FINANSMINISTERIET

Folketingets Finansudvalg
Christiansborg

Finansministeren
Den 28. august 2015

Svar på Finansudvalgets spørgsmål nr. 3 (Alm. del – § 7. Finansministeriet) af 6. august 2015 stillet efter ønske fra Pernille Skipper (EL)

Spørgsmål
Overvejer ministeren, på baggrund af Datatilsynets afgørelse i den såkaldte CSC-sag (journalnr. 2013-632-0050 om uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for), at foretage ændringer i sikkerhedsniveauerne for de systemer, som ministeren er ansvarlig for, herunder eksempelvis adskille webadgang fra bagvedliggende informationssystemer?

Svar
Moderniseringsstyrelsen oplyser, at Datatilsynets afgørelse har givet anledning til, at Moderniseringsstyrelsen har bedt CSC om at redegøre for nogle konkrete spørgsmål, ligesom også Datatilsynets vurderinger og konklusioner fortsat indarbejdes i Moderniseringsstyrelsens arbejde med alle leverandører om opsætningen af systemerne, samt det generelle løbende IT-sikkerhedsarbejde.

Datatilsynets afgørelse har ikke generelt givet anledning til at foretage ændringer i sikkerhedsniveauerne for Finansministeriets systemer.

Finansministeriets koncern gennemfører faste risikovurderinger på sine systemer og tager derigennem stilling til, om sikkerhedsniveauet er tilstrækkeligt og balanceret i forhold til systemernes kritikalitet og det aktuelle trusselsbillede, økonomi og brugervenlighed.

Finansministeriet tilpasser således fortløbende sikkerhedsniveauet, jf. den internationale standard for informationssikkerhed ISO27001, som det er besluttet at staten skal implementere og følge.

Hvorvidt der skal etableres konkrete tekniske foranstaltninger som fx adskillelse af webadgang fra bagvedliggende informationssystemer, vurderes i den enkelte tekniske løsning ud fra systemets formål, kritikalitet, trusselsbillede samt øvrige forhold, der måtte være relevante.

Som en udløber af CSC-sagen udarbejdede Digitaliseringsstyrelsen i samarbejde med Center for Cybersikkerhed rapporten "Styrkelse af sikkerheden i statens outsourcede it-drift" i 2014. Rapporten indeholder 11 konkrete anbefalinger til statslige myndigheder om bl.a. aktivt at vurdere cyber- og informationssikkerheden specielt i de løsninger, der drives af eksterne leverandører, og gå i dialog med leverandørerne herom med henblik på at sikre, at alle leverandører gennemfører relevante tiltag for at opnå den ønskede sikkerhed i de leverede ydelser.

Digitaliseringsstyrelsen vil i februar 2016 følge op på statslige myndigheders efterlevelse og indarbejdelse af anbefalinger i rapporten som en del af porteføljeoverblikket over it-driftskontrakter.

Med venlig hilsen

Claus Hjort Frederiksen