RIGSREVISIONEN

Rigsrevisionens notat om beretning om

styring af it-sikkerhed hos it-leverandører

August 2018

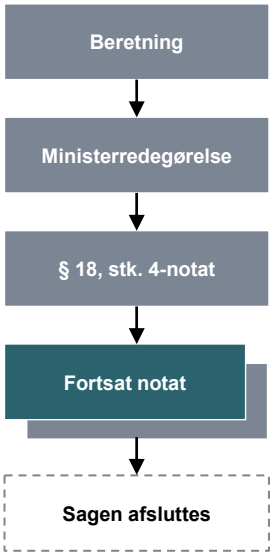
Opfølgning i sagen om styring af it-sikkerhed hos it-leverandører (beretning nr. 5/2016)

25. juni 2018

RN 1507/2018

1. Rigsrevisionen følger i dette notat op på sagen om styring af it-sikkerhed hos it-leverandører, som blev indledt med en beretning i 2016. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 17. februar 2017.

Sagsforløb for en større undersøgelse



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

KONKLUSION

Finansministeriet har gennemført en række initiativer for at præcisere omfanget af sit tilsyn med Statens It på kundernes vegne.

Rigsrevisionen finder initiativerne tilfredsstillende og vurderer, at sagen kan afsluttes.

Rigsrevisionen baserer konklusionen på følgende:

- Finansministeriet har udarbejdet en vejledning om tilsynet med Statens It's it-sikkerhed og inddraget Statens It's kunder i arbejdet hermed. I vejledningen uddyber og præciserer Finansministeriet omfanget af sit tilsyn med Statens It på kundernes vegne og beskriver ansvars- og opgavefordelingen mellem Finansministeriet og Statens It's kunder.

Rigsrevisionen finder, at initiativerne er et godt udgangspunkt for fordelingen af ansvar og opgaver mellem Finansministeriet og Statens It's kunder i tilsynet med Statens It. Rigsrevisionen vil dog som led i it-revisionen fortsat følge, om tilsynskonceptet også fungerer i praksis.

I. Baggrund

2. Rigsrevisionen afgav i november 2016 en beretning om styring af it-sikkerhed hos it-leverandører. Beretningen handlede om, hvordan 5 myndigheder havde styret it-sikkerheden for 6 systemer hos deres eksterne it-leverandører. De undersøgte myndigheder og systemer var Rigspolitiet (Det Centrale Pasregister), SKAT (TastSelv Borger og Nyt TastSelv Erhverv), Styrelsen for Arbejdsmarked og Rekruttering (Det fælles datagrundlag), Digitaliseringsstyrelsen (NemID) og Søfartsstyrelsen (Skibsregistret).

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-driften.

4. 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. Myndighedernes risikovurderinger.	Afsluttet i forbindelse med notat til Statsrevisorerne af 17. februar 2017.
2. Myndighedernes krav til opfølgning på it-leverandørernes it-sikkerhed.	Afsluttet i forbindelse med notat til Statsrevisorerne af 17. februar 2017.
3. Finansministeriets præcisering af tilsynet med it-systemer, der drives af Statens It.	Behandles i dette notat.

5. Vi redegør i dette notat for resultaterne af opfølgningen på det punkt, der ikke tidligere er afsluttet.

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

II. Finansministeriets initiativer

6. Vi gennemgår i det følgende Finansministeriets initiativer i forhold til det udestående opfølgningspunkt. Gennemgangen er baseret på drøftelser og mailkorrespondance med Finansministeriet samt den vejledning, Finansministeriet har udarbejdet om sit tilsyn med Statens It på kundernes vegne, hvori opgave- og ansvarsfordelingen i forhold til tilsynet bliver uddybet og præciseret. Derudover har vi modtaget præsentionsmateriale fra Finansministeriets møder med Statens It's kunder.

Finansministeriets præcisering af tilsynet med it-systemer, der drives af Statens It

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

8. Det fremgik af beretningen, at Finansministeriet fører tilsyn med Statens It's it-sikkerhed på vegne af de kunder, der får varetaget driften af deres it-systemer hos Statens It. Det fremgik endvidere, at Statens It's kunder samtidig selv har ansvaret for at foretage risikovurdering af egne fagsystemer og at stille krav til Statens It, hvis risikovurderingen viser, at der er behov for det. Det fremgik også, at Statens It's kunder er forpligtede til aktivt at forholde sig til det tilsyn, Finansministeriet fører på vegne af kunderne, og at der var uklarhed om denne ansvars- og opgavefordeling i forhold til tilsynet med Statens It.

Endelig fremgik det af beretningen, at Styrelsen for Arbejdsmarked og Rekruttering samt Søfartsstyrelsen, der begge er kunder hos Statens It, ikke havde været opmærksomme på deres forpligtelser med hensyn til krav til og opfølgning på it-sikkerheden i de undersøgte it-systemer. Det skyldtes, at de havde en anden opfattelse af ansvars- og opgavefordelingen end Finansministeriet, og at de fandt, at de var dækket af Finansministeriets tilsyn.

Driftsmodel

Statens It har struktureret sine leverancer over for kunderne i driftsmodeller, der afspejler, hvor mange af de i alt 8 lag i it-infrastrukturen (ledelsens informationssikkerhedsstyring, applikationer, middleware, operativsystem, server/storage, netværk, fysisk lokation og tværgående områder) der er indeholdt i driftsmodellen.

Når en kunde har overført sin basale it-drift til Statens It, bliver tilsynet med it-driften udført af Finansministeriet på kundens vegne (ressortoverførsel). Omfanget af Finansministeriets tilsyn og kundens forpligtelser er afhængige af den driftsmodel, der er indgået aftale om.

9. Ministeren for offentlig innovation oplyste i sin redegørelse, at Finansministeriet ville tage initiativ til at præcisere omfanget af ministeriets tilsyn med Statens It på kundernes vegne, herunder drøfte dette med kunderne.

10. Finansministeriet har på den baggrund udarbejdet en vejledning om tilsynet med Statens It. Heri har ministeriet beskrevet ansvars- og opgavefordelingen mellem Statens It's kunder og Finansministeriet samt omfanget af Finansministeriets tilsyn. Det fremgår af vejledningen, at Finansministeriets tilsyn og kundens eget ansvar afhænger af driftsmodellen for det enkelte system, og vejledningen er struktureret med udgangspunkt i de 6 driftsmodeller, der findes. Vejledningen beskriver opgave- og ansvarsfordelingen mellem Finansministeriet og Statens It's kunder for hver driftsmodel og eksemplificerer beskrivelserne med cases, bl.a. vedrørende *Det fælles datagrundlag* fra Styrelsen for Arbejdsmarked og Rekruttering og *Skibsregistret* fra Søfartsstyrelsen.

Det fremgår bl.a., at *Det fælles datagrundlag* er omfattet af driftsmodel 5, der fx indebærer, at kunden har ansvaret for det lag i it-infrastrukturen, der vedrører applikationer, og selv skal foretage risikovurdering, føre tilsyn med fx oprettede brugere og udarbejde egne beredskabsplaner i forhold til dette lag. Det fremgår også, at Finansministeriet fører tilsyn i forhold til de øvrige lag, fx operativsystem, server og netværk. Boks 1 viser et eksempel på en beskrivelse af kundens ansvar for driftsmodel 5 i vejledningen.

BOKS 1. EKSEMPEL PÅ KUNDENS ANSVAR MED EN AFTALE OM DRIFTSMODEL 5

Hvis institutionen har et system i driftsmodel 5, vil institutionen skulle:

- Foretage detaljeret risikovurdering af systemet i forbindelse med udbud og kontraktindgåelse.
- Foretage løbende risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold:
  - Hvis institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive (Statens It såvel som den eksterne leverandør). Dette sker gennem kontrol af den aftalte rapportering.
  - Forholde sig til Finansministeriets tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
  - Indhente revisorerklæringer fra Statens It og forholde sig til, om der er forbehold eller supplerende oplysninger, som kræver reaktioner.
  - Rekvirere og forholde sig til Statens It's årlige sikkerhedsaudit af eksterne leverandører.
  - Deltage i relevante kundefora, som Statens It stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

Kilde: Finansministeriets "Vejledning om tilsynet med Statens It", december 2017.

Revisorerklæring
I driftsmodel 5, hvor leverandørstyringen er ressortoverført til Statens It, og hvor den basale drift af et system sker hos en ekstern leverandør, er det muligt at indhente en revisorerklæring fra den eksterne leverandørs revisor.

11. Rigsrevisionen skal generelt bemærke, at ansvarsfordelingen og risikovurderingen altid skal tage udgangspunkt i de konkrete forhold, fx at det aktuelle system kræver særlige sikkerhedsforanstaltninger.

Vores gennemgang af det øvrige materiale viser, at Finansministeriet på en række møder for Statens It's eksisterende og nye kunder har præsenteret omfanget af sit tilsyn samt ansvars- og opgavefordelingen.

Gennemgangen viser desuden, at Finansministeriet – som led i udarbejdelsen af vejledningen – har inddraget Statens It's kunder. Ministeriet har således etableret en arbejdsgruppe med deltagelse af Erhvervsministeriet, Beskæftigelsesministeriet, Miljø- og Fødevareministeriet og Uddannelses- og Forskningsministeriet. Finansministeriet oplyser, at arbejdsgruppen har bidraget med indsigt i institutionernes behov for beskrivelse og præcisering af tilsynet og har givet input til niveau og omfang af beskrivelsen. Gennemgangen viser også, at Finansministeriet har drøftet vejledningen og tilsynsmodellen med Justitsministeriet og Datatilsynet. Vejledningen har også været drøftet med Rigsrevisionen.

12. Rigsrevisionen finder det tilfredsstillende, at Finansministeriet har præciseret omfanget af sit tilsyn med Statens It på kundernes vegne, at kunderne har været inddraget, og at opgave- og ansvarsfordelingen er præsenteret for og drøftet med kunderne. Rigsrevisionen vurderer derfor, at sagen kan afsluttes.

Rigsrevisionen finder, at initiativerne er et godt udgangspunkt for fordelingen af ansvar og opgaver mellem Finansministeriet og Statens It's kunder i tilsynet med Statens It. Rigsrevisionen vil dog som led i it-revisionen fortsat følge, om tilsynskonceptet også fungerer i praksis.

Lone Strøm