Skatteministeriet

17 JAN. 2017
J.nr. 16-1688614

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

Skatteministeriet
Nicolai Eigtveds Gade 28
DK 1402 – København K

Telefon +45 33 92 33 92
Mail skm@skm.dk

www.skm.dk

Ministerredegørelse til Statsrevisorernes beretning nr. 5/2016 om styring af it-sikkerhed hos it-leverandører

Statsrevisorerne har den 17. november 2016 sendt mig beretning nr. 5/2016 om styring af it-sikkerhed hos it-leverandører og bedt mig om at redegøre for de foranstaltninger og overvejelser, som beretningen og Statsrevisorernes bemærkninger giver anledning til.

I det følgende kommenteres beretningens konklusioner og Statsrevisorernes bemærkninger hertil.

1. Risikovurderinger
Jeg tager til efterretning, at Statsrevisorerne finder det utilfredsstillende, at 4 ud af 5 myndigheder – heriblandt SKAT – ikke har udarbejdet en tilstrækkelig risikovurdering, og at Statsrevisorerne finder det bekymrende, at der ikke i tilstrækkelig grad stilles krav til it-leverandørernes sikkerhedsniveau.

Jeg noterer mig, at Statsrevisorerne angiver, at kravene til it-leverandørernes sikkerhedsniveau bør være klare og baseret på risikovurderinger.

Særligt for så vidt angår SKAT bemærker Rigsrevisionen, at der ikke er foretaget en egentlig risikovurdering af TastSelv Borger, og at risikovurderingerne vedrørende Nyt TastSelv Erhverv er meget overordnede og mangler begrundelser, ligesom de ikke omfatter alle dele af systemernes infrastruktur. Der er derfor ikke et dækkende billede af risici i forhold til adgangsstyring og logning i it-infrastruktur.

Det er naturligvis ikke tilfredsstillende.

Jeg er enig med Rigsrevisionen i, at risikovurderinger er en forudsætning for, at man kan vurdere, hvilke krav der er relevante at stille til leverandørernes it-sikkerhed, og at sikkerhedskrav derfor bør sættes med udgangspunkt i en risikovurdering.

Jeg kan oplyse, at koblingen mellem sikkerhedskrav og risikovurdering er omdrejningspunktet for såvel Skatteministeriets informationssikkerhedspolitik som for ministeriets generelle arbejde med informationssikkerhed.

Jeg er enig i, at den nuværende risikovurderingsproces i SKAT i relation til it-systemer ikke er helt tilfredsstillende, og det er min vurdering, at der er behov for at styrke proces-

serne omkring risikovurderingerne. Skatteministeriet har udarbejdet en Risikostyringsmodel for informationssikkerhed, som har været anvendt til koncernens overordnede risikovurderinger, og som ministeriet nu vil udbrede til risikovurderinger af it-systemer. Modellen er bygget således op, så risikovurderinger foretages efter en kvalitetssikret og ensartet metode, kommer rundt om ISO27001 Anneks A, samt udmønter sig klart i konkrete sikkerhedskrav. Udbredelsen af modellen til risikovurderinger af it-systemer forventes afsluttet i andet kvartal 2017 og skal sikre, at Skatteministeriet fremadrettet stiller krav til it-sikkerhed efter en struktureret, systematisk og dækkende risikovurdering.

Jeg kan i forlængelse heraf oplyse, at der i første kvartal 2017 vil blive foretaget en opdateret risikovurdering af Nyt TastSelv Erhverv. TastSelv Borger vil blive risikovurderet i forbindelse med det kommende udbud af SKATs kritiske it-kontrakter.

2. Krav om revisorerklæringer og kontrol af it-sikkerhed

Jeg noterer mig Rigsrevisionens bemærkning om, at myndighederne bør sikre, at leverandørerne i relevant omfang er underlagt uafhængig ekstern it-sikkerhedsrevision, og at revisionsrapporterne løbende bør gøres tilgængelige for myndighederne, ligesom det er vigtigt, at der løbende følges op på it-sikkerheden – herunder med mulighed for at foretage kontrolinspektioner.

Jeg er enig med Rigsrevisionen i, at eksterne revisorerklæringer og muligheden for kontrolbesøg er et effektivt supplement til leverandørernes egne risikovurderinger i forbindelse med myndighedernes kontrol af leverandørens it-sikkerhed.

I forlængelse heraf kan jeg oplyse, at der for Nyt TastSelv Erhverv er modtaget en fornyet revisionserklæring for systemets it-sikkerhed den 12. december 2016 dækkende perioden fra overtagelsesdag til den 31. august 2016. I forbindelse med revisionen vil der blive foretaget en ekstraordinær undersøgelse af anvendelsen af brugerrettigheder, stærke passwords og beskyttelsen af logs i alle relevante dele af infrastrukturen.

3. Myndighedernes krav om og opfølgning på adgangsstyring og logning

Jeg noterer mig, at Rigsrevisionen finder, at blandt andet SKAT kan forbedre sine krav til leverandørernes adgangsstyring og logning og sin opfølgning herpå, da generelle og upræcise krav, der giver rum for fortolkning i forhold til leverandørens forpligtelser, medfører en risiko for, at leverandøren ikke har det tilstrækkelige eller forventede sikkerhedsniveau.

Skatteministeriets departement og SKAT arbejder med hjælp fra Kammeradvokaten på en opdatering af SKATs standard-sikkerhedsbilag til it-driftskontrakter for at sikre, at sikkerhedskravene er i overensstemmelse med ISO27001:2013, relevante lov- og myndighedskrav på informationssikkerhedsområdet, anbefalinger og vejledninger fra Center for Cybersikkerhed, samt bemærkningerne fra Rigsrevisionens beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver. I de kommende sikkerhedsbilag lægges der op til, at den til enhver tid gældende risikovurdering er omdrejningspunktet for sikkerheden omkring adgangsstyring, logning, opfølgning herpå m.m. Bilagene forventes at blive rullet ud i alle dele af ministeriet i januar 2017.

Særligt i forhold til TastSelv Borger, som er det af SKATs systemer i undersøgelsen, der har de største udfordringer i forhold til styring af it-sikkerhed hos leverandøren, kan jeg oplyse følgende. Systemet er en del af et større systemkompleks, der understøtter borgernes skatteberegning og årsopgørelse. SKAT har igangsat en udbudsproces vedrørende legacy-systemer, hvor TastSelv Borger indgår. SKAT er i gang med udarbejdelse af kravsspecifikation, herunder fastlæggelse af krav til informationssikkerhedsområdet i overensstemmelse med de ovenfor nævnte sikkerhedsbilag, den under punkt 1 nævnte risikostyringsmodel, og den under punkt 2 nævnte indhentelse af en ekstern revisorerklæring og fysiske kontrol.

Kopi af denne redegørelse er sendt til Rigsrevisionen.

Med venlig hilsen

Karsten Lauritzen