JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 31. august 2015
Kontor: Koncernstyringskontoret
Sagsbeh: Sidse Hansen Ünal
Sagsnr.: 2015-0030-3667
Dok.: 1692874

Hermed sendes besvarelse af spørgsmål nr. 57 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 6. august 2015. Spørgsmålet er stillet efter ønske fra Pernille Skipper (EL).

Søren Pind

/

Andreas Langsted

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 57 (Alm. del) fra Folketingets Retsudvalg:

> ”Ministeren bedes redegøre for, om der er taget tiltag til ændringer hos hhv. SKAT, Økonomi- og Indenrigsministeriet og Moderniseringsstyrelsen efter Datatilsynets afgørelse i den såkaldte CSC-sag (journalnummer 2013-632-0050 om uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for).”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Skatteministeriet, Social- og Indenrigsministeriet og fra Moderniseringsstyrelsen.

Skatteministeriet har oplyst følgende:

> ”Generelt har SKAT iværksat en række tiltag med henblik på forbedring af IT-sikkerheden ved driften af ministeriets IT-systemer. Der bliver således løbende gennemført eksterne sikkerhedsaudits af CSC og andre leverandører, ligesom ministeriets sikkerhedsorganisation er blevet efterset, således at det kan sikres, at både ministeriet, styrelserne og ministeriets leverandører lever op til best practices på området.”

Social- og Indenrigsministeriet har oplyst følgende:

> Det skal indledningsvist oplyses, at Økonomi- og Indenrigsministeriet blev nedlagt den 28. juni 2015, og at CPR-området blev overført til det samme dato oprettede Social- og Indenrigsministerium.
>
> Social- og Indenrigsministeriet kan oplyse, at Det Centrale Personregister (CPR-systemet) også befandt sig på den fælles mainframe hos CSC, som omtales i Datatilsynets afgørelse af 31. juli 2015, da hackerangrebet mod CSC fandt sted i 2012.
>
> I forbindelse med en modernisering af CPR-systemet blev systemet i marts 2014 flyttet fra den pågældende fælles mainframe hos CSC til sin egen selvstændige Linux platform. Driften af denne Linux platform finder sted hos CSC.
>
> Det bemærkes, at beslutningen om at forlade den fælles mainframe til fordel for en selvstændig Linux platform ikke blev truffet som følge af hackerangrebet, men derimod som led i den modernisering af CPR-systemet, som CPR-kontoret havde iværksat, inden CPR-kontoret blev bekendt med hackerangrebet.

> Det kan tilføjes, at CPR-kontoret i øvrigt løbende har fulgt de anbefalinger, som Center for Cybersikkerhed har afgivet i forbindelse med undersøgelsen af hackerangrebet mod CSC i 2012. Der henvises herom til den daværende økonomi- og indenrigsministers besvarelse af spørgsmål 249 (Alm. Del) fra Folketingets Forsvarsudvalg, der vedhæftes."

Moderniseringsstyrelsen har oplyst følgende:

> "Generelt arbejder Moderniseringsstyrelsen løbende med IT-sikkerheden og implementerer den internationale sikkerhedsstandard ISO27001. Derudover følger Moderniseringsstyrelsen anbefalinger fra Center for Cybersikkerhed og Digitaliseringsstyrelsen, samt er i løbende dialog med CSC om disse. Moderniseringsstyrelsen har gennemført risikovurderinger og en række sikkerhedsmæssige tiltag, herunder bl.a. fulgt op på, at CSC følger anbefalingerne, som Center for Cybersikkerhed kom med i publikationen "Styrkelse af informationssikkerheden i mainframeinstallationer" i 2015.
>
> Datatilsynets afgørelse blev offentliggjort 31. juli 2015. Moderniseringsstyrelsen har læst afgørelsen og fulgt sagen. Afgørelsen 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."