JUSTITSMINISTERIET

Dato: 25. juni 2013
Dok.: 801768

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmål W og X fra Folketingets Kommunaludvalg den 28. juni 2013 kl. 8.00

Samrådsspørgsmål W:

"Vil ministrene redegøre for forløbet i forbindelse med at politiets kørekortregister er blevet hacket, og hvilke initiativer ministrene i den sammenhæng planlægger at tage efterfølgende?"

Samrådsspørgsmål X:

"Vil ministeren i forbindelse med afsløringen (6. juni 2013) af hackerangrebet mod politiets centrale registre redegøre for, hvorvidt de ansvarlige myndigheder har levet op til deres tilsynspligt, og i hvilket omfang den konkrete sag giver ministeren anledning til at overveje, om tilsynskravene skal skærpes?"

[Indledning]

1. Temaet for dagens samråd er hacker-angrebet mod IT-leverandøren CSC.

I spørgsmål W anmodes økonomi- og indenrigsministeren og jeg om en redegørelse for forløbet i forbindelse med, at politiets kørekortregister er blevet hacket, og hvilke initiativer vi i den sammenhæng planlægger at tage efterfølgende.

Herudover ønskes med spørgsmål X, at jeg redegør for, hvorvidt de ansvarlige myndigheder har levet op til deres tilsynspligt, og i hvilket omfang den konkrete sag giver anledning til at overveje, om tilsynskravene skal skærpes.

2. Jeg forstår godt, hvis sagen giver anledning til bekymring.

Lad mig derfor starte med at slå fast, at regeringen tager sagen meget alvorlig. Det samme gælder alle involverede myndigheder. Jeg kan derfor også forsikre om, at alle nødvendige ressourcer bliver sat ind for at håndtere sagen og de sikkerhedsmæssige spørgsmål, som den rejser.

Jeg vil besvare de stillede samrådsspørgsmål på den måde, at jeg først giver et kronologisk overblik over forløbet – så langt som den igangværende efterforskning tillader det.

Derefter vil jeg redegøre for de ansvarlige myndigheders tilsynspligt, og til sidst vil jeg komme ind på de initiativer, som den konkrete hackersag giver anledning til.

[Redegørelse for forløbet: august 2012 - april 2013]

3. Min redegørelse for forløbet bygger på oplysninger fra Rigspolitiet, som også indgår i det svar på spørgsmål 904 fra Folketingets Retsudvalg, som jeg afgav i går.

Rigspolitiet har i den forbindelse understreget, at der er tale om en igangværende efterforskning med enorme datamængder, som dansk politi løbende modtager fra svensk politi og herefter analyserer, og at det derfor ikke kan udelukkes, at billedet senere ændrer sig.

Om sagens forløb har Rigspolitiet oplyst, at en svensk statsborger i slutningen af august 2012 blev anholdt i Cambodja, og at den pågældende i starten af september 2012 blev udleveret til Sverige og fængslet.

Det skete i forbindelse med efterforskningen af en sag om hacking og med henblik på afsoning af en dom om krænkelse af ophavsretsloven.

Den svenske efterforskning omhandlede blandt andet hacking af et pengeinstituts it-systemer. Og oplysninger fra efterforskningen pegede på, at også danske konti i pengeinstituttet havde været anvendt til kriminalitet i den sammenhæng.

Rigspolitiet var på den baggrund i dialog med svensk politi, der oplyste, at også danske hjemmesider kunne være forsøgt hacket.

4. I midten af januar 2013 modtog Rigspolitiet fra svensk politi uddrag af en række logfiler, som svensk politi var kommet i besiddelse af i forbindelse med deres efterforskning.

Rigspolitiets Nationale IT-efterforskningssektion – i daglig tale NITES – gennemgik i slutningen af februar 2013 materialet, som var modtaget fra svensk politi.

Og på baggrund af denne gennemgang konstaterede NITES, at der havde været uautoriseret adgang til politiets data fra et mainframesystem hos CSC.

Straks herefter holdt Rigspolitiet et møde med CSC, og en nærmere undersøgelse blev iværksat hos CSC med deltagelse af Rigspolitiet. Det skete med henblik på at identificere den nærmere karakter af sårbarheden i systemet og sikre, at denne blev lukket.

5. Rigspolitiet anmodede i begyndelsen af marts måned 2013 om en skriftlig redegørelse fra CSC samt sikring af data med henblik på efterforskningen.

CSC afrapporterede herefter skriftligt til Rigspolitiet ved flere lejligheder og oplyste i den forbindelse, at den sårbarhed i systemet, som havde været benyttet til at opnå den uautoriserede adgang, var blevet identificeret og lukket.

CSC oplyste endvidere, at såkaldte "bagdøre" til systemet var identificeret og fjernet, og at der ikke var fundet tegn på, at der havde været direkte adgang til Kriminalregisteret eller til andre registre på systemet.

Det var desuden CSC's vurdering, at det med stor sandsynlighed kunne udelukkes, at der var ændret, tilføjet eller slettet i oplysningerne i registrene.

Med henblik på at verificere CSC's oplysninger iværksatte Rigspolitiet en supplerende selvstændig undersøgelse og fortsatte sideløbende her-

med undersøgelserne af det tilvejebragte materiale, som er særdeles omfattende.

6. Københavns Politi har i marts 2013 med bistand fra NITES indledt en strafferetlig efterforskning.

Rigspolitiet modtog i april 2013 en CD-rom med materiale, som var sikret fra den svenske statsborgers computer i forbindelse med anholdelsen.

Rigspolitiet undersøgte herefter materialet og sammenholdt det med oplysninger fra CSC. Rigspolitiet konstaterede, at materialet bl.a. indeholdt en række talkoder og navne på fortrinsvis udenlandske statsborgere.

Efter en nærmere undersøgelse konstaterede Rigspolitiet endvidere, at materialet indeholdt ca. 1,2 millioner såkaldte "records" vedrørende efterlysninger i Schengen-informationssystemet – også kaldet SIS.

Rigspolitiet undersøger stadig materialet og får på den måde øget indsigt i omfanget og karakteren af den svenske statsborgers aktiviteter på mainframen hos CSC.

[Redegørelse for forløbet: maj-juni 2013]

7. Rigspolitiet vurderede i midten af maj at have fornøden klarhed over episoden.

Den 17. maj 2013 orienterede Rigspolitiet derfor telefonisk Datatilsynet om sikkerhedsbristen.

Justitsministeriet blev orienteret telefonisk den 21. maj og skriftligt den 24. maj 2013.

Den 29. maj 2013 orienterede Rigspolitiet Justitsministeriet om, at undersøgelser havde vist, at der den 8. april 2012 havde været aktivitet mod CPR-registerets miljø på mainframen fra politiets miljø på mainframen.

Rigspolitiet underrettede den 30. maj 2013 telefonisk Økonomi- og Indenrigsministeriet om aktiviteten.

Datatilsynet blev endvidere på ny orienteret om sagen den 31. maj 2013.

8. Som følge af den strafferetlige efterforskning afsagde Københavns Byret den 31. maj 2013 fængslingskendelse med henblik på udlevering af den svenske statsborger til Danmark.

Den 3. juni 2013 orienterede Rigspolitiet Kommissionen om sagen i relation til oplysningerne i Schengen-informationssystemet (SIS).

Københavns Politi foretog den 5. juni 2013 anholdelse af en dansk formodet medgerningsmand. Der blev samtidig foretaget ransagning på flere adresser.

Den anholdte formodede medgerningsmand blev den 6. juni 2013 fremstillet i grundlovsforhør for lukkede døre og varetægtsfængslet i foreløbig 4 uger.

9. Rigspolitiet, PET og Københavns Politi orienterede ved et fælles pressemøde samme dag offentligheden om sagen.

Efterfølgende holdt jeg samme dag ligeledes et kort pressemøde om sagen.

Rigspolitiet orienterede endvidere den 6. juni 2013 Schengen-landene, Rådssekretariatet, Kommissionen og den Europæiske Tilsynsførende for Databeskyttelse om sagen.

[Tilsyn med politiets centrale registre]

Efter denne redegørelse for forløbet vil jeg nu komme med nogle bemærkninger om de relevante tilsynsmyndigheder i forhold til hackerangrebet. Lad mig starte med Rigspolitiet.

10. Rigspolitiet er dataansvarlig for indholdet af politiets centrale registre og har i overensstemmelse med persondataloven indgået en såkaldt databehandleraftale med CSC.

Som dataansvarlig er Rigspolitiet overordnet ansvarlig for CSC's behandling af personoplysninger. Det indebærer, at Rigspolitiet skal sikre sig, at CSC kan træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Og Rigspolitiet skal påse, at dette også rent faktisk sker.

Rigspolitiet har i forbindelse med sit tilsyn hos CSC modtaget årlige revisionserklæringer fra en uafhængig revisor. Revisionserklæringen for kalenderåret 2012 er udstedt i marts 2013.

Som opfølgning på de nævnte revisionserklæringer og som led i det generelle tilsyn afholdes der sikkerhedsmøder mellem CSC og Rigspolitiet.

Der afholdes også løbende driftsstatusmøder og andre møder, når dette er relevant, herunder som opfølgning på sikkerhedshændelser.

11. Ud over Rigspolitiet fører Datatilsynet tilsyn med politiets centrale registre. Det sker som led i tilsynets generelle tilsynsvirksomhed i relation til behandling af personoplysninger omfattet af persondataloven.

Datatilsynet har i anledning af samrådet oplyst, at tilsynet med politiets centrale registre sker i forbindelse med behandling af konkrete klager fra borgere eller som egen drift undersøgelser.

Og Datatilsynet har gennemført flere inspektionsbesøg hos Rigspolitiet siden persondatalovens ikrafttræden i 2000.

Datatilsynet har endvidere oplyst, at tilsynet med Rigspolitiets centrale registre typisk udføres med fokus på at kontrollere, at registreringen af personoplysninger sker i overensstemmelse med reglerne i persondataloven og eventuel anden relevant lovgivning. Tilsynet undersøger om reglerne om registreredes rettigheder overholdes.

Datatilsynet foretager derimod ikke en mere omfattende it-revision eller en fuldstændig gennemgang af etablerede sikkerhedsforanstaltninger.

For så vidt angår det konkrete hackerangreb har Datatilsynet oplyst, at tilsynet har anmodet Rigspolitiet om en redegørelse for det skete og udbedt sig oplysninger om en række forhold.

12. I tillæg til de opgaver, som jeg netop har nævnt, er Datatilsynet national tilsynsmyndighed i relation til behandling af personoplysninger, der sker i den danske del af en række internationale informationssystemer, som Danmark deltager i. Dette gælder eksempelvis SIS, altså Schengen-informationssystemet.

I den forbindelse deltager Datatilsynet i de fælles tilsynsaktiviteter, som gennemføres i de samarbejdsfora, som er etableret på EU-niveau.

I forhold til SIS iværksættes og koordineres fælles tilsynsaktiviteter af Den Fælles Tilsynsmyndighed for Schengen.

Datatilsynet har oplyst, at en væsentlig del af tilsynsaktiviteten i forhold til SIS har været at deltage i sådanne undersøgelser.

Fokus for undersøgelserne har været kontrol af overensstemmelse mellem landenes indberetninger til SIS og Schengen-konventionens bestemmelser.

Datatilsynet har senest i 2011 gennemført inspektionsbesøg hos Rigspolitiet med særlig fokus på SIS. Herudover indgik databeskyttelse i den Schengen-evaluering af Danmark, som blev gennemført i 2011.

Rigspolitiet har i øvrigt oplyst, at et Schengen-inspektionshold, bestående af eksperter fra Schengen-lande, Rådssekretariatet og Kommissionen, aflagde besøg i Danmark så sent som i oktober 2012.

Inspektionsholdet aflagde blandt besøg hos CSC, hvor en række sikkerhedsmæssige forhold i forbindelse med CSC's drift af SIS blev gennemgået.

Og det er værd at understrege, at inspektionsholdet ikke fremkom med bemærkninger eller anbefalinger i forhold til CSC i sin efterfølgende evalueringsrapport.

Jeg kan i øvrigt nævne, at Rigspolitiet i juli måned vil deltage i et møde med de øvrige Schengen-lande, sikkerhedseksperter for EU-agenturerne og Europol samt den Europæiske Tilsynsførende for Databeskyttelse. Formålet med mødet er at give Rigspolitiet mulighed for at redegøre for sagens forløb og udvikling samt at diskutere fremadrettede sikkerhedstiltag.

13. I forbindelse med tilsynet med politiets registre skal en sidste myndighed nævnes. Det drejer sig om PET.

Efterretningstjenesten har til opgave at forebygge, efterforske og modvirke foretagender og handlinger, der udgør eller vil kunne udgøre en fare for Danmark som et selvstændigt, demokratisk og sikkert samfund.

PET er desuden national IT-sikkerhedsmyndighed for Justitsministeriets område, herunder altså for politiet og anklagemyndigheden.

Som led i PET's rolle som national IT-sikkerhedsmyndighed for Justitsministeriets område rådgiver PET løbende politiet og anklagemyndigheden. PET godkender også – i overensstemmelse med reglerne i det såkaldte sikkerhedscirkulære – IT-systemer, hvor klassificerede oplysninger bevares og behandles.

Det mainframe-anlæg hos CSC, som var udsat for hacker-angreb, er imidlertid ikke omfattet af PET's godkendelses- og kontrolvirksomhed. Det skyldes, at anlægget ikke behandler klassificerede oplysninger.

PET er løbende i dialog med politi og anklagemyndighed om håndtering af følsomme oplysninger.

I 2011 tog PET endvidere initiativ til et projekt, der har til formål at sikre et passende og ensartet beskyttelsesniveau for følsomme oplysninger, der behandles og opbevares af politi og anklagemyndighed.

PET har løbende bidraget med ekspertviden og rådgivning til projektet, der er forankret i Rigspolitiet. Projektets indledende anbefalinger er forelagt Rigspolitiets direktion i foråret 2013.

Desuden kan jeg nævne, at PET har iværksat en kortlægning af, hvordan trafikmonitorering og logning på politiets og anklagemyndighedens IT-systemer kan styrkes.

[Undersøgelser på Justitsministeriets område i anledning af hackersagen]

14. Som mine bemærkninger viser, er der allerede i dag et omfattende system, som fører tilsyn med politiets registre. Et naturligt og relevant spørgsmål er derfor, hvordan angrebet mod CSC kunne finde sted.

Det er for mig at se helt centralt at få fastlagt, hvordan noget sådant kunne ske, og hvordan vi kan modvirke, at det sker igen.

Der arbejdes da også målrettet på at undersøge omfanget af og årsagerne til sikkerhedsbruddet og sikre, at der træffes de nødvendige sikkerhedsforanstaltninger.

Det er PET, som står i spidsen for dette arbejde, og det foregår i tæt samarbejde med navnlig Center for Cybersikkerhed under Forsvarets Efterretningstjeneste.

Der vil blive udarbejdet en rapport om resultaterne af dette arbejde, når det er tilendebragt.

[Afrunding]

16. Som jeg indledte med at sige, er der tale om et angreb, som regeringen ser med største alvor på. Det fremstår yderst professionelt.

Samtidig er det afgørende, at sikkerheden omkring offentlige myndigheders registre er i orden. Det gælder ikke mindst politiets registre og andre centrale myndighedsregistre.

Såvel efterforskning som undersøgelser pågår stadig. Jeg kan derfor ikke i dag sige noget endegyldigt om, hvilke foranstaltninger hackerangrebet kommer til at medføre.

Som nævnt vil der blive afgivet en redegørelse om omfanget af og årsagerne til sikkerhedsbruddet og sikkerhedsanbefalingerne i den anledning, når undersøgelsen heraf er færdig.

Men jeg håber, at det siger sig selv, at relevante sikkerhedstiltag vil blive iværksat løbende, efterhånden som der viser sig behov herfor.

Når det gælder efterforskningen, så er der tale om en omfattende og kompleks efterforskning, som kommer til at tage tid. Man kan altså langt fra i dag sige noget om, hvordan efterforskningen ender.

Men jeg hæfter mig ved, at politidirektøren for København i forgårs udtalte, at politiet indtil videre ikke har kunnet påvise, at der skal være foretaget ændringer i systemerne af de personer, som er brudt ind.

Og der er ifølge politidirektøren desuden endnu ikke set tegn på, at de fortrolige oplysninger fra registrene er blevet lækket til uvedkommende.

Lad mig slutte - som jeg begyndte - med at gøre det klart, at alle nødvendige ressourcer er blevet og fortsat vil blive sat ind for at håndtere sagen.

Sagen tages meget alvorligt af alle involverede myndigheder.

Tak.