FOLKETINGET
RIGSREVISIONEN

Februar 2021

Rigsrevisionens notat om
beretning om

3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata

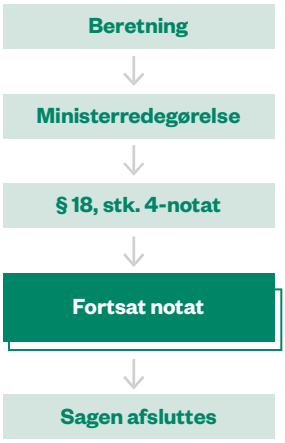
Opfølgning i sagen om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata (beretning nr. 4/2017)

21. januar 2021

RN 1401/21

1. Rigsrevisionen følger i dette notat op på sagen om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata, som blev indledt med en beretning i 2017. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 4. april 2018.

Sagsforløb for en større undersøgelse



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

Konklusion

Region Syddanmark, Region Midtjylland og Region Hovedstaden har siden Rigsrevisionens beretning fra 2017 arbejdet med initiativer til at sikre beskyttelse af adgangen til it-systemer og sundhedsdata. Alle 3 regioner har siden 2017 forbedret beskyttelsen af adgangen til it-systemer og sundhedsdata markant og opfylder i 2020 19 ud af de 20 tiltag, som indgik i beretningen, mod mellem 7 og 10 ud af 20 i 2017. Hver region mangler således kun at opfylde ét tiltag, og for alle 3 regioner er det udestående tiltag delvist opfyldt. Regionerne har desuden implementeret kompenserende foranstaltninger, der reducerer risikoen ved de delvist opfyldte tiltag. Alle 3 regioner har oplyst, at de er ved at rette op på de udestående tiltag og forventer at opfylde tiltagene i løbet af 2021.

Rigsrevisionen finder det tilfredsstillende, at regionerne har rettet op på hovedparten af de udestående tiltag siden 2017.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- de 3 regioners arbejde med at nå i mål med hver deres sidste udestående tiltag.

I. Baggrund

2. Rigsrevisionen afgav i november 2017 en beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata. Beretningen handlede om, hvad 3 regioner – Region Syddanmark, Region Midtjylland og Region Hovedstaden – gør for at beskytte adgangen til it-systemer, der indeholder sundhedsdata om borgerne. Regionerne har ansvaret for at beskytte sundhedsdata, der indeholder følsomme persondata om borgernes helbred. Regionerne skal sikre, at disse data er fortrolige, men også, at de er tilgængelige og pålidelige, så patienter kan få den rette behandling til den rette tid.

3. Da Statsrevisorerne behandlede beretningen, bemærkede de, at de 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata ikke var tilfredsstillende. Hermed er der risiko for, at følsomme og fortrolige persondata kommer i hænderne på uvedkommende eller ikke er pålidelige og tilgængelige, når der er brug for dem.

Af Statsrevisorernes bemærkning til Endelig betænkning af 26. april 2018 fremgår det, at Statsrevisorerne med tilfredshed konstaterede, at Region Syddanmark, Region Midtjylland og Region Hovedstaden havde iværksat en række tiltag, der skal beskytte adgangen til it-systemer og sundhedsdata, men at der fortsat udestod enkelte tiltag. Henset til områdets væsentlighed og risiko anmodede Statsrevisorerne Rigsrevisionen om at følge op på, at de udestående initiativer i de 3 regioner blev implementeret.

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkt:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. De 3 regioners implementering af de tiltag, hvor Rigsrevisionen påpegede mangler.	Behandles i dette notat.

5. Vi redegør i dette notat for resultaterne af opfølgningen på ovenstående punkt.

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

II. Regionernes initiativer

6. Vi gennemgår i det følgende de 3 regioners initiativer i forhold til de mangler, som Rigsrevisionen påpegede i beretningen fra 2017. Gennemgangen er baseret på revisionsbesøg hos Region Syddanmark, Region Midtjylland og Region Hovedstaden og på skriftlig dokumentation fra de 3 regioner.

Regionernes implementering af de tiltag, hvor Rigsrevisionen påpegede mangler

7. Det fremgik af beretningen, at beskyttelsen af adgangen til it-systemer og sundhedsdata ikke var tilfredsstillende i de 3 regioner. De 3 regioner havde en utilstrækkelig implementering af flere tiltag under følgende temaer: politik for it-sikkerhed på udvalgte områder, grundlæggende sikringstiltag mod hackerangreb, styring og kontrol af medarbejdere med privilegerede rettigheder, styring og kontrol af system- og servicekonti med privilegerede rettigheder og logning af konto med privilegerede rettigheder.

Politik, retningslinjer og procedurer for it-sikkerhed på udvalgte områder

8. Tabel 1 viser resultaterne af Rigsrevisionens opfølgning på, om regionerne har politikker, retningslinjer og procedurer for it-sikkerhed på udvalgte områder, og om regionernes politikker, retningslinjer og procedurer er forbedret siden 2017. I beretningen vurderede Rigsrevisionen, at tilstrækkelige politikker for it-sikkerhed som minimum bør omfatte de 4 nævnte tiltag i tabel 1.

Tabel 1

De 3 regioners politikker, retningslinjer og procedurer for it-sikkerhed på udvalgte områder i 2020 sammenlignet med 2017

	Region Syddanmark		Region Midtjylland		Region Hovedstaden	
	2017	2020	2017	2020	2017	2020
Regionen har udarbejdet en politik, retningslinjer og procedurer for grundlæggende sikringstiltag mod hackerangreb	●	●	●	-	●	-
Regionen har udarbejdet en politik, retningslinjer og procedurer for tildeling af privilegerede rettigheder til medarbejdere	●	●	●	-	●	-
Regionen har udarbejdet en politik, retningslinjer og procedurer for system- og servicekonti med privilegerede rettigheder	●	●	●	●	●	-
Regionen har udarbejdet en politik, retningslinjer og procedurer for logning af konti med privilegerede rettigheder	●	●	●	-	●	-

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da regionen allerede opfyldte tiltaget i 2017.

Kilde: Rigsrevisionens beretning fra 2017 og Rigsrevisionens opfølgning fra 2020.

Det fremgik af beretningen fra 2017, at Region Hovedstaden opfyldte alle 4 tiltag. Desuden fremgik det, at Region Syddanmark ikke havde udarbejdet politikker for it-sikkerhed på de udvalgte områder. Endelig fremgik det, at Region Midtjylland havde udarbejdet politikker, retningslinjer og procedurer på næsten alle områder, men kun i nogen grad havde udarbejdet en politik, retningslinjer og procedurer for system- og servicekonti med privilegerede rettigheder.

Vores opfølgning viser, at de 3 regioner i 2020 alle har udarbejdet politikker, retningslinjer og procedurer for it-sikkerhed på de udvalgte områder.

9. Rigsrevisionen finder det tilfredsstillende, at de 2 regioner nu opfylder alle tiltag. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Grundlæggende sikringstiltag mod hackerangreb

10. Statsrevisorerne bemærkede, at de grundlæggende sikringstiltag mod hackerangreb ikke i tilstrækkelig grad var implementeret i nogen af de 3 regioner. Statsrevisorerne fandt det særligt kritisk, at 27.000 medarbejdere i Region Syddanmark havde lokaladministratorrettigheder, da det øger risikoen for hackermisbrug.

11. Tabel 2 viser resultaterne af Rigsrevisionens opfølgning på, om regionerne har implementeret grundlæggende sikringstiltag mod hackerangreb, og om sikringstiltagene er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at tilstrækkelige grundlæggende sikringstiltag mod hackerangreb som minimum bør omfatte de 6 nævnte tiltag i tabel 2.

Tabel 2
De 3 regioners grundlæggende sikringstiltag mod hackerangreb i 2020 sammenlignet med 2017

	Region Syddanmark		Region Midtjylland		Region Hovedstaden	
	2017	2020	2017	2020	2017	2020
Regionen har begrænset download af programmer	🟡	🟢	🟡	🟢	🟡	🟢
Regionen har sikret, at kun godkendte programmer kan afvikles	🟡	🟢	🟢	-	🟡	🟢
Regionen har sikret, at regionen kan hente sikkerhedsopdateringer fra producenterne af relevante produkter	🟢	-	🟡	🟢	🟡	🟢
Regionen har løbende gennemført sikkerhedsopdateringer af relevante produkter, der kan opdateres	🟢	-	🟢	-	🟢	-
Regionen har sikret, at ingen medarbejdere har lokaladministratorrettigheder	🔴	🟢	🟢	-	🟢	-
Regionen har etableret tiltag, fx segmenteret netværket, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset	🟡	🟢	🟡	🟢	🟡	🟢

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da regionen allerede opfyldte tiltaget i 2017.

Kilde: Rigsrevisionens beretning fra 2017 og Rigsrevisionens opfølgning fra 2020.

Det fremgik af beretningen fra 2017, at alle 3 regioner manglede at opfylde mellem 3 og 4 grundlæggende sikringstiltag mod hackerangreb. Derudover fremgik det, at alle 3 regioner havde gennemført løbende sikkerhedsopdateringer af relevante produkter, der kan opdateres.

Vores opfølgning viser, at de 3 regioner alle har implementeret grundlæggende sikringstiltag mod hackerangreb i 2020. Revisionen har i den forbindelse vist, at Region Syddanmark er gået fra, at alle brugere (27.000) havde lokaladministratorrettigheder som standard, til, at ingen brugere nu har lokaladministratorrettigheder som standard.

12. Rigsrevisionen finder det tilfredsstillende, at de 3 regioner nu opfylder alle tiltag for grundlæggende sikringstiltag mod hackerangreb. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Styring og kontrol af medarbejdere med privilegerede rettigheder
13. Statsrevisorerne bemærkede, at styring og kontrol af medarbejdere med privilegerede rettigheder var mangelfuld i alle 3 regioner, herunder at der var utilstrækkelig begrænsning af muligheder for at tilgå internettet, når der logges på med privilegerede rettigheder.

14. Tabel 3 viser resultaterne af Rigsrevisionens opfølgning på de 3 regioners styring og kontrol af medarbejdere med privilegerede rettigheder, og om styringen og kontrollen er forbedret siden 2017. Rigsrevisionen vurderede i beretningen, at tilstrækkelig styring og kontrol af medarbejdere med privilegerede rettigheder som minimum bør omfatte de 5 nævnte tiltag i tabel 3.

Tabel 3

De 3 regioners styring og kontrol af medarbejdere med privilegerede rettigheder i 2020 sammenlignet med 2017

	Region Syddanmark		Region Midtjylland		Region Hovedstaden	
	2017	2020	2017	2020	2017	2020
Regionen har et begrænset antal medarbejdere, der permanent har privilegerede rettigheder	●	●	●	-	●	●
Regionen har sikret, at alle medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto	●	-	●	-	●	-
Regionen har implementeret en regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder	●	●	●	●	●	●
Regionen har sikret, at personlige passwords til konti med privilegerede rettigheder følger god praksis og er systemunderstøttede	●	-	●	●	●	●
Regionen har sikret, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder	●	●	●	●	●	●

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da regionen allerede opfyldte tiltaget i 2017.

Kilde: Rigsrevisionens beretning fra 2017 og Rigsrevisionens opfølgning fra 2020.

Det fremgik af beretningen i 2017, at de 3 regioner manglede at opfylde mellem 3 og 4 tiltag. Derudover fremgik det, at alle 3 regioner havde sikret, at alle medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto.

Vores opfølgning viser, at Region Midtjylland i 2020 opfylder alle 5 tiltag med hensyn til styring og kontrol af medarbejdere med privilegerede rettigheder. Derudover viser vores opfølgning, at Region Syddanmark og Region Hovedstaden hver mangler at opfylde ét tiltag.

Region Syddanmark har ikke sikret, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder. Regionen har dog en ledelsesgodkendt risikovurdering heraf. Desuden har regionen kompenserende foranstaltninger, der delvist reducerer risikoen. Region Syddanmark har oplyst, at regionen arbejder på et projekt, der skal begrænse adgangen til internettet for brugere med privilegerede rettigheder. Regionen forventede, at projektet ville være gennemført ultimo 2020, men projektet er blevet forsinket som følge af Corona-situationen og forventes i stedet gennemført i 1. kvartal 2021.

Region Hovedstaden har implementeret en kontrol af medarbejdere med privilegerede adgangsrettigheder, men kontrollen omfatter ikke alle domæner, og regionen har ikke dokumenteret det konkrete arbejdsbetingede behov for hver af de enkelte medarbejdere med privilegerede rettigheder. De domæner, der ikke er omfattet, er under afvikling, og desuden har regionen implementeret kompenserende foranstaltninger, der reducerer risikoen. Region Hovedstaden har oplyst, at regionen vil påbegynde afviklingen af domænerne primo 2021. Det er ikke muligt at give en fast tidshorisont for, hvornår domænerne er afviklet, men at dette vil ske i et tempo, der er driftsmæssigt forsvarligt.

Domæner

Domæner er grupper af enheder (netværksenheder, computere og brugere), der styres af et fælles brugeradministrationssystem (AD), hvori regionen styrer og kontrollerer adgange og rettigheder til it-systemer og data.

15. Rigsrevisionen finder det tilfredsstillende, at Region Midtjylland opfylder alle tiltagene. Derudover finder Rigsrevisionen det tilfredsstillende, at Region Syddanmark og Region Hovedstaden opfylder 4 ud af 5 tiltag og arbejder på at implementere de resterende tiltag. Rigsrevisionen vil fortsat følge Region Syddanmarks og Region Hovedstadens arbejde med at implementere hver deres resterende tiltag.

Styring og kontrol af system- og servicekonti med privilegerede rettigheder
16. Statsrevisorerne bemærkede, at Region Syddanmark og Region Hovedstaden havde passwords til system- og servicekonti, der ikke havde været skiftet i lang tid – op til 9 år – og passwords, der ikke levede op til god praksis.

17. Tabel 4 viser resultaterne af Rigsrevisionens opfølgning på Region Syddanmarks og Region Hovedstadens styring og kontrol af system- og servicekonti med privilegerede rettigheder, og om styringen og kontrollen er forbedret siden 2017. I beretningen vurderede Rigsrevisionen, at tilstrækkelig styring og kontrol af system- og servicekonti med privilegerede rettigheder som minimum bør omfatte de 2 nævnte tiltag i tabel 4.

Tabel 4
De 3 regioners styring og kontrol af system- og servicekonti med privilegerede rettigheder

	Region Syddanmark		Region Midtjylland		Region Hovedstaden	
	2017	2020	2017	2020	2017	2020
Regionen har et begrænset antal system- og servicekonti med privilegerede rettigheder	●	-	●	-	●	●
Regionen har sikret, at passwords til system- og servicekonti med privilegerede rettigheder følger god praksis og er systemunderstøttede	●	●	●	-	●	●

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da regionen allerede opfyldte tiltaget i 2017.

Kilde: Rigsrevisionens beretning fra 2017 og Rigsrevisionens opfølgning fra 2020.

Det fremgik af beretningen fra 2017, at Region Syddanmark ikke havde sikret, at passwords til system- og servicekonti med privilegerede rettigheder fulgte god praksis og var systemunderstøttede. Derudover fremgik det, at Region Midtjylland opfyldte begge tiltag, og at Region Hovedstaden manglede at opfylde begge tiltag.

Vores opfølgning viser, at både Region Syddanmark og Region Hovedstaden har opfyldt tiltagene om styring og kontrol af system- og servicekonti med privilegerede rettigheder i 2020. Revisionen viser, at passwords i Region Syddanmark og Region Hovedstaden nu følger god praksis, herunder at de er systemunderstøttede og er skiftet for nyligt.

18. Rigsrevisionen finder det tilfredsstillende, at de 2 regioner nu alle opfylder begge tiltag. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Logning af konti med privilegerede rettigheder
19. Statsrevisorerne bemærkede, at alle 3 regioners logningstiltag var mangelfulde, hvilket gør det vanskeligt at opdage og opklare hackerangreb og misbrug af rettigheder. Statsrevisorerne bemærkede derudover, at Region Midtjylland ikke havde implementeret nogen af de undersøgte logningstiltag, til trods for at regionen havde udarbejdet en politik for området.

20. Tabel 5 viser resultaterne af Rigsrevisionens opfølgning på de 3 regioners logning af konti med privilegerede rettigheder, og om logningen er forbedret siden 2017. I beretningen vurderede Rigsrevisionen, at tilstrækkelig logning af konti med privilegerede rettigheder som minimum bør omfatte de 3 nævnte tiltag i tabel 5.

Tabel 5
De 3 regioners logning af konti med privilegerede rettigheder

	Region Syddanmark		Region Midtjylland		Region Hovedstaden	
	2017	2020	2017	2020	2017	2020
Regionen har sikret, at konti med privilegerede rettigheder logges, når de starter programmer, så sporbarheden sikres	●	●	●	●	●	●
Regionen har sikret, at logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet	●	-	●	●	●	●
Regionen har sikret, at medarbejder med privilegerede rettigheder, der logges, ikke har adgang til loggen	●	-	●	●	●	●

Note: Farverne angiver, om tiltaget er opfyldt (grøn), delvist opfyldt (gul) eller ikke opfyldt (rød). "-" angiver, at der ikke er foretaget revision i 2020, da regionen allerede opfyldte tiltaget i 2017.

Kilde: Rigsrevisionens beretning fra 2017 og Rigsrevisionens opfølgning fra 2020.

Det fremgik af beretningen fra 2017, at Region Syddanmark ikke havde sikret, at konti med privilegerede rettigheder blev logget, når de startede programmer, så sporbarheden blev sikret. Derudover fremgik det af beretningen, at Region Midtjylland og Region Hovedstaden ikke opfyldte nogen af tiltagene i tilstrækkelig grad.

Vores opfølgning viser, at Region Syddanmark og Region Hovedstaden i 2020 begge har sikret en tilstrækkelig logning af konto med privilegerede rettigheder. Region Midtjylland lever op til 2 ud af 3 tiltag.

Region Midtjylland har delvist sikret, at logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet. Regionen foretager en løbende – men ikke systematisk – gennemgang af logfiler og anvender ikke alarmer. Region Midtjylland har oplyst, at regionen er ved at implementere en løsning, der inden for et år forventes at rette op herpå. Regionen vil i den forbindelse løbende implementere systematisk indsamling og gennemgang af logfiler, alarmer og kontroller og udvide brugen af loganalyserne.

21. Rigsrevisionen finder det tilfredsstillende, at Region Syddanmark og Region Hovedstaden opfylder alle 3 tiltag, og at Region Midtjylland opfylder 2 tiltag og arbejder på at opfylde det tredje tiltag. Rigsrevisionen vil fortsat følge Region Midtjyllands arbejde med at implementere det resterende tiltag.

Lone Strøm