RIGSREVISIONEN

Notat til Statsrevisorerne om beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver

Februar 2016

Vedrører:
Statsrevisorernes beretning nr. 1/2015 om adgangen til it-systemer, der understøtter samfundsvigtige opgaver

11. februar 2016

RN 1501/16

Finansministerens redegørelse af 8. december 2015
Energi-, forsynings- og klimaministerens redegørelse af 7. januar 2016
Justitsministerens redegørelse af 14. januar 2016
Transport- og bygningsministerens redegørelse af 15. januar 2016
Sundheds- og ældreministerens redegørelse af 18. januar 2016

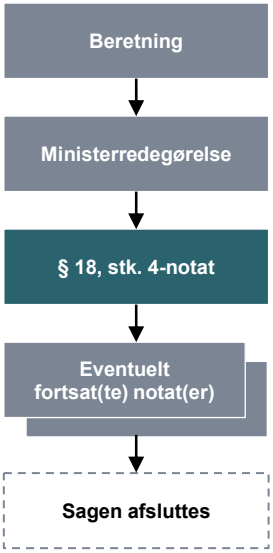
1. Rigsrevisionen vurderer i dette notat de initiativer, som ministrene har iværksat og vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner.

KONKLUSION

Ministrene har alle oplyst, at institutionerne vil rette op på de konstaterede mangler i forhold til styring, kontrol og logning af de udvidede administratorrettigheder. De har således planlagt, igangsat og/eller gennemført en række initiativer. Rigsrevisionen finder det tilfredsstillende, at institutionerne vil rette op på de konstaterede mangler, og vurderer derfor, at beretningssagen kan afsluttes.

Rigsrevisionen vil dog som led i it-revisionen fortsat følge, at initiativerne bliver gennemført og fungerer i praksis samt følge op på beretningens anbefalinger. Hvis Rigsrevisionen ikke finder initiativerne tilstrækkelige, vil Rigsrevisionen orientere Statsrevisorerne herom i beretning om revisionen af statsregnskabet.

Sagsforløb for en større undersøgelse



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

I. Baggrund

2. Rigsrevisionen afgav i oktober 2015 en beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver. Beretningen handlede om, hvad 6 udvalgte statslige institutioner gør for at beskytte adgangen til it-systemer og data, som understøtter samfundsvigtige opgaver, via de såkaldte udvidede administratorrettigheder.

Beretningen omhandlede følgende 6 institutioner: Energinet.dk (under Energi-, Forsynings- og Klimaministeriet), Banedanmark (under Transport- og Bygningsministeriet), National Sundheds-it (under Sundheds- og Ældreministeriet), der varetager it-drift for Sundheds- og Ældreministeriet, Statens It (under Finansministeriet), der varetager it-drift for en række ministerområder, og Direktoratet for Kriminalforsorgen og Rigspolitiets Koncern IT (under Justitsministeriet).

Formålet med undersøgelsen var at vurdere, om de statslige institutioner følger anbefalingerne om god it-sikkerhedspraksis for at beskytte adgangen til it-systemer og data, som understøtter samfundsvigtige opgaver. Rigsrevisionen undersøgte derfor ud fra 16 revisionskriterier, hvordan institutionerne styrer og kontrollerer de udvidede administratorrettigheder, herunder hvordan institutionerne sikrer logning af anvendelsen af udvidede administratorrettigheder.

It-systemer, der understøtter samfundsvigtige opgaver, kan – ligesom andre it-systemer – tilgås med udvidede administratorrettigheder. Disse rettigheder giver det højeste niveau af rettigheder, adgang og kontrol over institutionernes it-systemer og data, som styres i brugeradministrationssystemet Active Directory (AD). Desuden kan rettighederne give mulighed for at omgå institutionernes sikkerhedsforanstaltninger. I nogle tilfælde kan de udvidede administratorrettigheder – afhængigt af institutionens systemopbygning – også give adgang til andre væsentlige it-systemer og data, der ikke styres i AD.

3. Da Statsrevisorerne behandlede beretningen, fandt de det kritisabelt og foruroligende, at en række samfundsvigtige opgaver er udsat for alvorlige it-sikkerhedsmæssige risici, der kan true opgavernes løsning og kompromittere fortrolige data.

Statsrevisorerne fandt det tilfredsstillende, at institutionerne har oplyst, at de har gennemført kompenserende foranstaltninger og er i færd med at planlægge, igangsætte og gennemføre tiltag, der skal rette op på de konstaterede mangler.

4. Det fremgik af beretningen, at der på undersøgelsestidspunktet var en række mangler i alle 6 institutioner i styringen, kontrollen og logningen af de udvidede administratorrettigheder.

5. Det bemærkes, at Rigsrevisionen undtagelsesvist besluttede at anonymisere resultaterne i beretningen ud fra et it-sikkerhedshensyn, da revisionen påviste en række alvorlige mangler, der udgør en it-sikkerhedsrisiko, indtil institutionerne har rettet op på manglerne.

Ministerredegørelserne er som vanligt offentligt tilgængelige og er ikke anonymiserede.

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

II. Gennemgang af ministrenes redegørelser

Styring, kontrol og logning af udvidede administratorrettigheder

7. Statsrevisorerne fremhævede, at ingen af de 6 undersøgte institutioner har håndteret de udvidede administratorrettigheder med den nødvendige professionalisme. Institutionerne har derfor ikke efterlevet en række anerkendte anbefalinger om god it-sikkerhedspraksis til beskyttelse af adgangen til it-systemer og data.

8. Rigsrevisionen fandt, at institutionerne bør forbedre deres styring, kontrol og logning af de udvidede administratorrettigheder for at modvirke misbrug og kompromittering af it-systemer og data, der styres i AD. Rigsrevisionen fandt desuden, at institutionerne jævnligt bør tage aktivt stilling til tilstrækkeligheden af deres styring, kontrol og logning af de udvidede administratorrettigheder. Endelig var det Rigsrevisionens vurdering, at der er behov for ledelsesmæssig fokus og prioritering for at rette op på de konstaterede forhold.

9. Justitsministeren oplyser, at han ser med stor alvor på Rigsrevisionens konklusioner. Ministeren oplyser videre, at Justitsministeriet i samarbejde med PET og de 2 undersøgte institutioner på ministerområdet (Rigspolitiet og Kriminalforsorgen) har iværksat tiltag for at rette op på kritikpunkterne i beretningen. Ministeriet har desuden iværksat et skærpet tilsyn med it-sikkerheden, og ministeriet og PET følger implementeringen af tiltagene tæt. Ministeren oplyser desuden, at ministeriet igennem de seneste år har arbejdet på at etablere en systematisk og professionel tilgang med arbejdet med it-sikkerhed, som er forankret hos ledelsen i de enkelte institutioner. Endelig oplyser ministeren, at ministeriet har etableret et samarbejde på tværs af ministerområdet om implementering af ISO 27001 og opstillet styringsmål for implementeringen i mål- og resultatplaner på ministerområdet for 2015 og 2016.

10. Finansministeren erklærer sig enig i, at håndtering af de udvidede administratorrettigheder er en vigtig forudsætning for at beskytte mod uretmæssig adgang til statslige institutioners it-systemer og data.

Ministeren oplyser, at Statens It siden revisionsbesøget i marts har rettet op på de 16 punkter, som beretningen omhandler. Statens It har desuden implementeret en række processer, der skal medvirke til at forbedre styringen af udvidede administratorrettigheder, herunder bl.a. i forhold til skærpede krav til passwords for system- og servicekonti, samt opdage unormalt trafikmønster i it-miljøet.

11. Energi-, forsynings- og klimaministeren finder, at konklusionerne i beretningen er alvorlige, og deler Statsrevisorernes kritik.

Ministeren oplyser, at Energinet.dk forud for Rigsrevisionens undersøgelse har lagt en plan for at højne den it-sikkerhedsmæssige modenhed med afsæt i virksomhedsstrategien. På baggrund af beretningen er planen blevet tilføjet enkelte punkter. Planen har ledelsens bevågenhed og styres inden for rammerne af ISO 27001. Ministeren hæfter sig ved, at Energinet.dk følger planen, og at den vil behandle alle Rigsrevisionens kritikpunkter. Ministeren oplyser, at Energinet.dk gennem denne indsats har udbedret hovedparten af de kritikpunkter, som Rigsrevisionen påviste, og at de få punkter, der fortsat er under behandling, forventes udbedret i 2016.

Ministeren oplyser, at Energinet.dk for at være på forkant med den teknologiske udvikling og udviklingen i trusselsbilledet bl.a. har etableret en styringsmodel, der sikrer løbende risikovurdering og opdatering af sikkerhedsforanstaltninger.

Ministeren oplyser desuden, at Energinet.dk i foråret 2015 har etableret tekniske systemer, der på isoleret vis logger trafik og på systematisk vis overvåger anomalier i it-miljøet.

Endelig oplyser ministeren, at han samlet set er af den opfattelse, at de aktuelle indsatser og det ledelsesmæssige fokus vil bidrage til fortsat at højne informationssikkerheden i Energinet.dk.

12. Transport- og bygningsministeren oplyser, at Banedanmark tager Rigsrevisionens anbefalinger til efterretning og fx har begrænset såvel antallet af betroede it-medarbejdere som system- og servicekonti med udvidede administratorrettigheder. Endvidere vil Banedanmark bl.a. tilpasse personlige passwords og systempasswords som anbefalet og sikre, at system- og servicekonti med udvidede administratorrettigheder ikke kan tilgå netværket fra lokale arbejdsstationer.

Ministeren oplyser desuden, at Banedanmark forud for beretningen har igangsat tiltag, der skal medvirke til at forbedre opfølgningen på logning. På baggrund af beretningen vil Banedanmark igangsætte tiltag, der skal medvirke til yderligere at forbedre de eksisterende rutiner for at opfange anomalier.

13. Sundheds- og ældreministeren tager arbejdet med informationssikkerhed særdeles alvorligt og oplyser, at der arbejdes målrettet på løbende at højne informationssikkerheden i Sundheds- og Ældreministeriets koncern.

Ministeren oplyser desuden, at gennemførelsen af de konkrete tiltag, som Sundhedsdatastyrelsen har iværksat i forbindelse med Rigsrevisionens udarbejdelse af beretningen, i det store og hele følger planen. Ministeren oplyser, at en række af de kritikpunkter, som Rigsrevisionen påviste, er udbedret, og de resterende punkter forventes udbedret i 2016.

14. Ministrene har således oplyst, at institutionerne vil rette op på de konstaterede mangler i forhold til styring, kontrol og logning af de udvidede administratorrettigheder, og at de har planlagt, igangsat og/eller gennemført en række initiativer. Rigsrevisionen finder det tilfredsstillende, at institutionerne vil rette op på de konstaterede mangler, og vurderer derfor, at beretningssagen kan afsluttes.

Rigsrevisionen vil dog som led i it-revisionen fortsat følge, at initiativerne bliver gennemført og fungerer i praksis, og at institutionerne således forbedrer deres styring, kontrol og logning af de udvidede administratorrettigheder. Rigsrevisionen vil i den forbindelse foretage en gennemgang af de 16 revisionskriterier, som beretningen omhandlede. Derudover vil Rigsrevisionen i forbindelse med it-revisionen følge op på beretningens anbefalinger om, at institutionerne jævnligt bør tage aktivt stilling til tilstrækkeligheden af deres styring, kontrol og logning af de udvidede administratorrettigheder og sikre ledelsesmæssigt fokus og prioritering for at rette op på de konstaterede forhold.

Hvis Rigsrevisionen ikke finder initiativerne tilstrækkelige, vil Rigsrevisionen orientere Statsrevisorerne herom i beretning om revisionen af statsregnskabet.

Lone Strøm