JUSTITSMINISTERIET
Administrationsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 31. august 2015
Kontor: Koncernstyringskontoret
Sagsbeh: Sidse Hansen Ünal
Sagsnr.: 2015-0030-3668
Dok.: 1692885

Hermed sendes besvarelse af spørgsmål nr. 58 (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. 58 (Alm. del) fra Folketingets Retsudvalg:

> ”Ministeren bedes redegøre for, hvorvidt problemerne omkring manglende separation/at flere systemer deler mainframe i de tidligere analyser af sikkerheden hos CSC er blevet påpeget af enten PET, CfCs eller andre, samt om der ved disse mange gennemgange af sikkerheden hos CSC's fællesoffentlige mainframe er blevet påpeget problemer ift. webadgangen i Moderniseringsstyrelsens system.”

Svar:

Datatilsynet offentliggjorde den 31. juli 2015 tilsynets udtalelse om ”Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for”. I udtalelsen kritiserer Datatilsynet blandt andet Rigspolitiet for, at Rigspolitiet ikke har efterlevet kravene om sikkerhed i persondataloven og Schengen-konventionen. Datatilsynet efterspørger i udtalelsen endvidere en række konkrete svar fra Rigspolitiet i relation til CSC-sagen.

Rigspolitiet har på den baggrund den 24. august 2015 fremsendt en redegørelse til Datatilsynet, hvori Rigspolitiet besvarer de pågældende spørgsmål. Samtidig redegør Rigspolitiet for de gennemførte initiativer med henblik på at styrke beskyttelsen af borgernes følsomme personoplysninger.

Datatilsynet har den 27. august 2015 kvitteret for modtagelsen af Rigspolitiets redegørelse. Datatilsynet vurderer, at Rigspolitiet har besvaret Datatilsynets spørgsmål, ligesom Rigspolitiet i overordnede træk har orienteret Datatilsynet om de tiltag, som er gennemført siden sikkerhedshændelsen i 2012. Datatilsynet oplyser afslutningsvist, at tilsynet herefter ikke foretager sig yderligere i sagen.

Rigspolitiets redegørelse samt Datatilsynets brev af den 27. august 2015 er vedlagt denne besvarelse.

Det kan endvidere oplyses, at Rigspolitiet er den overordnede dataansvarlige for politiets centrale systemer og registre, herunder de oplysninger der behandles heri. Det er således Rigspolitiets ansvar at sikre, at politiets data behandles sikkerhedsmæssigt forsvarligt – uanset om data måtte ligge hos en ekstern leverandør. Imidlertid er personalemæssige spørgsmål et internt anliggende.

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet udtalelser fra Rigspolitiet og Politiets Efterretningstjeneste.

Rigspolitiet har oplyst følgende:

> ”Rigspolitiet kan indledningsvis bemærke, at CSC driver en række systemer, herunder bl.a. Schengen-informationssystemet for Rigspolitiet og andre danske myndigheder. Det har CSC gjort, siden virksomheden købte Datacentralen fra den danske stat i 1996. Rigspolitiet har løbende en tæt dialog med CSC om driften af politiets systemer.
>
> Angrebet mod CSC var foretaget af en særdeles kompetent hacker, som formåede at udnytte to uopdagede huller i CSC's systemer. Hackeren blev i juni 2015 kendt skyldig ved Østre Landsret for hacking og hærværk.
>
> Rigspolitiet er den overordnede dataansvarlige for politiets centrale systemer og registre, herunder de oplysninger der behandles heri. Det er således Rigspolitiets ansvar at sikre, at politiets data behandles sikkerhedsmæssigt forsvarligt – uanset om data måtte ligge hos en ekstern leverandør.
>
> Oplysninger i politiets it-systemer er undergivet den til enhver tid gældende lovgivning samt interne fastsatte retningslinjer, herunder politiets IT-sikkerhedshåndbog.
>
> Rigspolitiet modtog den 31. juli 2015 Datatilsynets udtalelse vedrørende uvedkommendes adgang til personoplysninger. Rigspolitiet har som opfølgning herpå afholdt et møde med Datatilsynet, hvor Rigspolitiet mundtligt har besvaret de spørgsmål, som Datatilsynet har rejst i udtalelsen. Rigspolitiet har samtidig over for Datatilsynet beklaget, at Datatilsynet ikke tidligere har modtaget tilstrækkeligt præcise svar. Rigspolitiet tager kritikken fra Datatilsynet meget alvorligt og vil fremover sikre, at Datatilsynet rettidigt får præcise svar på deres spørgsmål.
>
> I forhold til den konkrete sag har Rigspolitiet iværksat en række foranstaltninger, der vanskeliggør lignende angreb:
>
> - Den omtalte webserver er nedlagt
> - Opsætningen omkring Schengen-informationssystemet er grundlæggende ændret, så datafiler, som den hackeren kopierede, ikke længere genereres i systemet.
> - Sikkerhedsniveauet for flytning af data til internettet er højnet.
>
> Sikkerheden i forhold til den tekniske arkitektur på mainframemiljøet har forud for sikkerhedsbristen ikke været drøftet mellem Rigspolitiet og Justitsministeriet.

Efter sikkerhedsbruddet i 2012 er det blevet påpeget af PET, at manglende fysisk separation i mainframemiljøet kan udgøre et informationssikkerhedsmæssigt problem, hvis der ikke sker differentiering af sikkerhedsniveauet på anden vis. Rigspolitiet har på den baggrund gennemført en række tiltag for at sikre, at der er den nødvendige isolation, adskillelse og tilstrækkeligt forsvar i dybden. Disse tiltag baserer sig på anbefalinger fra PET, Center for Cybersikkerhed (CfCS), og en uafhængig it-revisor. De konkrete gennemførte tiltag er gennemgået nærmere i den vedlagte redegørelse til Datatilsynet.

Det er Rigspolitiets vurdering, at den tekniske arkitektur for det omhandlende mainframemiljø ikke er en hindring for implementering af anerkendte principper for sikkerhed – en vurdering som også fremgår af sikkerhedsanbefalingen fra CfCS vedrørende styrkelse af informationssikkerheden i mainframe-installationer (januar 2015).

Rigspolitiet har ikke fundet konkret information om, hvem der traf beslutning om etablering af den pågældende webserver. Det fremgår af de svar, som CSC har fremsendt i forbindelse med Datatilsynets undersøgelse, at webserveren er etableret for en anden statslig kunde. Det er sket på et tidspunkt, hvor der ikke har været anvendt de standardiserede processer for etablering og kontrol af leverandørservices, som anvendes i dag.

Rigspolitiet har derfor også under de aktuelle forhandlinger med CSC understreget, at Rigspolitiet skal inddrages, når CSC foretager ændringer, der kan påvirke Rigspolitiets it-miljø hos CSC.

Rigspolitiet har herudover iværksat et forhandlingsforløb med CSC, som bl.a. skal sikre en styrkelse af de nødvendige processer og styringsredskaber for it-sikkerhed, og at disse tydeliggøres i kontraktsgrundlaget.

Rigspolitiet vil samtidig følge den teknologiske udvikling med henblik på løbende at iværksætte relevante forebyggende tiltag i forhold til det aktuelle risikobillede."

Politiets Efterretningstjeneste har oplyst følgende:

"PET blev den 5. juni 2013 af Rigspolitiet bedt om at forestå en undersøgelse af sagen om hackerangrebet mod CSC med henblik på dels at afdække omfanget af og årsagerne til sikkerhedsbruddet, dels at komme med fremadrettede sikkerhedsanbefalinger.

PET afgav den 19. juli 2013 en indledende rapport om hackerangrebet på politiets systemer hos CSC, som indeholdt enræk-

ke indledende anbefalinger rettet mod at forbedre sikkerheden for politiets systemer.

Den 12. juni 2014 afgav PET sine endelige anbefalinger til forbedring af sikkerheden for politiets systemer. Anbefalingerne, der bl.a. vedrørte CSC's mainframemiljø, er optrykt som bilag 2 til den rapport fra Center for Cybersikkerhed og PET om sikkerhedsbruddet hos CSC, som i delvis afklassificeret form blev sendt til Folketingets Retsudvalg ved Justitsministeriets svar af 16. oktober 2014 på spørgsmål nr. 1469 (Alm. del) fra udvalget.

PET har ikke forud for hackerangrebet gennemgået CSC's mainframemiljø. Det bemærkes i den forbindelse, at mainframemiljøet ikke behandler klassificerede oplysninger og således falder uden for den godkendelses- og kontrolvirksomhed, som PET i egenskab af national it-sikkerhedsmyndighed på Justitsministeriets område udøver i henhold til cirkulæret om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt information af sikkerhedsmæssig beskyttelse i øvrigt (cirkulære nr. 10338 af 17. december 2014, som afløste cirkulære nr. 204 af 7. december 2001)."