RIGSREVISIONEN

Rigsrevisionens notat om beretning om

styring af it-sikkerhed hos it-leverandører

Marts 2017

Vedrører:
Statsrevisorernes beretning nr. 5/2016 om styring af it-sikkerhed hos it-leverandører

Erhvervsministerens redegørelse af 13. januar 2017
Justitsministerens redegørelse af 16. januar 2017
Ministeren for offentlig innovations redegørelse af 17. januar 2017
Skatteministerens redegørelse af 17. januar 2017
Beskæftigelsesministerens redegørelse af 18. januar 2017

17. februar 2017

RN 1502/17

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

KONKLUSION

Det fremgik af beretningen, at Rigspolitiet opfyldte alle de opstillede kriterier vedrørende it-sikkerhed. Justitsministeren oplyser, at Justitsministeriet vil sørge for, at Rigspolitiet deler sine positive erfaringer med at styre it-sikkerheden hos eksterne it-leverandører med andre relevante myndigheder på ministeriets område.

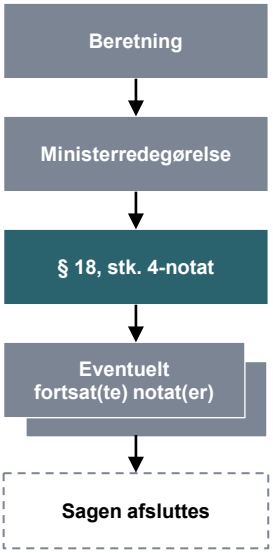
Ministeren for offentlig innovation, skatteministeren og beskæftigelsesministeren oplyser, at de vil følge og rette op på de mangler, som Rigsrevisionen konstaterede i beretningen. Ministerierne har således iværksat eller vil iværksætte en række initiativer i forhold til myndighedernes styring af it-sikkerheden hos eksterne it-leverandører, både i forhold til myndighedernes risikovurderinger og myndighedernes krav til og opfølgning på de eksterne it-leverandørers it-sikkerhed.

Erhvervsministeren oplyser ligeledes, at Søfartsstyrelsen vil forbedre sine risikovurderinger. Ministeren oplyser derudover, at ministeren imødeser, at Finansministeriet præciserer tilsynet med it-sikkerheden for de it-systemer, der drives af Statens It.

Rigsrevisionen finder det tilfredsstillende, at myndighederne vil følge og rette op på de konstaterede mangler. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Rigsrevisionen vil dog som led i it-revisionen fortsat følge, om myndighedernes initiativer bliver gennemført og fungerer i praksis, og følge op på anbefalingerne i beretningen.

Sagsforløb for en større undersøgelse



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

Ministeren for offentlig innovation oplyser, at Finansministeriet vil præcisere omfanget af ministeriets tilsyn med Statens It på vegne af de myndigheder, som er kunder hos Statens It, med henblik på at der fremadrettet fremstår en klar ansvars- og opgavefordeling i relation til omfanget af Finansministeriets tilsyn og kundernes forpligtelser.

Rigsrevisionen finder det positivt, at Finansministeriet præciserer omfanget af ministeriets tilsyn og kundernes forpligtelser. Rigsrevisionen finder det vigtigt, at Finansministeriet skaber klarhed om ansvars- og opgavefordelingen, og vil fortsat følge ministeriets arbejde hermed og orientere Statsrevisorerne herom.

I. Baggrund

- *Rigspolitiet hører under Justitsministeriet.*
- *SKAT hører under Skatteministeriet.*
- *Styrelsen for Arbejdsmarked og Rekruttering hører under Beskæftigelsesministeriet.*
- *Digitaliseringsstyrelsen hører under Finansministeriet.*

  Søfartsstyrelsen hører under Erhvervsministeriet.

2. Rigsrevisionen afgav i november 2016 en beretning om styring af it-sikkerhed hos it-leverandører. 5 myndigheder og 6 it-systemer indgik i beretningen: Rigspolitiet (Det Centrale Pasregister), SKAT (TastSelv Borger og Nyt TastSelv Erhverv), Styrelsen for Arbejdsmarked og Rekruttering (Det fælles datagrundlag), Digitaliseringsstyrelsen (NemID) og Søfartsstyrelsen (Skibsregistret).

Det fremgik af beretningen, at hovedparten af de undersøgte myndigheder skulle forbedre deres risikovurderinger, som bør danne grundlag for myndighedernes styring af it-sikkerheden hos it-leverandørerne. Rigsrevisionen vurderede desuden, at hovedparten af de undersøgte myndigheder kunne forbedre deres krav til og opfølgning på adgangsstyring og logning.

For Søfartsstyrelsen og Styrelsen for Arbejdsmarked og Rekruttering, som er kunder hos Statens it, fremgik det af beretningen, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser.

3. Da Statsrevisorerne behandlede beretningen, bemærkede de bl.a., at statslige myndigheder generelt kan outsource it-driften til eksterne it-leverandører, men ikke ansvaret for it-sikkerheden.

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

II. Gennemgang af ministrenes redegørelser

5. Det fremgik af beretningen, at Rigspolitiet opfyldte alle de opstillede kriterier. Justitsministeren oplyser i sin redegørelse, at Justitsministeriet vil sørge for, at Rigspolitiet deler sine positive erfaringer med at styre it-sikkerheden hos eksterne it-leverandører med andre relevante myndigheder på ministeriets område. Vi gennemgår derfor ikke justitsministerens redegørelse yderligere i dette notat.

Myndighedernes risikovurderinger

6. Statsrevisorerne fandt det utilfredsstillende, at 4 ud af de 5 myndigheder ikke havde udarbejdet en tilstrækkelig risikovurdering.

7. Erhvervsministeren, skatteministeren og beskæftigelsesministeren oplyser, at deres ministerier vil styrke risikovurderingerne af de undersøgte it-systemer. Ministerierne vil også arbejde for at styrke risikovurderingerne af it-systemer på tværs af deres ministerområder.

8. Ministeren for offentlig innovation oplyser, at Digitaliseringsstyrelsen ligeledes vil styrke risikovurderingen. Derudover oplyser ministeren, at Finansministeriet på baggrund af beretningen vil vurdere, om anbefalingerne i beretningen giver anledning til at opdatere de generelle vejledninger om it-sikkerhed, herunder vejledninger om ISO 27001 og den risikobaserede tilgang.

Myndighedernes krav til og opfølgning på it-leverandørernes it-sikkerhed
9. Statsrevisorerne fandt det bekymrende, at myndighederne – med undtagelse af Rigspolitiet – ikke i tilstrækkelig grad stiller krav til it-leverandørers sikkerhedsniveau. Kravene bør være klare og baseret på risikovurderinger, og myndighederne bør følge op herpå.

10. Skatteministeren og beskæftigelsesministeren oplyser, at de har iværksat eller vil iværksætte en række tiltag til at forbedre krav og opfølgning.

Beskæftigelsesministeren oplyser endvidere, at ministeren ser frem til, at Finansministeriet og Statens It afklarer og præciserer ansvars- og opgavefordelingen i forhold til tilsynet, så Styrelsen for Arbejdsmarked og Rekruttering kan indgå aftale med Statens It om de eksakte rammer for opgavevaretagelsen. Endelig oplyser ministeren, at styrelsen vil aftale med Statens It, hvilke revisorerklæringer der skal benyttes fremover, og præcisere, hvordan der kan gennemføres yderligere supplerende kontroller med it-sikkerheden hos it-leverandøren. Dette sker ifølge redegørelsen på baggrund af Rigsrevisionens kritik af, at styrelsen hidtil har modtaget en overordnet revisorerklæring.

Rigsrevisionen bemærker, at vi i beretningen gjorde opmærksom på, at hvis en myndighed modtager en generel revisorerklæring, bør myndigheden på anden vis følge op på det, revisorerklæringen ikke dækker. Det skyldes, at generelle revisorerklæringer omhandler it-leverandørernes generelle it-kontroller og dækker leverandørernes fælles it-miljø, der normalt kun dækker lag 5-8 i it-infrastrukturen.

11. Erhvervsministeren konstaterer, at Erhvervsministeriet har været uenig med Rigsrevisionen i, at tilsynsforpligtelsen med Skibsregistret alene påhviler Søfartsstyrelsen. Ministeren konstaterer videre, at der lader til at være uklarhed om omfanget af Finansministeriets tilsynsforpligtelse med Statens It. Ministeren tilslutter sig derfor Statsrevisorerne, som fandt det væsentligt, at Finansministeriet præciserer ansvaret med tilsynet med it-sikkerheden for de it-systemer, der drives af Statens It. Erhvervsministeriet arbejder løbende med at forbedre it-sikkerheden og har valgt at indgå i et samarbejde med Statens It og Finansministeriet om at synliggøre sikkerheds- og tilsynsniveauet for kunderne i Statens It. Både Rigsrevisionens beretning og resultatet af Finansministeriets præcisering af tilsynsforpligtelsen vil indgå i dette arbejde.

12. Ministeren for offentlig innovation bemærker, at Rigsrevisionen ikke anfægter, at Digitaliseringsstyrelsen i forhold til NemID stiller de rigtige og tilpas eksplicitte krav til it-leverandøren.

Rigsrevisionen bemærker hertil, at det fremgik af beretningen, at Digitaliseringsstyrelsen kunne forbedre kravene om adgangsrettigheder og brugerrettighedskontroller af it-leverandørens medarbejdere.

13. Ministeren for offentlig innovation bemærker videre, at Digitaliseringsstyrelsen vil igangsætte et arbejde for at hæve niveauet for afrapportering i revisionsprotokollatet, så det inkluderer mere eksplicitte redegørelser for de udførte kontroller, som i højere grad kan bruges i risikovurderingen af NemID.

Finansministeriets præcisering af tilsynet med it-systemer, der drives af Statens It
14. Statsrevisorerne fandt det væsentligt, at Finansministeriet præciserer ansvaret for tilsynet med it-sikkerheden for de it-systemer, som drives af Statens It.

15. Ministeren for offentlig innovation oplyser, at Finansministeriets departement vil tage initiativ til at præcisere omfanget af ministeriets tilsyn med Statens It på kundernes vegne. Herunder vil ministeriet drøfte ansvars- og opgavefordelingen med Statens It's kunder ved afrapportering af tilsynet for 2016, med henblik på at der fremadrettet fremstår en klar ansvars- og opgavefordeling i relation til omfanget af Finansministeriets tilsyn og kundernes forpligtelser. Arbejdet med præciseringer og drøftelser med Statens It's kunder forventes ifølge redegørelsen afsluttet inden udgangen af 2017.

Opsummering
16. Ministrene oplyser således, at de vil følge og rette op på de konstaterede mangler i forhold til myndighedernes styring af it-sikkerheden hos deres eksterne it-leverandører. Ministrene har iværksat eller vil iværksætte en række initiativer, herunder i forhold til myndighedernes arbejde med risikovurderinger, myndighedernes krav til de eksterne it-leverandørers sikkerhedsniveau og deres opfølgning herpå.

17. Rigsrevisionen finder det tilfredsstillende, at myndighederne vil følge og rette op på de konstaterede mangler, og vurderer derfor, at denne del af sagen kan afsluttes.

Rigsrevisionen vil dog som led i it-revisionen fortsat følge, om initiativerne bliver gennemført og fungerer i praksis.

18. Ministeren for offentlig innovation oplyser, at Finansministeriet vil præcisere omfanget af ministeriets tilsyn med Statens It og kundernes forpligtelser.

Rigsrevisionen finder dette positivt. Rigsrevisionen finder det vigtigt, at Finansministeriet skaber klarhed om ansvars- og opgavefordelingen, og vil fortsat følge ministeriets arbejde hermed og orientere Statsrevisorerne herom.

Lone Strøm