Statsrevisorernes Sekretariat
Christiansborg
1240 København K

ministersvar@ft.dk

Beskæftigelsesministeren
Ved Stranden 8
1061 København K

T +45 72 20 50 01
E bm@bm.dk
www.bm.dk

CVR 10172748

18 JAN. 2017

J.nr. 16/16912

Beskæftigelsesministerens redegørelse vedr. Beretning om styring af it-sikkerhed hos it-leverandører (nr. 5/2016)

Statsrevisorerne har den 9. november afgivet bemærkninger til Rigsrevisionens beretning nr. 5/2016 om styring af it-sikkerhed hos it-leverandører samt i brev af 17. november 2016 anmodet om en redegørelse for de foranstaltninger og overvejelser, som beretningen giver anledning til.

For Beskæftigelsesministeriet er det af afgørende betydning at have fokus på it-sikkerheden i de it-systemer, som anvendes af ministeriet og dets styrelser. Jeg er derfor glad for, at vi med beretningen nu får sat fælles standarder og rammer for statsinstitutionernes fastsættelse af fremtidige sikkerhedskrav over for it-leverandørerne.

Rigsrevisionen har i sin beretning set på, hvordan Styrelsen for Arbejdsmarked og Rekruttering (STAR) samt en række andre statslige myndigheder har styret it-sikkerheden hos de eksterne leverandører bl.a. med henblik på at kunne give anbefalinger om, hvordan statslige myndigheder fremadrettet bør stille krav til styringen af it-sikkerheden hos it-leverandørerne.

Rigsrevisionen rejser kritik af STAR for ikke at have udarbejdet en tilstrækkelig grundig risikovurdering af Det Fælles Datagrundlag (DFDG) vedrørende it-sikkerhed. Rigsrevisionen bemærker, at tilstrækkelige risikovurderinger er et væsentligt grundlag for, at myndighedernes styring tager udgangspunkt i deres dokumenterede behov vedrørende sikring af tilgængelighed, fortrolighed og integritet i forhold til den samlede it-infrastruktur.

Statsrevisorerne finder det utilfredsstillende, at STAR og en række andre statslige myndigheder ikke løbende foretager tilstrækkelige risikovurderinger, ligesom Statsrevisorerne betegner det som bekymrende, at bl.a. STAR efter Statsrevisorernes opfattelse ikke i tilstrækkelig grad har stillet krav til it-leverandørernes sikkerhedsniveau, adgangsstyring og logning.

Jeg tager Rigsrevisionens anbefalinger og Statsrevisorernes bemærkninger til efterretning.

Jeg er helt enig i, at det er nødvendigt at prioritere en høj kvalitet i styringen af it-sikkerheden hos de it-leverandører, Beskæftigelsesministeriet anvender. Derfor er jeg også parat til at styrke rammerne og i nødvendigt omfang skærpe retningslinjerne, så Beskæftigelsesministeriet og dets styrelser er klædt godt på til at løfte opgaven med at styre it-sikkerheden hos de eksterne it-leverandører.

Jeg hæfter mig særligt ved den uklarhed om tilsynsforpligtelsen med Statens It, som beretningen omtaler, og jeg ser meget positivt på, at Statsrevisorerne også fremhæver væsentligheden i, at Finansministeriet tager initiativ til en afklaring. Jeg har en forventning om, at der i samarbejde med Finansministeriet skabes fuld afklaring af tilsynsansvaret med hensyn til de it-systemer, som drives af Statens It eller eksterne leverandører under Statens It's rammeaftale. Det har stor betydning for, at Beskæftigelsesministeriet og andre statsinstitutioner også fremover kan sætte de nødvendige sikkerhedskrav.

Jeg vil i det følgende redegøre for de initiativer, som beretningens indhold og konklusioner samt Statsrevisorernes bemærkninger har givet anledning til.

Risikovurdering
Det fremgår af beretningen, at Rigsrevisionen vurderer, at STAR skal forbedre sin risikovurdering af DFDG, og at den nuværende risikovurdering er for overordnet.

På den baggrund kan jeg oplyse, at STAR vil sikre, at der i første halvår 2017 bliver udarbejdet en forbedret risikovurdering af DFDG for alle dele af it-infrastrukturen. STAR vil desuden benytte anledningen til at udarbejde retningslinjer med fastsættelse af kriterier for risikovurdering generelt.

Adgangsstyring
Jeg konstaterer, at Rigsrevisionen finder, at STAR har fastsat utilstrækkelige krav vedrørende adgangsrettigheder og brugerrettighedskontrol for leverandørens ansatte samt krav til opfølgning på leverandørens passwordkvalitet.

Hertil vil jeg bemærke, at STAR i 2017 vil fastsætte nærmere retningslinjer for at sikre, at der konkret tages stilling til medarbejderadgang, adgangsstyring og brugerrettighedskontrol for de leverandøransatte på alle niveauer i it-infrastrukturen.

Jeg kan supplerende nævne, at STAR efter aftale med KMD allerede har ændret og skærpet passwordkvaliteten i overensstemmelse med Rigsrevisionens anbefalinger.

Logning
Med hensyn til logning noterer jeg, at STAR kun delvist opfylder kravet om, at der skal stilles krav om logning i alle dele af it-infrastrukturen.

Endvidere konkluderer Rigsrevisionen, at STAR kun delvist følger op på leverandørens logning, herunder via en revisorerklæring om overholdelse af logningspraksis m.v., og at STAR ikke fuldt ud lever op til kravet om fastsatte opbevaringsperioder af logningen i alle dele af it-infrastrukturen.

STAR vil derfor udarbejde konkrete retningslinjer for alle niveauer i it-infrastrukturen, og STAR har oplyst, at de vil drøfte med Statens It, hvordan den nødvendige kontrol af leverandørens logning kan sikres.

Endelig vil der fra styrelsens side blive fastsat regler for, hvor længe loggen i alle dele af it-infrastrukturen fremadrettet skal gemmes, herunder også regler for loggennemgang og opbevaringsperiode m.v.

Revisorerklæring
For så vidt angår kritikken af, at STAR kun har modtaget en overordnet revisorerklæring, der ikke forholder sig detaljeret til adgangsstyring og logning i it-systemets hele infrastruktur, kan jeg oplyse, at STAR vil aftale med Statens It, hvilke revisorerklæringer STAR fremover skal benytte. Herudover bemærker jeg, at styrelsen vil præcisere, hvordan der kan gennemføres yderligere, supplerende kontroller med it-sikkerheden hos leverandøren.

Uklarhed om tilsynsforpligtelse
Jeg har noteret, at Rigsrevisionens undersøgelse har vist, at der er en uklarhed om ansvars- og opgavefordelingen mellem Finansministeriet, Statens It og Statens It's kunder i forhold til tilsynsforpligtelsen. Jeg ser meget frem til, at Finansministeriet og Statens It afklarer og præciserer opgave- og tilsynsansvaret, så STAR i forlængelse heraf kan indgå nærmere aftale med Statens It om de eksakte rammer for opgavevaretagelsen. På den baggrund er det min forventning, at en større klarhed af tilsynsforpligtelsen vil styrke fundamentet for at fastsætte af et solidt sikkerhedsniveau i forhold til DFDG.

Det er min sammenfattende vurdering, at de ovenfor skitserede initiativer tilsammen vil skabe den fornødne og tilstrækkelige kontrol med sikkerheden hos it-leverandørerne på beskæftigelsesområdet. Endvidere vil Beskæftigelsesministeriet og dets styrelser fortsat have fokus på at iværksætte de nødvendige initiativer, som kan sikre, at de it-systemer, der anvendes af ministeriet og styrelserne, er baseret på et betryggende grundlag.

Afslutningsvis skal jeg bemærke, at ministeriet har sendt en kopi af ovenstående til rr@rigsrevisionen.dk.

Venlig hilsen

Troels Lund Poulsen