JUSTITSMINISTERIET
Administrationsafdelingen

Dato: 31. august 2015
Kontor: Koncernstyringskontoret
Sagsbeh: Sidse Hansen Ünal
Sagsnr.: 2015-0035-0304
Dok.: 1711196

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmål A fra Folketingets Retsudvalg den 1. september 2015

Det talte ord gælder

Samrådsspørgsmål A:

"På baggrund af Datatilsynets afgørelse i sagen vedrørende uvedkommendes adgang til personoplysninger, som Rigspolitiet er dataansvarlig for (journalnummer 2013-632-0050), bedes ministeren redegøre for, hvilke initiativer ministeren vil tage for at imødekomme den skarpe kritik af Rigspolitiet, som Datatilsynet er kommet med, så det fremadrettet sikres, at myndighederne behandler og håndterer personfølsomme oplysninger i overensstemmelse medlovgivningen. Dertil bedes ministeren redegøre for, hvordan Datatilsynet og tilsynets arbejde fremover kan styrkes.?"

Spørgsmålene er stillet efter ønske fra Lisbeth Bech Poulsen (SF).

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

[Indledning]

1. Indledningsvist vil jeg gerne sige tak for denne mulighed for at redegøre for, hvilke initiativer Rigspolitiet har taget for at styrke it-sikkerheden på baggrund af CSC-sagen.

Dette er jo en sag, som af gode grunde optager mange folk. På Justitsministeriets område håndterer vi dagligt mange følsomme personoplysninger, og vi har derfor et særligt ansvar for at sikre en høj grad af beskyttelse af de personlige oplysninger om borgerne.

Det er naturligvis også en sag, jeg ser på med stor alvor.

[Om selve hackerangrebet]

2. I 2012 skete der desværre det, at en række it-systemer blev udsat for et hackerangreb. Angrebet omtales typisk som CSC-sagen, da de hackede systemer blev drevet af CSC.

Angrebet blev rettet mod en mainframe, hvor der lå it-systemer, som tilhørte Rigspolitiet, SKAT, Økonomi- og Indenrigsministeriet og Moderniseringsstyrelsen.

3. Ved hackerangrebet fik hackeren adgang til blandt andet Rigspolitiets systemer, herunder Schengen-informationssystemet, Kriminalregisteret og Kørekortregisteret.

Hackeren skaffede sig adgang til it-systemerne via en adgang, som kunne tilgås direkte fra internettet.

Ved at udnytte to ukendte sårbarheder opnåede hackeren indledningsvis adgang til mainframen. Derefter øgede han sine beføjelser og fik på den måde mere kontrol med mainframen.

Forløbet førte til, at hackeren opnåede ubegrænset adgang til alle data og dermed adgang til at kopiere, slette, ændre og tilføje data.

Endvidere opnåede hackeren adgang til at afbryde logningen af sine aktiviteter, hvorefter han kunne bevæge sig anonymt i it-systemerne. Netop logning kan ellers bruges til at følge en brugers digitale fodspor.

Det er konstateret, at hackeren har udtrukket en mængde data, herunder en kopi af en fil indeholdende oplysninger om alle efterlyste personer i Schengen-området.

4. For god ordens skyld kan jeg oplyse, at den svenske statsborger, der stod bag hackerangrebet, blev anholdt i Cambodja og siden udleveret til Danmark, hvor han ved Østre Landsret i juni 2015 blev dømt for hacking og hærværk.

[Hvorfor var det overhovedet muligt?]

5. Man kan spørge sig selv, hvorfor hackerangrebet overhovedet var muligt?

For det første skaffede hackeren sig adgang til it-systemerne via en adgang, som kunne tilgås direkte fra internettet.

For det andet blev angrebet mod CSC foretaget af en særdeles kompetent hacker, der formåede at udnytte to sikkerhedsbrister i CSC's systemer.

Og for det tredje var der sikkerhedsmæssige forhold ved politiets informationssystemer, der ikke var gode nok.

Det er selvfølgelig beklageligt.

[Datatilsynets udtalelse]

6. Den 31. juli 2015 offentliggjorde Datatilsynet en udtalelse om CSC-sagen.

I udtalelsen gennemgår Datatilsynet de forhold, der muliggjorde hackerangrebet. Datatilsynet fokuserer særligt på forholdene ved Schengen-informationssystemet. Dette informationssystem er en database, der bl.a. indeholder oplysninger om eftersøgte og forsvundne personer eller personer under overvågning.

Datatilsynet finder det i udtalelsen overordentligt kritisabelt, at Rigspolitiet ikke har efterlevet bestemmelserne om sikkerhed i persondataloven og Schengen-konventionen.

Således kritiserer Datatilsynet bl.a., at Rigspolitiet ikke havde truffet de nødvendige tekniske og organisatoriske foranstaltninger for at hindre, at uvedkommende ville kunne tilgå følsomme personoplysninger i Schengen-systemet.

Endelig finder Datatilsynet sagens langstrakte forløb meget beklageligt, og det er Datatilsynets opfattelse, at Rigspolitiet i væsentlig grad har bidraget til det meget lange forløb. Datatilsynet har således oplyst, at tilsynet under forløbet stillede de samme spørgsmål flere gange, og i flere tilfælde har tilsynet fået uklare eller ufyldestgørende svar.

Det er naturligvis en kritik, både jeg og Rigspolitiet tager særdeles alvorligt.

7. Som opfølgning på kritikken stiller Datatilsynet endvidere Rigspolitiet en række konkrete spørgsmål.

Jeg skal understrege vigtigheden af, at Datatilsynet skal modtage rettidige og præcise svar. Det er meget beklageligt, at det ikke er sket. Jeg forventer, at der fremover bliver rettet op herpå.

Jeg kan i den forbindelse oplyse, at Rigspolitiet [den 24. august 2015] har fremsendt en redegørelse til Datatilsynet indeholdende svar på de stillede spørgsmål.

Datatilsynet har den 27. august 2015 kvitteret for modtagelsen af Rigspolitiets redegørelse. Jeg kan med tilfredshed konstatere, at Datatilsynet vurderer, at Rigspolitiet har besvaret tilsynets 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.

Både Rigspolitiets redegørelse samt Datatilsynets brev er oversendt til Folketinget i forbindelse med besvarelsen af spørgsmål 53-58 fra Retsudvalget.

[Hvordan der følges op på Datatilsynets skarpe kritik af Rigspolitiet]

8. I samrådsspørgsmålet spørges der til, hvilke initiativer ministeren vil tage for at imødekomme kritikken af Rigspolitiet.

CSC-sagen er særdeles beklagelig. Men jeg kan også konstatere, at Rigspolitiet efterfølgende har behandlet sagen med den fornødne alvor.

Jeg har således noteret mig, at Rigspolitiet siden sikkerhedshændelsen i 2012 har iværksat en række initiativer, der

skal højne sikkerheden og dermed mindske risikoen for et lignende angreb.

9. Tiltagene er iværksat på baggrund af de analyser og anbefalinger, der er udarbejdet af særligt PET og Center for Cybersikkerhed.

Rigspolitiet og CSC har grundigt analyseret og prioriteret disse rapporters anbefalinger, og alle kritiske tekniske anbefalinger er blevet implementeret.

De iværksatte initiativer er nærmere beskrevet i Rigspolitiets redegørelse til Datatilsynet, så jeg vil ikke gå i detaljen med dem i dag, da flere af forholdene også er af en meget teknisk karakter. [Såfremt der måtte være spørgsmål til de mere tekniske forhold, vil jeg meget gerne svare skriftligt herpå].

Jeg kan overordnet oplyse, at følgende forhold er ændret:

- Den webserver, der gjorde det muligt for hackeren at tilgå mainframen fra internettet, er blevet nedlagt.
- De to sårbarheder, som blev benyttet i forbindelse med angrebet, er blevet lukket.
- Opsætningen omkring Schengen-informationssystemet er grundlæggende ændret, så datafiler, som hackeren kopierede, ikke længere skabes i systemet.
- Sikkerhedsniveauet for flytning af data til internettet er højnet.
- Logning og monitorering er skærpet.

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

Politiet har således allerede iværksat initiativer for at sikre et tidssvarende it-sikkerhedsniveau og implementerer derudover løbende tiltag, der skal sikre, at politiets følsomme personoplysninger bliver håndteret på betryggende vis og i henhold til lovgivningen.

10. Rigspolitiet har orienteret mig om, at de definerer sikkerhedsniveauet og kontrollerer efterlevelsen heraf i henhold til anbefalinger fra blandt andre Center for Cybersikkerhed og PET.

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

11. Samlet set er det Rigspolitiets vurdering, at de grundlæggende kritikpunkter i Datatilsynets afgørelse vedrørende sikkerheden er håndteret med den lange række af tiltag, som Rigspolitiet har taget siden hændelsen i 2012.

Situationen omkring driften hos CSC i dag er således en helt anden end før angrebet i 2012.

[Hvordan kan Datatilsynet og tilsynets arbejde styrkes?]

12. Udvalget beder mig også redegøre for, hvordan Datatilsynet og tilsynets arbejde fremover kan styrkes.

Jeg vil i den forbindelse starte med at sige, at databeskyttelse er et område, som regeringen tager yderst alvorligt.

Det er et område af stigende betydning som følge af samfundsudviklingen. Et enigt Retsudvalg har med sin beretning

om databeskyttelse fra januar i år også bekræftet, at det er et område, der er bred enighed om at prioritere.
13. Jeg har imidlertid ikke i dag de konkrete svar på, hvilke nærmere initiativer der skal tages på området. Det håber jeg, at udvalget har forståelse for.

Som også Retsudvalgets beretning fra januar viser, så er der mange forskellige spørgsmål i spil.

Jeg vil snarest muligt [i løbet af september] sende et brev til udvalget med regeringens umiddelbare svar på, hvilke kommentarer beretningen giver anledning til.

14. Som det endvidere er udvalget bekendt, så bad den daværende justitsminister i foråret 2014 sine embedsmænd sammen med Erhvervs- og Vækstministeriet om at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger mv.

Kortlægningsarbejdet er fortsat i gang, men det forventes afsluttet snarest. [I starten af oktober.]

Kortlægningen vil så skulle danne udgangspunkt for en politisk drøftelse af området. Og den politiske drøftelse vil også omfatte spørgsmålet om styrkelse af Datatilsynet, som der spørges til her i dag.

Der har jo de seneste år været en række sager, som viser nogle udfordringer med datasikkerheden rundt omkring – den konkrete sag om hackerangrebet mod CSC og Rigspolitiet er desværre et af eksemplerne herpå. Og det skal vi selvfølgelig se på, om vi kan gøre noget ved.

Og det er klart, at en styrkelse af Datatilsynet er noget af det, som vi muligvis kommer til at se på.

15. Det hører også med til billedet, at der i øjeblikket i EU foregår forhandlinger om en ny forordning om databeskyttelse. Forordningen vil bl.a. skulle regulere Datatilsynets beføjelser. Det må man selvfølgelig tage i betragtning i forbindelse med de videre overvejelser om, hvorvidt der skal gennemføres nye initiativer på området.

Forordningen forventes vedtaget inden jul.

Og som sagt, så er det her et område, denne regering taget yderst alvorligt. Bl.a. gør vi i Justitsministeriet det, at vi i forbindelse med en omorganisering af ministeriets struktur opretter et nyt Databeskyttelseskontor. Det skal bl.a. ses som en opprioritering af området.

Jeg ser meget frem til det videre arbejde med udvalget på dette område.

[Afsluttende bemærkninger]

16. Afslutningsvist vil jeg runde af med at sige, at hackerangrebet mod CSC har bidraget til at understrege vigtigheden af it-sikkerhed i offentlige it-systemer.

Når store mængder følsomme personoplysninger gemmes på samme sted, så kan konsekvenserne af en sikkerhedsbrist være enorme.

CSC-sagen viser, at it-sikkerhed er noget både offentlige og private virksomheder skal tage meget alvorligt, og der skal lægges en meget stor og stadig stigende indsats i at sikre vores elektroniske data.

Tak for ordet.