svar på blodprøver vedrørende kræft og seksuelt overførte sygdomme. En mindre del af de krypterede data er blevet offentliggjort på internettet. I 2 uger efter angrebet blev over 1.000 planlagte operationer aflyst, herunder kræftbehandlinger og organtransplantationer.

Regionernes sundhedsdata

8. Regionerne behandler årligt tusindvis af patienter på de offentlige hospitaler. Når man som patient får behandling på et hospital, registrerer sundhedspersonalet følsomme personoplysninger. Oplysningerne bliver en del af de sundhedsdata, som regionerne har ansvaret for, og som er nødvendige for at opretholde hospitalernes kritiske funktioner.

Sundhedsdata tilgås af sundhedspersonalet gennem it-systemer, der er forbundet i regionernes netværk. Alle de offentlige hospitaler håndterer fx sundhedsdata i elektroniske patientjournaler. De elektroniske patientjournaler samler mange forskellige former for sundhedsdata ét sted. Figur 1 viser et udsnit af de sundhedsdata, de elektroniske patientjournaler indeholder.

Figur 1
Sundhedsdata i de elektroniske patientjournaler



Kilde: Rigsrevisionen på baggrund af oplysninger fra regionerne.

9. Regionerne skal beskytte deres netværk og de it-systemer, der indeholder sundhedsdata, mod cyberangreb. Det skal de gøre på 2 måder.

For det første skal regionerne sikre, at det ikke er muligt for hackere at komme ind i netværkene gennem det netværksudstyr, der forbinder netværkene til internettet. Det kaldes den *eksterne sikring*. Det kan fx ske ved at stille krav om sikre passwords og multifaktorlogin på netværksudstyret.

For det andet skal regionerne forhindre, at hackere kan sprede deres cyberangreb, hvis de først har opnået adgang til netværkene. Det kaldes den *interne sikring*. Det kan fx gøres ved at inddele netværkene i mindre dele (segmenter), så hackerne ikke kan bevæge sig fra ét it-system til et andet. Hvis hackerne først har opnået adgang til regionernes netværk, netværksudstyr og pc'er m.m. inden for netværket, kan hackerne fx lukke for regionernes internetadgang, slette data og skabe driftsforstyrrelser.

Det er vigtigt at understrege, at den eksterne sikring aldrig kan blive så god, at regionerne ikke behøver at implementere tiltag til at styrke den interne sikring. Det skyldes, at truslen fra cyberangreb konstant forandrer sig i takt med den teknologiske udvikling.

Multifaktorlogin
Multifaktorlogin er en loginproces, hvor brugeren får adgang på baggrund af sit brugernavn og 2 eller flere faktorer, fx:

- noget brugeren ved (fx password)
- noget brugeren har (fx mobiltelefon eller nøglekort)
- noget brugeren er (fx ansigtsgenkendelse eller fingeraftryk).

1.3. Vurderingskriterier, metode og afgrænsning

Vurderingskriterier

ISO 27001
ISO 27001 er den internationale standard for informationssikkerhed. Vedligeholdelse af ISO-standarderne varetages af internationalt sammensatte ekspertgrupper, der med jævne mellemrum vurderer behovet for revision.

"Cyberforsvar der virker"
Center for Cybersikkerheds grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb udkom første gang i 2013. Den seneste udgave udkom i juli 2023 i en opdateret version af udgaven fra januar 2017.

10. Regionerne har med aftalen "Fællesregional Informationssikkerhedspolitik" fra 2017 forpligtet sig til at efterleve den internationale standard for informationssikkerhed ISO 27001. Undersøgelsen tager derfor udgangspunkt i kravene i ISO 27001.

Undersøgelsen tager også udgangspunkt i Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (4. udgave fra juli 2023). Vejledningen beskriver sikringstiltag, der skal give en høj grad af beskyttelse mod cyberangreb.

På baggrund af ISO 27001 og "Cyberforsvar der virker" har vi defineret 15 konkrete vurderingskriterier, som vi har undersøgt i hver af de 5 regioner. Sammenhængen mellem de 15 vurderingskriterier, ISO 27001 og anbefalingerne fra Center fra Cybersikkerhed er beskrevet i bilag 1.

Vi skal understrege, at de retningslinjer og anbefalinger, der ligger til grund for de 15 vurderingskriterier, ikke er statiske. Da risikobilledet løbende ændrer sig, vil anbefalinger til god praksis inden for cybersikkerhed også ændre sig. Opfyldelse af de 15 vurderingskriterier er dermed ikke ensbetydende med et tilstrækkeligt niveau af cybersikkerhed fremover.

Metode

11. Undersøgelsen er baseret på en dokumentgennemgang. Vi har bl.a. undersøgt regionernes planer, retningslinjer og politikker, herunder deres risikovurderinger, it-beredskabsplaner, procesbeskrivelser for ændringer i firewallregler samt politikker for it-sikkerhed, passwords og backup.

Vi har desuden set på, hvordan regionerne har implementeret tekniske tiltag til at beskytte hospitalsvæsenets sundhedsdata mod cyberangreb. Det har vi bl.a. gjort ved at lade regionerne demonstrere deres tiltag i praksis. Vi har også gennemgået rapporter, hvor regionernes status på sikkerhedsopdateringer af servere, pc'er, mobiltelefoner, tablets og netværksudstyr fremgår.

Gennemgangen af de 15 vurderingskriterier skal tages med det forbehold, at ikke alle kriterierne er lige væsentlige i forhold til cybersikkerhed.

Vi har undersøgt regionernes beskyttelse af sundhedsdata mod cyberangreb i perioden januar-oktober 2024. Flere af regionerne har forbedret deres sikkerhed i undersøgelsesperioden. Undersøgelsens resultater er derfor et udtryk for regionernes beskyttelse af sundhedsdata mod cyberangreb ved revisionens afslutning i oktober 2024.

12. Undersøgelsens metode og de 15 vurderingskriterier uddybes i bilag 1.

13. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

14. Undersøgelsen er afgrænset til regionernes beskyttelse af hospitalsvæsenets sundhedsdata mod cyberangreb. Vi har ikke undersøgt beskyttelsen af sundhedsdata i praksissektoren, hvor ansvaret for cybersikkerheden påhviler de praktiserende læger.

Vi vurderer, at de undersøgte tiltag er de væsentligste. Det vurderer vi på baggrund af den aktuelle sikkerhedssituation, undersøgelsens genstandsfelt (sundhedsdata i hospitalsvæsenet) og regionernes organisering af arbejdet med cybersikkerhed. Tiltagene er dog ikke udtømmende i forhold til god cybersikkerhed. Vi har fx ikke undersøgt den fysiske sikkerhed omkring servere.

15. Vi har undersøgt regionernes netværk og de it-systemer med sundhedsdata, som regionerne vurderer som kritiske for hospitalsdriften. I afsnit 2.3 har vi afgrænset os til at undersøge regionernes beredskab i forhold til de elektroniske patientjournaler. Det har vi gjort, fordi de elektroniske patientjournaler – også ifølge regionerne – er de it-systemer med sundhedsdata, som er mest kritiske for hospitalsvæsenet.

Forskelle i regionernes elektroniske patientjournaler

Region Hovedstaden og Region Sjælland bruger Sundhedsplatformen, som er et bredt dækkende it-system. Sundhedsplatformen erstatter op til 30 tidligere it-systemer. Region Nordjylland, Region Midtjylland og Region Syd bruger Columna Cis, som ikke dækker så bredt, og derfor har de 3 regioner andre supplerende it-løsninger.

2. Regionernes beskyttelse af sundhedsdata mod cyberangreb

16. Dette kapitel handler om, hvorvidt regionerne beskytter hospitalsvæsenets sundhedsdata mod cyberangreb.

17. Figur 2 viser 3 overordnede indsatsområder til beskyttelse af sundhedsdata og kapitlets struktur.

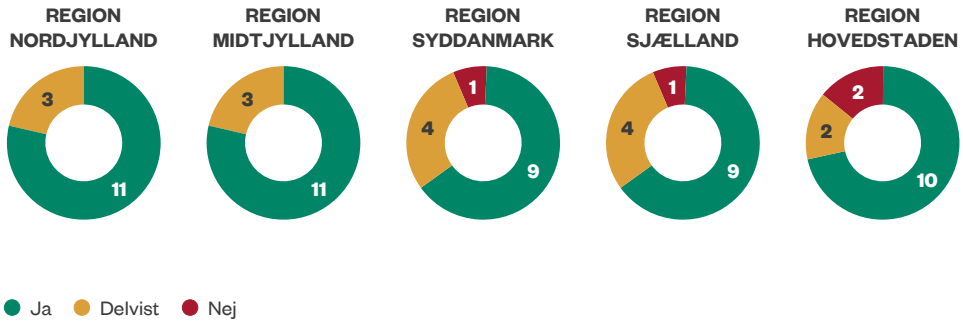
Figur 2
Indsatsområder og kapitlets struktur

AFSNIT 2.1	AFSNIT 2.2	AFSNIT 2.3
Har regionerne et tilstrækkeligt **grundlag** for at beskytte sundhedsdata mod cyberangreb?	Har regionerne iværksat tilstrækkelige tiltag til at **beskytte** sundhedsdata mod cyberangreb?	Har regionerne et **beredskab** til at håndtere konsekvenserne af cyberangreb, der rammer de elektroniske patientjournaler?
		
Regionerne skal: • have overblik over it-systemer med sundhedsdata • udføre sårbarhedsskanninger og følge op på resultaterne på ledelsesniveau • have opdaterede og ledelsesgodkendte risikovurderinger og handleplaner • have politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb.	**Regionerne skal:** • sikre, at netværksudstyret er sikkerhedsopdateret • have en hensigtsmæssig brug af firewalls • bruge sikre passwords på netværksudstyret • bruge multifaktorlogin på netværksudstyret • implementere systematisk logning og overvågning af netværkstrafikken • segmentere netværket • sikre, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede • sikre, at de servere, der er kritiske for behandlingen af sundhedsdata, er sikkerhedsopdaterede.	**Regionerne skal:** • have opdaterede beredskabsplaner for de elektroniske patientjournaler, herunder krisestyringsplaner, nødplaner og reetableringsplaner • tage backup af de elektroniske patientjournaler • gennemføre regelmæssige restoretest af de elektroniske patientjournaler.

Kilde: Rigsrevisionen på baggrund af ISO 27001 og anbefalinger fra Center for Cybersikkerhed.

18. Vi har undersøgt de 3 indsatsområder ved at gennemgå, om regionerne opfylder konkrete vurderingskriterier. Figur 3 viser, hvor mange af kriterierne regionerne har opfyldt.

Figur 3
Opfylder regionerne Rigsrevisionens vurderingskriterier?



Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rødt, hvis ingen af de nødvendige elementer er til stede. Sammenligninger mellem regionernes resultater skal tages med det forbehold, at ikke alle vurderingskriterier er lige vigtige i forhold til cybersikkerhed. For en uddybende oversigt, se tabel B i bilag 1.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Det fremgår af figur 3, at alle regionerne opfylder mere end halvdelen af vurderingskriterierne for beskyttelse af sundhedsdata mod cyberangreb. Alle regionerne har dog også områder, hvor de kun delvist opfylder kriterierne. 3 regioner har desuden områder, hvor de ikke opfylder kriterierne. Det betyder, at de 3 regioner på disse områder ikke følger ISO 27001 og anbefalingerne fra Center for Cybersikkerhed.

I de følgende afsnit uddybes undersøgelsens resultater og indholdet af de enkelte vurderingskriterier.

2.1. Grundlag for at beskytte sundhedsdata mod cyberangreb

19. For at undersøge, om regionerne har et tilstrækkeligt grundlag for at beskytte sundhedsdata mod cyberangreb, har vi undersøgt, om regionerne:

- har overblik over it-systemer med sundhedsdata
- har udført sårbarhedsskanninger og fulgt op på resultaterne på ledelsesniveau
- har opdaterede og ledelsesgodkendte risikovurderinger og handleplaner
- har politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb.

Hver region har 10-20 it-systemer med sundhedsdata, som er kritiske for hospitalsdriften.

Sårbarhedsskanninger
Sårbarhedsskanninger er en test af cybersikkerheden. En sårbarhedsskanning simulerer delelementer af et cyberangreb ved at udsætte en organisations systemer og netværk for kendte trusler. Formålet er at opdage eventuelle sårbarheder.

20. Undersøgelsen viser, at grundlaget for at beskytte sundhedsdata mod cyberangreb varierer på tværs af regionerne. 2 af regionerne har et tilfredsstillende grundlag, mens der er mangler hos de øvrige regioner, jf. tabel 1.

Tabel 1
Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen overblik over it-systemer med sundhedsdata?	●	●	●	●	●
Har regionen udført sårbarhedsskanninger og fulgt op på resultaterne på ledelsesniveau?	●	●	●	●	●
Har regionen opdaterede og ledelsesgodkendte risikovurderinger og handleplaner?	●	●	●	●	●
Har regionen politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb?	●	●	●	●	●

● Ja ● Delvist ● Nej

Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rødt, hvis ingen af de nødvendige elementer er til stede.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

I det følgende gennemgår vi de enkelte resultater.

Overblik over it-systemer med sundhedsdata

Overblik over it-systemer med sundhedsdata

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

21. Regionerne skal have overblik over deres it-systemer for at efterleve ISO 27001. Overblikket bør indeholde en angivelse af, hvem der har adgang til it-systemerne, og regionernes vurdering af, hvor kritiske it-systemerne er for hospitalsdriften. Overblikket skal danne grundlag for, at regionerne kan prioritere, hvilke tiltag der skal til for at beskytte sundhedsdata mod cyberangreb. Overblikket er også afgørende for, at regionerne kan prioritere, hvilke it-systemer der skal håndteres først i en krisesituation.

22. Undersøgelsen viser, at alle regionerne har overblik over deres it-systemer med sundhedsdata. 2 af regionerne har dog ikke foretaget en systematisk vurdering af, hvor kritiske it-systemerne er for hospitalsdriften. Det indebærer en risiko for, at regionerne fejlvurderer, hvilke it-systemer der skal håndteres først i en krisesituation.

Sårbarhedsskanninger og opfølgning på resultaterne på ledelsesniveau

23. Regionerne skal indhente viden om tekniske sårbarheder i deres it-løsninger og evaluere sikkerheden på baggrund heraf for at efterleve ISO 27001. De tekniske sårbarheder kan afdækkes på flere måder. Center for Cybersikkerhed fremhæver bl.a. sårbarhedsskanninger som en metode til at teste den eksisterende sikkerhed.

24. Undersøgelsen viser, at alle regionerne har udført sårbarhedsskanninger. 2 af regionerne har dog ikke fulgt samlet op på resultaterne af sårbarhedsskanningerne på ledelsesniveau. Resultaterne af sårbarhedsskanningerne indgår således ikke som en del af ledelsens grundlag for at prioritere mellem de tekniske tiltag, der skal minimere hullerne i sikkerheden omkring sundhedsdata. Dermed er der risiko for, at regionerne ikke får fulgt op på og prioriteret, at eventuelle sårbarheder løses. Der er også risiko for, at hackere kan udnytte disse sårbarheder til at angribe it-systemer med sundhedsdata.

Sårbarhedsskanninger

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Opdaterede og ledelsesgodkendte risikovurderinger og handleplaner

25. Regionerne skal udarbejde risikovurderinger og handleplaner som en del af ledelsens risikostyring for at efterleve ISO 27001. Risikovurderingerne og handleplanerne skal være ledelsesgodkendte for bl.a. at sikre, at ledelsen er orienteret om de identificerede risici.

26. Undersøgelsen viser, at 4 af regionerne har opdaterede og ledelsesgodkendte risikovurderinger og handleplaner. Region Sjælland har ikke risikovurderet sine kritiske it-systemer med sundhedsdata og har ikke udarbejdet tilhørende handleplaner. Dermed har regionen ikke et tilstrækkeligt grundlag for at prioritere mellem de tekniske tiltag, der kan øge cybersikkerheden.

Risikovurderinger og handleplaner

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb

27. Regionerne skal have politikker og retningslinjer for cybersikkerheden for at efterleve ISO 27001 og anbefalingerne fra Center for Cybersikkerhed. Vi har undersøgt regionernes politikker og retningslinjer for adgangsstyring, genoprettelse af data, it-beredskab og behandling af sundhedsdata.

28. Undersøgelsen viser, at alle regionerne har retningslinjer for beskyttelse af sundhedsdata på de indsatsområder, vi har undersøgt. Regionsrådene i de 5 regioner godkendte i 2017 en fællesregional informationssikkerhedspolitik. Alle regionerne har herudover udarbejdet specifikke informationssikkerhedspolitikker for den enkelte region.

Politikker og retningslinjer

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

2.2. Beskyttelse af sundhedsdata mod cyberangreb

Firewall
En firewall har til formål at kontrollere netværkstrafikken. Oftest sidder firewallen mellem adgangen til et ubeskyttet netværk, fx internettet, og et beskyttet netværk.

Netværksudstyr
Netværksudstyr dækker bl.a. over routere, der forbinder regionernes netværk med internettet, og firewalls, der begrænser, hvilken information der kan modtages fra internettet og sendes mellem it-systemerne.

Segmentering af netværket
Et netværk er segmenteret, når det er opdelt i afgrænsede områder. Det medvirker fx til at sikre, at cyberangreb ikke kan sprede sig til alle it-systemerne.

Logning
Alle handlinger på regionernes it-systemer efterlader et digitalt fingeraftryk, som kan opsamles i en log. Med logningen kan man spore hændelsesforløbet for tidligere cyberangreb, og man kan dermed opnå værdifuld viden, der kan bruges til at forebygge fremtidige angreb.

29. Regionerne skal iværksætte passende tiltag for at mindske tekniske sårbarheder for at efterleve ISO 27001. Center for Cybersikkerhed anbefaler desuden en række konkrete tekniske tiltag, som skal beskytte mod cyberangreb.

30. For det første har vi undersøgt den eksterne sikring af regionernes netværk. Den eksterne sikring består af tiltag, der skal forhindre, at hackere opnår adgang til regionernes netværk. Konkret har vi undersøgt, om regionerne:

- har sikret, at netværksudstyret er sikkerhedsopdateret
- har en hensigtsmæssig brug af firewalls
- bruger sikre passwords på netværksudstyret
- bruger multifaktorlogin på netværksudstyret
- har implementeret systematisk logning og overvågning af netværkstrafikken.

Undersøgelsen viser, at alle regionerne – målt på de fleste parametre – har iværksat tilstrækkelige tiltag til at styrke den eksterne sikring af deres netværk.

31. For det andet har vi undersøgt den interne sikring af regionernes netværk. Den interne sikring består af tiltag, som skal forhindre spredning af et eventuelt succesfuldt cyberangreb. Det har vi gjort ved at undersøge, om regionerne:

- har segmenteret netværket
- har sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede
- har sikret, at de servere, der er kritiske for behandlingen af sundhedsdata, er sikkerhedsopdaterede.

Undersøgelsen viser, at ingen af regionerne har iværksat tilstrækkelige tiltag til at forhindre spredning af succesfulde cyberangreb.

Ekstern sikring af netværket mod cyberangreb

32. Tabel 2 viser resultatet af Rigsrevisionens undersøgelse af regionernes tiltag til at forhindre, at hackere opnår adgang til netværket.

Tabel 2
Regionernes tiltag til at forhindre, at hackere opnår adgang til netværket

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen sikret, at netværksudstyret er sikkerhedsopdateret?	●	●	●	●	●
Har regionen en hensigtsmæssig brug af firewalls?	●	●	●	●	●
Bruger regionen sikre passwords på netværksudstyret?	●	●	●	●	●
Bruger regionen multifaktorlogin på netværksudstyret?	●	●	●	●	●
Har regionen implementeret systematisk logning og overvågning af netværkstrafikken?	●	●	●	●	●

● Ja ● Delvist ● Nej

Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rødt, hvis ingen af de nødvendige elementer er til stede.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Sikkerhedsopdatering af netværksudstyret

33. Regionerne skal iværksætte passende tiltag for at minimere tekniske sårbarheder for at efterleve ISO 27001. Opdateringer af software bør indgå som en del af dette arbejde. Center for Cybersikkerhed anbefaler desuden, at al software, herunder software på netværksudstyret, er sikkerhedsopdateret.

Regionernes netværksudstyr, fx routere og firewalls, er et attraktivt mål for hackere. Hvis hackerne lykkes med at kompromittere netværksudstyret, kan de bruge det som en adgang til at nå dybere ind i regionernes netværk. Vi har på den baggrund undersøgt, om regionerne har sikret, at det netværksudstyr, der forbinder regionernes netværk med internettet, er sikkerhedsopdateret.

34. Undersøgelsen viser, at alle regionerne har sikret, at deres netværksudstyr er sikkerhedsopdateret.

Sikkerhedsopdatering af netværksudstyret

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Hensigtsmæssig brug af firewalls

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Hensigtsmæssig brug af firewalls

35. Regionerne skal sikre, styre og kontrollere deres netværk og netværksudstyr, herunder firewalls, for bl.a. at beskytte data i it-systemerne. Det følger af ISO 27001. Regionernes firewalls skal sættes op, så de forhindrer uønsket datatrafik mellem regionernes netværk og internettet. Det gør regionerne ved at sætte regler op for datatrafikken. For at sikre en hensigtsmæssig brug af firewalls skal regionerne derfor systematisk gennemgå, om reglerne sikrer, at det kun er den ønskede datatrafik, der tillades.

36. Undersøgelsen viser, at 4 af regionerne har en hensigtsmæssig brug af deres firewalls. Regionerne har en fast praksis for at gennemgå reglerne i deres firewalls. Region Sjælland har ikke en fast praksis herfor, og gennemgangen sker mere sporadisk.

Sikre passwords

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Sikre passwords på netværksudstyret

37. For at efterleve ISO 27001 skal regionernes medarbejdere bruge sikre passwords i overensstemmelse med bedste praksis. Vi har undersøgt, om regionerne stiller krav om, at medarbejdere med privilegeret adgang til netværksudstyret bruger passwords med minimum 15 karakterer. Karaktererne skal bestå af tal, specialtegn samt store og små bogstaver i overensstemmelse med anbefalingerne fra Center for Cybersikkerhed. Lange og komplekse passwords er sværere for hackere at afkode. Det er særligt vigtigt, at medarbejdere med adgang til netværksudstyret bruger sikre passwords, bl.a. fordi deres adgang giver mulighed for, at hackere kan ændre i opsætningen af regionernes firewalls i forbindelse med cyberangreb.

38. Undersøgelsen viser, at alle regionerne bruger passwords, der er i overensstemmelse med anbefalingerne fra Center for Cybersikkerhed, når de logger ind på netværksudstyret.

Multifaktorlogin

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Multifaktorlogin på netværksudstyret

39. For at efterleve ISO 27001 og anbefalingerne fra Center for Cybersikkerhed skal regionerne bruge multifaktorlogin ved ekstern adgang til kritiske it-systemer. Ekstern adgang er fx, når medarbejdere logger på hjemmefra, eller når en it-leverandør har adgang til regionens it-systemer fra sin egen virksomhed. Multifaktorlogin betyder, at en medarbejder skal bruge 2 eller flere faktorer for at opnå adgang til et it-system. En faktor er fx et password, en kode sendt til en mobil enhed via en app eller biometriske data som fingeraftryk eller ansigtsgenkendelse. Multifaktorlogin øger sikkerheden ved login ved at sikre, at det er den korrekte bruger, der logger ind.

Vi har ligesom med sikre passwords afgrænset os til at undersøge, om medarbejdere med privilegeret adgang til regionernes netværksudstyr bruger multifaktorlogin.

40. Undersøgelsen viser, at 4 af regionerne har implementeret multifaktorlogin ved login på netværksudstyret. Hos Region Hovedstaden, som ikke bruger multifaktorlogin, er der risiko for, at hackere kan opnå adgang til regionens netværk, hvis de stjæler brugernavne og passwords fra brugerne.

Systematisk logning og overvågning af netværkstrafikken

41. Regionerne skal systematisk logge aktiviteter og hændelser, herunder netværkstrafikken. Det følger af ISO 27001 og af anbefalingerne fra Center for Cybersikkerhed. Formålet med logningen er bl.a. at identificere unormale trafikmønstre, der kan være tegn på cyberangreb. Regionernes logning af netværkstrafikken vedrører både trafikken inden for de regionale netværk og trafikken fra de regionale netværk til internettet. Vi har undersøgt, om regionerne har implementeret systematisk logning og overvågning af netværkstrafikken.

42. Undersøgelsen viser, at 4 af regionerne har implementeret en systemunderstøttet logning og overvågning af netværkstrafikken. Region Midtjyllands logning og overvågning er delvist systemunderstøttet. Det betyder, at regionen ikke har et fuldt overblik over trafikken på sit netværk. Konsekvensen er, at der er større risiko for, at regionen overser cyberangreb mod regionens netværk.

Logning og overvågning

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Intern sikring af netværket mod cyberangreb

43. Tabel 3 viser resultatet af Rigsrevisionens undersøgelse af regionernes tiltag til at forhindre spredning af cyberangreb.

Tabel 3
Regionernes tiltag for at forhindre spredning af cyberangreb

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen segmenteret netværket?	●	●	●	●	●
Har regionen sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede?	●	●	●	●	●

● Ja ● Delvist ● Nej

Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rødt, hvis ingen af de nødvendige elementer er til stede.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Segmentering af netværket

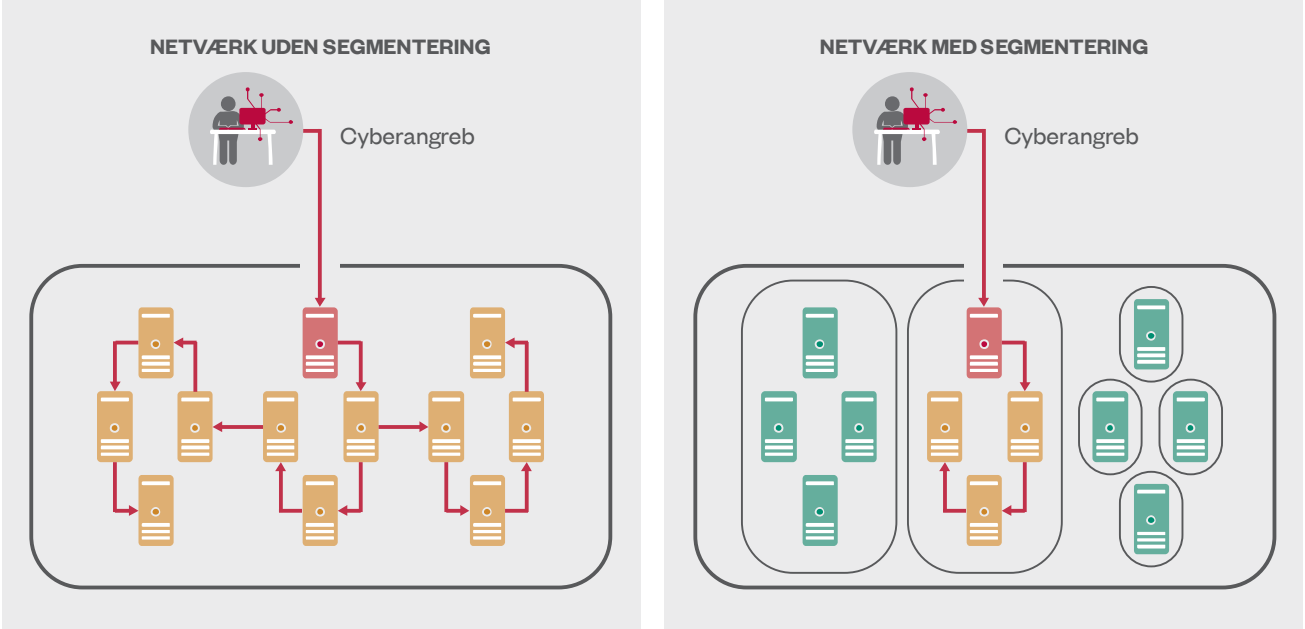
44. For at efterleve ISO 27001 og anbefalingerne fra Center for Cybersikkerhed skal regionerne segmentere deres netværk.

Segmentering betyder, at man opdeler netværket i mindre dele (segmenter). Opdelingen begrænser netværkstrafikken mellem forskellige it-systemer inden for netværket. På den måde kan man undgå, at et cyberangreb, der rammer ét it-system eller en mindre gruppe af it-systemer, spreder sig til andre it-systemer inden for netværket. Segmentering er ifølge Center for Cybersikkerhed et af de vigtigste tiltag, som man kan iværksætte for at begrænse skaderne af cyberangreb. På den baggrund har vi undersøgt, om regionerne har segmenteret deres netværk.

45. Figur 4 viser, hvordan et cyberangreb kan sprede sig mellem it-systemer i et netværk, der er segmenteret, og i et netværk, der ikke er. Segmenteringen kan foregå på forskellige niveauer og altså være mere eller mindre detaljeret. Man kan opdele netværket i grupper, men man kan også segmentere ned på hvert enkelt it-system. Den sidstnævnte model giver den bedste beskyttelse, men er også den dyreste.

Venstre side af figuren viser, hvordan et cyberangreb kan sprede sig inden for et netværk, der ikke er segmenteret. Højre side viser, hvordan segmenteringen opdeler netværket i mindre segmenter, som forhindrer cyberangrebet i at sprede sig. Højre side viser også, hvordan segmenteringen kan være mere eller mindre detaljeret.

Figur 4
Spredning af et cyberangreb



Kilde: Rigsrevisionen.

Segmentering af netværket

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Regionerne har oplyst, at det både er dyrt og tidskrævende at gennemføre en fuldstændig segmentering af deres netværk. Det skyldes bl.a., at det er teknisk vanskeligt at segmentere ældre it-systemer. Ældre it-systemer er designet i en tid, før segmentering blev almindelig praksis inden for arbejdet med cybersikkerhed. Det betyder, at man ofte mangler viden om, hvordan de ældre it-systemer er forbundet til resten af netværket. Igangsættelsen af segmenteringen indebærer derfor en risiko for, at man sætter it-systemer ud af drift.

Der er ikke tydelige krav til, hvordan og i hvilken grad regionerne skal segmentere deres netværk. Vi har vurderet, om regionerne har segmenteret de it-systemer med sundhedsdata, som regionerne selv vurderer er kritiske for hospitalsdriften.

46. Undersøgelsen viser, at ingen af regionerne har foretaget en tilstrækkelig segmentering af de it-systemer med sundhedsdata, som de selv vurderer er kritiske for hospitalsdriften. Region Hovedstaden har ikke segmenteret nogen af sine it-systemer med sundhedsdata.

4 af regionerne har oplyst, at de er gået i gang med en mere detaljeret segmentering af deres netværk. Region Hovedstaden har påbegyndt et mindre pilotprojekt vedrørende segmentering på ét af regionens hospitaler, inden segmenteringen rulles ud på andre hospitaler. Når Region Hovedstaden både mangler multifaktorlogin og segmentering af sine it-systemer med sundhedsdata, øger det risikoen for succesfulde cyberangreb.

Region Midtjylland har fremført, at man helt eller delvist kan nå samme sikkerhed ved hjælp af andre tiltag end segmentering, herunder intensiv overvågning. Rigsrevisionen er enig i, at cybersikkerheden kan styrkes på flere måder, og at der findes flere metoder til at begrænse spredningen af cyberangreb. Aktuelt er segmentering af netværk ifølge Center for Cybersikkerhed 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 kompenserer for manglende segmentering.

Sikkerhedsopdatering af pc'er, mobiltelefoner og tablets med adgang til sundhedsdata

47. For at efterleve ISO 27001 og anbefalingerne fra Center for Cybersikkerhed skal regionerne sørge for, at al software, herunder operativsystemer på pc'er, mobiltelefoner og tablets, er sikkerhedsopdateret. Vi har undersøgt, om regionerne har sikret, at operativsystemerne på pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede.

Sikkerhedsopdatering af pc'er m.m.

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

48. Undersøgelsen viser, at 2 af regionerne har sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede.

3 af regionerne har et større antal enheder, som ikke er sikkerhedsopdaterede. Det er enheder med adgang til sundhedsdata. Hvis operativsystemerne på fx regionernes pc'er med sundhedsdata ikke er sikkerhedsopdaterede, betyder det, at hackere kan udnytte disse sårbarheder til at sprede et succesfuldt cyberangreb inden for regionernes netværk.

Sikkerhedsopdatering af servere, der er kritiske for behandlingen af sundhedsdata

49. Regionerne skal sørge for, at deres servere er sikkerhedsopdaterede, for at efterleve ISO 27001 og anbefalingerne fra Center for Cybersikkerhed. Vi har undersøgt, om regionerne har sikret, at operativsystemerne på de servere, der er kritiske for behandlingen af sundhedsdata, er sikkerhedsopdaterede.

50. Undersøgelsen viser, at kun én af regionerne har sikret, at alle servere, der er kritiske for behandlingen af sundhedsdata, er sikkerhedsopdaterede. De øvrige regioner har et mindre antal servere, der ikke er sikkerhedsopdaterede. Resultaterne er ikke afrapporteret med angivelse af regionernes navne, da én af regionerne har rejst spørgsmål om fortrolighed. Se en uddybende beskrivelse i bilag 1.

2.3. Beredskab til at håndtere cyberangreb

3 typer af beredskabsplaner

Krisestyringsplan: Plan for myndighedernes krisestyring og kommunikation til eksterne parter.

Nødplan: Plan for, hvordan myndigheden viderefører de opgaver, som påvirkes, hvis der er et nedbrud på kritiske it-systemer.

Reetableringsplan: Plan for, hvordan et it-system skal reetableres efter et nedbrud.

51. Vi har undersøgt, om regionerne har et beredskab til at håndtere konsekvenserne af cyberangreb. De elektroniske patientjournaler er ifølge regionerne de it-systemer med sundhedsdata, som er mest kritiske for hospitalsdriften. Vi har undersøgt, om regionerne:

- har opdaterede beredskabsplaner for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan
- har taget backup af de elektroniske patientjournaler
- har gennemført regelmæssige restoretest af de elektroniske patientjournaler.

52. Undersøgelsen viser, at alle regionerne har et beredskab til at håndtere konsekvenserne af cyberangreb, men at dele af beredskabet er mangelfuldt i 3 af regionerne.

53. Tabel 4 viser resultatet af vores undersøgelse.

Tabel 4
Regionernes beredskab til at håndtere konsekvenserne af cyberangreb, der rammer de elektroniske patientjournaler

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen en opdateret beredskabsplan for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan?	●	●	●	●	●
Har regionen taget backup af de elektroniske patientjournaler?	●	●	●	●	●
Har regionen gennemført regelmæssige restoretest af de elektroniske patientjournaler?	●	●	●	●	●

● Ja ● Delvist ● Nej

Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rød t, hvis ingen af de nødvendige elementer er til stede.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Opdaterede beredskabsplaner for de elektroniske patientjournaler

54. Regionerne skal have et beredskab til at håndtere et cyberangreb, der sætter dele af hospitalsvæsenet ud af drift. Det følger af ISO 27001 og af anbefalingerne fra Center for Cybersikkerhed. Vi har derfor undersøgt, om regionerne har beredskabsplaner for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan. Vi har desuden undersøgt, om planerne er opdaterede, og om regionerne har testet dem regelmæssigt.

55. Undersøgelsen viser, at alle regionerne har beredskabsplaner til at håndtere cyberangreb, der rammer de elektroniske patientjournaler. Region Midtjylland og Region Syddanmark har dog ikke testet deres beredskabsplaner regelmæssigt. Når regionerne ikke tester deres beredskabsplaner, er der risiko for, at de ikke tager højde for de aktuelle cybertrusler. De 2 regioner mangler desuden planer for reetablering af de elektroniske patientjournaler. Det medfører en risiko for, at regionerne ikke kan genskabe de elektroniske patientjournaler inden for kort tid ved nedbrud.

Backup af de elektroniske patientjournaler

56. Regionerne skal som et led i deres efterlevelse af ISO 27001 løbende tage backup af kritiske data og it-systemer.

57. Undersøgelsen viser, at alle regionerne løbende har taget backup af de elektroniske patientjournaler.

Restoretest af de elektroniske patientjournaler

58. Regionerne skal gennemføre restoretest for at sikre, at de gemte backups kan bruges til at gendanne de elektroniske patientjournaler. Det følger af ISO 27001. En restoretest er en test af, om data og it-systemer kan gendannes ud fra en backup. Testene er vigtige, fordi de viser, om backuppen fungerer efter hensigten, og om den kan bruges i forbindelse med reetablering af de elektroniske patientjournaler. Hvis regionerne ikke tester, har de ikke sikkerhed for, at sundhedsdata kan genskabes i forbindelse med et cyberangreb.

59. Undersøgelsen viser, at 3 af regionerne har gennemført regelmæssige restoretest af de elektroniske patientjournaler, og at de har gennemgået resultaterne systematisk. Region Nordjylland har også gennemført regelmæssige restoretest, men har ikke sikret, at resultaterne bliver gennemgået systematisk. Region Syddanmark har ikke gennemført regelmæssige restoretest af de elektroniske patientjournaler.

Rigsrevisionen, den 9. januar 2025

Birgitte Hansen

/Signe Blaabjerg Christoffersen

Beredskabsplaner

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Backup

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Restoretest

Region	
Nordjylland	●
Midtjylland	●
Syddanmark	●
Sjælland	●
Hovedstaden	●

Bilag 1. Metodisk tilgang

I undersøgelsen indgår alle 5 regioner: Region Nordjylland, Region Midtjylland, Region Syddanmark, Region Sjælland og Region Hovedstaden.

Grundlaget for undersøgelsens vurderingskriterier

Undersøgelsens vurderingskriterier tager udgangspunkt i den internationale standard for informationssikkerhed ISO 27001. Regionerne har med aftalen "Fællesregional Informationssikkerhedspolitik" fra 2017 forpligtet sig til at efterleve ISO 27001.

Undersøgelsens vurderingskriterier tager også udgangspunkt i Center for Cybersikkerheds vejledninger "Cyberforsvar der virker" (4. udgave fra juli 2023) og "Passwordsikkerhed" (4. udgave fra oktober 2023). I "Cyberforsvar der virker" har Center for Cybersikkerhed udarbejdet en liste med 10 områder med tekniske tiltag, der bør være en prioritet i arbejdet med cybersikkerhed. Vi har valgt at fokusere på de vigtigste tiltag i forhold til beskyttelsen af netværket omkring sundhedsdata.

Vurderingskriterierne i undersøgelsen er derfor dækkende for 5 af de 10 områder i "Cyberforsvar der virker". Vi undersøger følgende områder:

- opdatering af operativsystemer
- segmentering af netværk
- brug af sikre passwords og multifaktorlogin
- backup og test af reetablering
- logning.

De 5 områder dækker over tiltag til at beskytte mod, at hackere opnår uautoriseret adgang til regionernes netværk (*ekstern sikring*), og tiltag til at begrænse skaden af et succesfuldt cyberangreb (*intern sikring*).

Vi undersøger ikke følgende områder:

- adgangsstyring
- antivirus, der beskytter klienter
- fjernadgang til it-systemer
- kryptering
- whitelisting.

Undersøgelsen er derfor ikke udtømmende i forhold til alle tiltag, der kan bruges til at forbedre cybersikkerheden i regionerne. Undersøgelsen giver derimod et indblik i regionernes arbejde med at beskytte deres netværk omkring sundhedsdata mod cyberangreb.

Vi undersøger desuden ikke adgangsstyring af brugerkonti, fordi det tidligere har været et centralt fokus i Rigsrevisionens *beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata* fra 2017.

Vi vurderer, at de 5 undersøgte områder er de væsentligste. Det vurderer vi på baggrund af den aktuelle sikkerhedssituation, undersøgelsens genstandsfelt (sundhedsdata i hospitalsvæsenet) og regionernes organisering af arbejdet med cybersikkerhed.

For nogle af undersøgelsens vurderingskriterier er ISO 27001 og Center for Cybersikkerheds vejledninger generelle eller forholder sig til cybersikkerhed på et mere overordnet niveau. For disse vurderingskriterier har det derfor været nødvendigt at konkretisere, hvad vi har lagt til grund for vores vurderinger. Det har gjort ved at bruge ISO 27002, som er en vejledning i den praktiske gennemførelse af ISO 27001. Vi har i visse tilfælde også fastsat vurderingskriterierne ud fra en konkret vurdering af, hvad der er god praksis på området.

Én af regionerne har rejst spørgsmål om fortrolighed i forhold til enkelte dele af undersøgelsen, men uden at konkretisere dette tilstrækkeligt til, at Rigsrevisionen kan anse oplysningerne for at være fortrolige efter forvaltningsloven. Rigsrevisionen vurderer derfor, at beretningen ikke indeholder fortrolige oplysninger. Rigsrevisionen har dog i et enkelt tilfælde ikke afrapporteret resultatet med angivelse af regionernes navne.

Møder og dokumentgennemgang

Undersøgelsen baserer sig på møder med regionernes it-afdelinger og en gennemgang af dokumenter, der vedrører cybersikkerheden i regionerne.

Møder

Vi har holdt en række møder med regionerne om deres beskyttelse af sundhedsdata mod cyberangreb. Formålet med møderne var at få en dybere forståelse af de forhold, som vi har undersøgt, og at opklare eventuelle spørgsmål til det materiale, som regionerne har udleveret. Regionerne blev desuden bedt om at demonstrere udvalgte tekniske tiltag i praksis på møderne, herunder implementeringen af sikre passwords, multifaktorlogin og ændringer i firewallregler.

Dokumentgennemgang

Vi har gennemgået en række dokumenter fra regionerne for at kunne besvare undersøgelsens spørgsmål. Tabel A viser, hvilke dokumenter vi har gennemgået under hvert enkelt vurderingskriterie i undersøgelsen.

Tabel A

Vurderingskriterier i forhold til regionernes beskyttelse af sundhedsdata mod cyberangreb

Vurderingskriterie	Ophæng til vurderingskriterie	Metode
Har regionen overblik over it-systemer med sundhedsdata?	• ISO 27001 og ISO 27002.	*Dokumenter, der er gennemgået:* • Fortegnelser over it-systemer med sundhedsdata. • Procesbeskrivelser for opdatering af fortegnelser over it-systemer med sundhedsdata.
Har regionen udført sårbarhedsskanninger og fulgt op på resultaterne på ledelsesniveau?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Resultater af sårbarhedsskanninger og penetrationstest de seneste 2 år. • Dokumenter, der beskriver opfølgningen på sårbarhedsskanninger.
Har regionen opdaterede og ledelsesgodkendte risikovurderinger og handleplaner?	• ISO 27001 og ISO 27002.	*Dokumenter, der er gennemgået:* • Risikovurderinger og dokumentation for, at vurderingerne er ledelsesgodkendt. • Handleplaner.
Har regionen politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • It-sikkerhedspolitikker og andre politikker, der vedrører sundhedsdata. • Rollebeskrivelser i forhold til adgangen til sundhedsdata.
Har regionen sikret, at netværksudstyret er sikkerhedsopdateret?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Oversigter over internetvendt netværksudstyr med angivelser af versioner af software. • Procesbeskrivelser for opdatering af software på internetvendt netværksudstyr. *Gennemgået i forbindelse med revisionsmødet:* • Stikprøver af dokumentation af opdateringer af netværksudstyr i form af screenshots fra sagsstyringssystemer.
Har regionen en hensigtsmæssig brug af firewalls?	• ISO 27001 og ISO 27002.	*Dokumenter, der er gennemgået:* • Oversigter over firewalls og firewallregler. • Procesbeskrivelser for oprettelse og nedlæggelse af firewallregler. *Gennemgået i forbindelse med revisionsmødet:* • Stikprøver af ændringer i firewallregler.
Bruger regionen sikre passwords på netværksudstyret?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Passwordsikkerhed" (2023).	*Dokumenter, der er gennemgået:* • Passwordpolitikker. • Lister med brugere, som har adgang til netværksudstyret. *Gennemgået i forbindelse med revisionsmødet:* • Stikprøver af implementeringen af passwordpolitikken for brugere, som har adgang til netværksudstyret.

Tabel A – fortsat

Vurderingskriterie	Ophæng til vurderingskriterie	Metode
Bruger regionen multifaktorlogin på netværksudstyret?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Passwordsikkerhed" (2023).	*Dokumenter, der er gennemgået:* • Politik for adgangsstyring, herunder multifaktorlogin. • Lister med brugere, som har adgang til netværksudstyret. *Gennemgået i forbindelse med revisionsmødet:* • Stikprøver af implementeringen af multifaktorlogin ved login på netværksudstyret.
Har regionen implementeret systematisk logning og overvågning af netværkstrafikken?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Retningslinjer for logning af netværkstrafikken. • Proces for håndtering af alarmer. *Gennemgået i forbindelse med revisionsmødet:* • Stikprøver af, hvilke alarmer der er opsat på baggrund af logningen.
Har regionen segmenteret netværket?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Beskrivelser af principper for segmentering. • Netværkstegninger, der viser segmenteringen.
Har regionen sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Oversigter over operativsystemerne på pc'er, mobiltelefoner og tablets med adgang til sundhedsdata. • Procesbeskrivelser for sikkerhedsopdatering af pc'er, mobiltelefoner og tablets.
Har regionen sikret, at servere, der er kritiske for behandlingen af sundhedsdata, er sikkerhedsopdaterede?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • Vurderingen af kriteriet er foretaget på baggrund af lister med servere fra hver region. Regionerne er blevet bedt om at sende en liste med servere, som regionen vurderer er kritiske i forhold til sundhedsdata. Der kan således være forskel på, hvor omfattende listerne er. • Procesbeskrivelser for sikkerhedsopdatering af servere.
Har regionen en opdateret beredskabsplan for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan?	• ISO 27001 og ISO 27002. • Center for Cybersikkerheds vejledning "Cyberforsvar der virker" (2023).	*Dokumenter, der er gennemgået:* • It-beredskabsplaner, herunder krisestyringsplaner, nødplaner og reetableringsplaner. • Rapporter eller tilsvarende, der viser test af it-beredskabsplanerne.

Tabel A – fortsat

Vurderingskriterie	Ophæng til vurderingskriterie	Metode
Har regionen taget backup af de elektroniske patientjournaler?	• ISO 27001 og ISO 27002.	*Dokumenter, der er gennemgået:* • Politikker for backup. • Krav og retningslinjer for backup af de elektroniske patientjournaler. *Gennemgået i forbindelse med revisionsmødet:* • Dokumentation for, at der er taget backup, bl.a. i form af screenshots.
Har regionen gennemført regelmæssige restoretest af de elektroniske patient-journaler?	• ISO 27001 og ISO 27002.	*Dokumenter, der er gennemgået:* • Procesbeskrivelser og krav til restoretest. • Dokumentation for gennemførte restore-test i 2023.

Kilde: Rigsrevisionen.

Tabel B viser resultaterne af Rigsrevisionens gennemgang af regionernes beskyttelse af sundhedsdata mod cyberangreb.

Tabel B

Rigsrevisionens gennemgang af regionernes beskyttelse af sundhedsdata mod cyberangreb

2.1. Har regionerne et tilstrækkeligt grundlag for at beskytte sundhedsdata mod cyberangreb?

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen overblik over it-systemer med sundhedsdata?	●	●	●	●	●
Har regionen udført sårbarhedsskanninger og fulgt op på resultaterne på ledelsesniveau?	●	●	●	●	●
Har regionen opdaterede og ledelsesgodkendte risikovurderinger og handleplaner?	●	●	●	●	●
Har regionen politikker og retningslinjer for beskyttelse af sundhedsdata mod cyberangreb?	●	●	●	●	●

2.2. Har regionerne iværksat tilstrækkelige tiltag til at beskytte sundhedsdata mod cyberangreb? (ekstern sikring)

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen sikret, at netværksudstyret er sikkerhedsopdateret?	●	●	●	●	●
Har regionen en hensigtsmæssig brug af firewalls?	●	●	●	●	●
Bruger regionen sikre passwords på netværksudstyret?	●	●	●	●	●
Bruger regionen multifaktorlogin på netværksudstyret?	●	●	●	●	●
Har regionen implementeret systematisk logning og overvågning af netværkstrafikken?	●	●	●	●	●

2.2. Har regionerne iværksat tilstrækkelige tiltag til at beskytte sundhedsdata mod cyberangreb? (intern sikring)

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen segmenteret netværket?	●	●	●	●	●
Har regionen sikret, at pc'er, mobiltelefoner og tablets med adgang til sundhedsdata er sikkerhedsopdaterede?	●	●	●	●	●

2.3. Har regionerne et beredskab til at håndtere konsekvenserne af cyberangreb, der rammer de elektroniske patientjournaler?

	Region Nordjylland	Region Midtjylland	Region Syddanmark	Region Sjælland	Region Hovedstaden
Har regionen en opdateret beredskabsplan for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan?	●	●	●	●	●
Har regionen taget backup af de elektroniske patientjournaler?	●	●	●	●	●
Har regionen gennemført regelmæssige restoretest af de elektroniske patientjournaler?	●	●	●	●	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Kvalitetssikring

Undersøgelsen er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos de reviderede samt ledelsesbehandling og sparring med chefer og medarbejdere i Rigsrevisionen.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision, herunder standarderne for større undersøgelser (SOR 3). Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).