



JUSTITSMINISTERIET

Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 16. oktober 2014
Kontor: Sikkerheds- og Forebyg-
gelseskontoret
Sagsbeh: Rasmus Krøgh Pedersen
Sagsnr.: 2014-0030-2435
Dok.: 1288718

Hermed sendes endelig besvarelse af spørgsmål nr. 1469 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 28. august 2014. Spørgsmålet er stillet efter ønske fra Karsten Lauritzen (V).

Mette Frederiksen

/

Rikke-Louise Ørum Petersen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1469 (Alm. del) fra Folketingets Retsudvalg:

”Under henvisning til oversendt fortrolig rapport om hackerangrebet mod CSC, REU alm. del - bilag 356, bedes ministeren udskille og oversende de dele af rapporten, som ikke er fortrolige. Såfremt ministeren betragter hele rapporten som fortrolig, bedes ministeren redegøre for dette, og afsnit for afsnit redegøre for, hvorfor afsnittet er fortroligt. Særligt bedes ministeren forklare, hvorfor kun dele af den foreløbige rapport var fortrolig.”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Politiets Efterretningstjeneste. I den anledning har efterretningstjenesten sammen med Center for Cybersikkerhed udarbejdet en delvis afklassificeret version af den i spørgsmålet omtalte rapport om sikkerhedsbrud hos CSC.

Den afklassificerede version af rapporten vedlægges. Det bemærkes i den forbindelse, at de afsnit, som fortsat er klassificeret til tjenestebrug, er dækket med sorte markeringer.

Politiets Efterretningstjeneste har endvidere oplyst, at de afsnit, som fortsat er klassificeret, indeholder oplysninger, hvis hemmeligholdelse vurderes at være af væsentlig betydning for statens sikkerhed, jf. offentlighedslovens § 31, og nødvendig til beskyttelse af væsentlige hensyn til forebyggelse af lovovertrædelser, jf. offentlighedslovens § 33, nr. 1. Det vurderes således, at der er tale om oplysninger vedrørende statslige myndigheders it-infrastruktur, angrebsteknikker og sårbarheder ved it-systemer, som i sig selv eller sammenholdt med andre oplysninger vil kunne anvendes til eventuelle fremtidige hackerangreb.