JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 29. august 2014
Kontor: Sikkerheds- og Forebyggelseskontoret
Sagsbeh: Yassmina Amadid
Sagsnr.: 2014-0030-2364
Dok.: 1242190

Hermed sendes endelig besvarelse af spørgsmål nr. 1299 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 4. juli 2014. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Karen Hækkerup

/

Rikke-Louise Ørum Petersen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

**Spørgsmål nr. 1299 (Alm. del) fra Folketingets Retsudvalg:**

> ”Vil ministeren redegøre for, hvorfor man ikke reagerede på Deloittes rapport, som afslørede alvorlige sikkerhedsproblemer i CSC under hacker-angrebet, og hvorfor man ikke udførte en konsekvensanalyse, som kunne vise, at der faktisk var sket læk?”

**Svar:**

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet kan indledningsvis oplyse, at Rigspolitiet er overordnet ansvarlig for politiets centrale systemer og registre samt den information, der behandles heri. Driften af politiets centrale registre er outsourcet til CSC som ekstern driftsleverandør, og der er i overensstemmelse med persondataloven indgået databehandleraftale med CSC.
>
> Rigspolitiet fører tilsyn med Rigspolitiets driftsleverandører, herunder gennem revisionserklæringer fra uafhængig revisor, afholdelse af regelmæssige sikkerheds- og driftsstatusmøder mellem Rigspolitiet og leverandøren samt øvrig relevant opfølgning. Hertil kommer opfølgning på eventuelle it-sikkerhedshændelser.
>
> Rigspolitiet Koncern IT foretog på baggrund af den modtagne revisionserklæring fra 2011 opfølgning i overensstemmelse med det af Koncern IT på daværende tidspunkt kendte trusselsbillede og konkrete risikovurdering.
>
> På det pågældende tidspunkt var opfølgningen på revisionsanmærkninger primært objektiv kontrol og konstatering af, om de foretagne tiltag var gennemført effektivt samt fokus på opfølgning vedrørende de revisionsbemærkninger, hvor løsning endnu ikke var effektueret.
>
> Der var på det pågældende tidspunkt ikke praksis for at foretage konkret efterprøvning af mulige konsekvenser eller risici efter implementering af sikkerhedsrettelser, f.eks. i form af patches, såfremt der ikke var konstateret konkrete sikkerhedshændelser vedrørende den potentielle sårbarhed.
>
> Rigspolitiet er særlig opmærksom på de initiativer, der er nødvendige for i tilstrækkeligt omfang at øge it-sikkerheden for politiets systemer og registre med henblik på at beskytte systemer, registre og data mod trusler, herunder lækage, cybertrusler og hackerangreb.”