FINANSMINISTERIET

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

17. januar 2017

Redegørelse fra Ministeren for offentlig innovation om beretning nr. 5/2016 om styring af it-sikkerhed hos it-leverandører i Finansministeriet

Med henvisning til Statsrevisorernes skrivelse af 9. november 2016 angående beretning 5/2016 om styring af it-sikkerhed hos it-leverandører fremsender jeg hermed ministerredegørelse herom.

Statsrevisorernes beretning omhandler, hvordan fem myndigheder: Rigspolitiet (Det centrale Pasregister), SKAT (TastSelv Borger og Nyt TastSelv Erhverv), Styrelsen for Arbejdsmarked og Rekruttering (Det fælles datagrundlag), Digitaliseringsstyrelsen (NemID) og Søfartsstyrelsen (Skibsregistret) styrer it-sikkerheden hos deres eksterne it-driftsleverandører. I nærværende redegørelse besvares forhold vedrørende Digitaliseringsstyrelsens tilsyn med NemID og Finansministeriets tilsyn med Statens It.

Jeg er enig med Statsrevisorerne i, at myndigheder har ansvaret for styring af it-sikkerheden i outsourcet it-drift. Endvidere mener jeg også, at denne styring skal være baseret på sikkerhedsstandarden ISO 27001.

Statsrevisorerne finder det bekymrende, at myndighederne – med undtagelse af Rigspolitietet – ikke i tilstrækkelig grad stiller krav til it-leverandørernes sikkerhedsniveau. Kravene bør være klare og baseret på risikovurderinger, og myndighederne bør følge op herpå.

Rigsrevisionen anfægter ikke, at Digitaliseringsstyrelsen i forhold til NemID stiller de rigtige og tilpas eksplicitte krav til leverandøren fx vedrørende brugerstyring, logning mv. Den eksterne årlige revision af leverandøren udføres endvidere i overensstemmelse med den standard, Rigsrevisionen selv anbefaler til formålet. Dog finder Rigsrevisionen, at opfølgningen på Digitaliseringsstyrelsens krav foretages på et for overfladisk niveau i revisionsprotokollatet. Dermed får styrelsen ikke indblik i, hvilke kontroller revisor lægger til grund for sine konklusioner samt hvilke områder, der eventuelt ikke er undersøgt tilstrækkeligt grundigt efter styrelsens vurdering. Digitaliseringsstyrelsen anerkender kritikken og vil på den baggrund straks igangsætte et arbejde for at hæve niveauet for afrap-

porteringen i revisionsprotokollatet, således at det inkluderer mere eksplicitte redegørelser for de udførte kontroller og dermed også i højere grad leverer input til den årlige risikovurdering af NemID.

Statsrevisorerne finder det utilfredsstillende, at 4 ud af de 5 myndigheder ikke har udarbejdet en tilstrækkelig risikovurdering.

Digitaliseringsstyrelsen modtager løbende kvartalsvise risikovurderinger udarbejdet af leverandøren og udarbejder selv en årlig risikovurdering af NemID. Digitaliseringsstyrelsen foretager opfølgning på den løbende kvartalsvise risikovurdering. Arbejdet er baseret på den anerkendte internationale ISO-standard og national DS-standard. Digitaliseringsstyrelsen forholder sig dermed løbende til de risici, der knytter sig til NemID og foretager en vurdering af leverandørens tiltag. Digitaliseringsstyrelsen anerkender dog, at den årlige risikovurdering skal gennemgå en kritisk revision, så det bliver muligt for Digitaliseringsstyrelsen at dokumentere sikkerhedsstyringen, og at denne er baseret på en risikovurdering. En sådan revision vil blive gennemført i 2017.

Finansministeriet sætter rammerne for arbejdet med informationssikkerhed i den offentlige sektor. På baggrund af beretningen vil Finansministeriet vurdere, om anbefalingerne giver anledning til at opdatere de generelle vejledninger om informationssikkerheden. Det vil eksempelvis være relevant at vurdere, om vejledningerne om ISO27001 og den risikobaserede tilgang til drift skal knyttes op imod endnu mere præcise krav til styring af sikkerhed såvel som afrapportering af overholdelsen af kravene. Det vil selvsagt også indgå i disse vurderinger, om Rigsrevisionens beretning giver anledning til at ændre praksis vedrørende andre it-løsninger, som Digitaliseringsstyrelsen administrerer.

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

Finansministeriets departement fører tilsyn med Statens It på kundernes vegne. Rigsrevisionens undersøgelse viser dog en uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It, idet STAR og Søfartsstyrelsen, som de undersøgte kunder hos Statens It, i forbindelse med undersøgelsen har oplyst, at de to styrelser ikke har været opmærksomme på deres forpligtelser med hensyn til krav og opfølgning i forhold til Statens It. Dette skyldes – ifølge undersøgelsen – at de to styrelser har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It end Finansministeriets opfattelse.

Finansministeriets departement vil tage initiativ til at præcisere omfanget af tilsynet med Statens It på kundernes vegne, herunder drøfte ansvars- og opgavefordelingen med Statens It's kunder ved afrapporteringen af tilsynet for 2016. Dette

med henblik på, at der fremadrettet fremstår et klart opgave- og ansvarssnit i relation til omfanget af tilsynet og kundernes forpligtelser i den forbindelse.

Arbejdet med præciseringer og drøftelser med Statens It's kunder forventes tilendebragt inden udgangen af 2017.

Dette brev er fremsendt per post og elektronisk til Statsrevisorerne og i kopi til Rigsrevisor.

Med venlig hilsen

Sophie Løhde
Minister for offentlig innovation