FOLKETINGET
RIGSREVISIONEN

December 2023

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)

14. november 2023

RN 1412/23

I. Baggrund og konklusion

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. Opfølgningen sker med henblik på at vurdere, om Region Syddanmarks, Region Midtjyllands og Region Hovedstadens initiativer adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning. Vi har tidligere behandlet sagen i notater til Statsrevisorerne af 4. april 2018 og 21. januar 2021.

2. Beretningen handlede om, hvad 3 regioner – Region Syddanmark, Region Midtjylland og Region Hovedstaden – gør for at beskytte adgangen til it-systemer, der bl.a. 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, fandt de, at de 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata ikke var tilfredsstillende.

4. Ved opfølgningen i 2021 fandt Rigsrevisionen, at de 3 regioner på forskellige områder fortsat havde mangler vedrørende beskyttelse af adgangen til deres it-systemer og sundhedsdata.

Konklusion

Rigsrevisionen finder det tilfredsstillende, at de 3 regioner er nået i mål med hver deres udestående tiltag fra beretningen vedrørende beskyttelse af adgangen til it-systemer og sundhedsdata.

Region Syddanmark har sikret, at medarbejdere med privilegerede adgangsrettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder. Region Midtjylland har implementeret alarmer, der vedrører anvendelsen af Domain Admin-konti, med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet. Region Hovedstaden har implementeret en regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder.

Rigsrevisionen vurderer på den baggrund, at sagen kan afsluttes.

Sagsforløb for en større undersøgelse

- Beretning
- Ministerredegørelse
- § 18, stk. 4-notat
- **Fortsat notat**
- Sagen afsluttes

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

Domain Admin-konti
It-medarbejderkonti, der er medlem af "Domain Admins-gruppen" i brugeradministrationssystemet Active Directory. Disse konti har det højeste niveau af rettigheder, adgang og kontrol over institutionens it-systemer og data.

II. Status på sagen

5. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

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.	19 af i alt 20 tiltag for hver region blev afsluttet i forbindelse med notat til Statsrevisorerne af 21. januar 2021.
2. De 3 regioners arbejde med at nå i mål med hver deres sidste udestående tiltag.	Det sidste tiltag for hver region behandles og afsluttes i dette notat.

III. De 3 regioners initiativer

6. Vi gennemgår i det følgende Region Syddanmarks, Region Midtjyllands og Region Hovedstadens initiativer i forhold til det udestående opfølgningspunkt.

7. Opfølgningen er baseret på virtuelle revisionsbesøg hos de 3 regioner i april-juni 2022 og april 2023. Derudover har vi gennemgået redegørelser og anden skriftlig dokumentation af regionernes tiltag, herunder udtræk af it-systemer og skærmdumps.

Region Syddanmarks styring af internetadgang for medarbejdere med privilegerede adgangsrettigheder

Region Syddanmark har sikret, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder. Regionen har desuden indført yderligere tiltag, der begrænser risiciene ved medarbejderkonti med privilegerede rettigheder. Dette finder Rigsrevisionen tilfredsstillende og vurderer derfor, at denne del af sagen kan afsluttes.

8. Statsrevisorerne bemærkede bl.a., at der var utilstrækkelig begrænsning af muligheder for at tilgå internettet, når der blev logget på med privilegerede rettigheder.

9. Rigsrevisionen vurderede i forbindelse med notatet af 21. januar 2021, at Region Syddanmark kun delvist havde adresseret denne mangel.

10. Vores opfølgning viser, at Region Syddanmark i 2022 har sikret, at medarbejdere med privilegerede brugerrettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder og er medlemmer af en særlig sikkerhedsgruppe. Hvis medarbejderne melder sig ud af sikkerhedsgruppen, kan de tilgå internettet, men ved udmeldelse sendes automatiske adviseringsmails om ændringen til alle i sikkerhedsgruppen. Desuden logger regionen ændringer i sikkerhedsgruppen, herunder ind- og udmeldelser. Regionen har i juni 2022 også implementeret, at der 2 gange i løbet af døgnet foretages en automatisk genindmelding i sikkerhedsgruppen af alle medarbejdere med privilegerede brugerrettigheder, der har meldt sig ud. Herudover aktiveres en alarm, hvis processen fejler. Som en ekstra sikkerhedsforanstaltning fører regionen halvårlig kontrol med, hvem der er medlem af sikkerhedsgruppen.

Region Midtjyllands arbejde med at identificere sikkerhedshændelser eller misbrug af privilegerede brugerrettigheder

Region Midtjylland har implementeret alarmer, der vedrører anvendelsen af Domain Admin-konti, og som har til hensigt at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet. Dette finder Rigsrevisionen tilfredsstillende og vurderer derfor, at denne del af sagen kan afsluttes.

11. Statsrevisorerne bemærkede, at Region Midtjylland ikke havde implementeret nogen af de undersøgte logningstiltag, selv om regionen havde udarbejdet en politik for området.

12. Rigsrevisionen vurderede i forbindelse med notatet af 21. januar 2021, at Region Midtjylland kun delvist havde implementeret tiltag, som adresserede de påpegede mangler. Regionen foretog løbende – men ikke systematisk – gennemgange af logfiler. Regionen anvendte heller ikke alarmer med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet.

13. Vores opfølgning viser, at Region Midtjylland ikke gennemgår logfiler regelmæssigt, men at regionen i stedet har implementeret alarmer, der vedrører anvendelsen af Domain Admin-konti, i regionens SIEM-løsning. Alarmerne aktiveres ved specifikke handlinger og har til hensigt at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet. Regionen anser alarmer som en mere effektiv og systematisk overvågning end gennemgang af logfiler. Hvis alarmerne bliver udløst, underrettes regionens 24/7-funktionspostkasse, og alarmerne visiteres og håndteres efter den pågældende instruks.

SIEM-løsning
SIEM (Security Information and Event Management) er en løsning, der leverer overvågning, sporing og alarmering af sikkerhedshændelser eller hændelser inden for et it-miljø.

14. Region Midtjylland oplyser, at regionen – ud over implementeringen af alarmer – har reduceret antallet af Domain Admin-konti til et minimum. Rigsrevisionen er enig i, at et lavt antal Domain Admin-konti reducerer risikoen for uautoriseret anvendelse, herunder uautoriserede ændringer og uhensigtsmæssigheder i it-miljøet.

15. Rigsrevisionen bemærker, at Region Midtjylland løbende bør foretage en risikobaseret vurdering af, om regionen har de fornødne og rigtige alarmer, herunder for Domain Admin-konti, for at sikre, at regionen opdager uautoriserede ændringer eller uhensigtsmæssigheder. Regionen oplyser, at regionen løbende vil vurdere, om der skal etableres yderligere overvågning af de relevante typer konti. Desuden oplyser regionen, at regionen snarest muligt vil implementere yderligere 2 alarmer for Domain Admin-konti.

Region Hovedstadens kontrol af medarbejdere med privilegerede adgangsrettigheder

Region Hovedstaden har implementeret en månedlig kontrol af medarbejdere med privilegerede adgangsrettigheder. Samtidig har regionen månedligt dokumenteret en ledelsesgodkendt vurdering af det konkrete arbejdsbetingede behov for privilegerede adgangsrettigheder. Regionen har også afviklet 3 legacy-domæner, som tidligere ikke var omfattet af regionens kontrol af privilegerede adgangsrettigheder. Dette finder Rigsrevisionen tilfredsstillende og vurderer derfor, at denne del af sagen kan afsluttes.

Legacy-domæne
Et legacy-domæne er et ældre domæne, som generelt ikke bliver udviklet eller opdateret. Legacy-domæner kan udgøre en sikkerhedsrisiko, fx på grund af forældede sikkerhedsforanstaltninger eller kendte sårbarheder.

16. Statsrevisorerne bemærkede bl.a., at styring og kontrol af medarbejdere med privilegerede rettigheder var mangelfuld i alle 3 regioner.

17. Rigsrevisionen vurderede i forbindelse med notatet af 21. januar 2021, at Region Hovedstaden kun delvist havde adresseret manglerne vedrørende kontrol af medarbejdere med privilegerede brugerrettigheder.

18. Vores opfølgning viser, at Region Hovedstaden fra april 2022 har udarbejdet månedlige ledelsesgodkendte kontroller af brugerrettigheder. Opfølgningen viser også, at regionen fra maj 2022 har foretaget en dokumenteret og ledelsesgodkendt vurdering af det konkrete arbejdsbetingede behov for privilegerede adgangsrettigheder, herunder om det er nødvendigt med permanente eller midlertidige privilegerede rettigheder. Opfølgningen viser desuden, at regionen har afviklet de 3 legacy-domæner, som tidligere ikke var omfattet af regionens kontrol af privilegerede rettigheder.

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

Birgitte Hansen