JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Dato: 27. november 2014
Kontor: Sikkerhed og Forebyggelseskontoret
Sagsbeh: Andreas Christensen
Sagsnr.: 2014-0035-0256
Dok.: 1354204

UDKAST TIL TALE

til brug for besvarelsen af samrådsspørgsmål G
fra Folketingets Retsudvalg den 28. november 2014

Samrådsspørgsmål G:

"Ministeren bedes forholde sig til de af Center for Cybersikkerhed udarbejdede rapporter om hackerangrebet på CSC, jf. REU alm. del – bilag 353 og 356 (folketingsåret 2013-14) og den efterfølgende massive og usædvanlige kritik af myndighedernes håndtering af sagen som bl.a. er fremført i artiklen "Fortrolig rapport afslører elendig it-sikkerhed ved hackerangreb på CSC", bragt i Politiken den 11. oktober 2014."

Spørgsmålet er stillet efter ønske fra Karsten Lauritzen (V).

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

1. Hackerangrebet mod CSC har været med til at sætte en tyk streg under, at it-sikkerhed er noget, der skal tages meget alvorligt.

Det er klart, at når store mængder følsomme data gemmes på samme sted, så kan konsekvenserne af en sikkerhedsbrist være meget store. Og derfor skal sikkerheden simpelthen være i orden.

Og med den teknologiske udvikling kan man næppe være i tvivl om, at der også fremover vil skulle lægges en meget stor indsats i at sikre vores elektroniske data.

Som CSC-sagen jo også har vist, står vi på det her felt over for modstandere, som er exceptionelt dygtige til det, de laver, og alligevel er det myndighedernes opgave hele tiden at søge at være på omgangshøjde med dem.

2. Sagen har som bekendt ført en strafferetlig efterforskning med sig. Hacking er strafbart efter reglerne i straffeloven, og den politimæssige efterforskning af sagen er nu endt med, at en mand er blevet dømt for at stå bag hackerangrebet, ligesom en anden mand også er dømt i sagen.

Jeg skal i den forbindelse lige skynde mig at sige, at den svenske statsborger, som blev dømt for at stå bag hackerangrebet, har anket dommen til Østre Landsret. Den danske statsborger har derimod accepteret byrettens dom.

3. Til brug for min besvarelse af samrådsspørgsmålet er det gavnligt at få slået fast, at CSC-sagen giver anledning til to mere overordnede spørgsmål:

For det første: Har sikkerheden hos CSC været god nok?

For det andet: Har den efterfølgende håndtering af sagen været god nok?

4. Den 30. august 2012 blev en svensk statsborger i anden anledning anholdt i Cambodja på foranledning af svensk politi. Samtidig med anholdelsen fik den svenske statsborger beslaglagt en computer.

Kort efter blev han udleveret til Sverige og fængslet som led i en hackersag i Sverige.

I forbindelse med undersøgelserne af computeren fandt svensk politi tegn på, at computeren kunne have været brugt til et angreb mod CSC i Danmark.

CSC er en privat virksomhed, som bl.a. er antaget af en række danske myndigheder, heriblandt Rigspolitiet, til at varetage driften af vigtige it-systemer.

Det svenske politi underrettede dansk politi om deres opdagelse. Det skete bl.a. flere gange i løbet af efteråret 2012, hvor der blev sendt e-mails i september, oktober og november.

Der blev bl.a. oplyst om spor fundet på den anholdtes it-udstyr, herunder om nogle danske systemer, som formentlig var blevet forsøgt hacket. Der var i den forbindelse dialog mellem dansk og svensk politiet, men der blev imidlertid ikke på det tidspunkt indledt en egentlig efterforskning af sagen i Danmark. Det vender jeg tilbage til.

I januar 2013 modtog Rigspolitiet fra svensk politi oplysninger i form af logfiler, som viste, at data hos CSC kunne være blevet kompromitteret ved et hackerangreb.

Først i slutningen af februar 2013 fik Rigspolitiet gennemgået det omfattende materiale. Her kunne man konstatere, at CSC var blevet udsat for et hackerangreb.

Det var på dét tidspunkt, at der blev indledt en efterforskning i Danmark. Og det er da ærgerligt og beklageligt, at efterforskningen ikke kom i gang på et tidligere tidspunkt.

Efterfølgende har politiet, herunder Politiets Efterretningstjeneste i samarbejde med Center for Cybersikkerhed, gennemført en omfattende undersøgelse af hackerangrebet.

Undersøgelserne har vist, at nogen i februar 2012 foretog rekognoscering af CSC's it-systemer, og at selve hackerangrebet stod på fra april til august 2012, hvor den svenske statsborger blev anholdt i Cambodja.

Som det fremgår af en af de rapporter om hackerangrebet, som jeg vil vende tilbage til om lidt, er det vurderingen, at der har været tale om en omfattende og alvorlig kompromittering af de dele af CSC's it-miljø, som indeholder data fra politiet, CPR-kontoret, SKAT og Moderniseringsstyrelsen.

Hackeren har haft mulighed for at tilgå, kopiere, slette og ændre i myndighedernes data hos CSC, og der er med sikkerhed kopieret data fra politiets systemer.

Det har ikke været muligt at give et komplet overblik over, hvilke data der med sikkerhed er eller ikke er kopieret.

Som det også fremgår af den pågældende rapport, har det heller ikke været muligt at sige noget sikkert om, hvorvidt der er blevet ændret i myndighedernes data, men ud fra undersøgelserne af angrebet vurderes det ikke at være sandsynligt.

I juni 2013 blev en dansk medgerningsmand anholdt og fængslet i Danmark, og i november 2013 blev den svenske statsborger så udleveret til Danmark og fængslet her i landet.

Mændene blev den 31. oktober 2014 idømt henholdsvis ½ års og 3½ års fængsel ved Retten på Frederiksberg.

5. I august 2014 modtog regeringen to rapporter om hackerangrebet. Begge rapporter blev kort efter oversendt til Folketinget.

Den ene rapport er udarbejdet af Politiets Efterretningstjeneste og Center for Cybersikkerhed i fællesskab. Det er den rapport, som jeg henviste til for et øjeblik siden. Rapporten beskriver hackerangrebet og angrebets konsekvenser, og man kan bl.a. læse om omfanget af og årsagerne til sikkerhedsbruddet hos CSC.

Derudover indeholder rapporten en række sikkerhedsanbefalinger.

Rapporten indeholder bl.a. oplysninger om statslige myndigheders it-infrastruktur, ligesom man kan læse om forskellige angrebsteknikker og sårbarheder ved it-systemer.

De oplysninger vil kunne udnyttes af hackere ved eventuelle fremtidige hackerangreb, og bl.a. for at sikre, at oplysningerne ikke falder i de forkerte hænder, er rapporten klassificeret.

Som bekendt har Retsudvalget i øvrigt modtaget en delvis afklassificeret version af rapporten den 16. oktober 2014.

Den anden rapport er udarbejdet af Center for Cybersikkerhed og Digitaliseringsstyrelsen i fællesskab. Denne rapport indeholder en række anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

6. Med samrådsspørgsmålet er jeg blevet bedt om at forholde mig til de to rapporter.

Det kan jeg gøre forholdsvis enkelt:

Hvad angår PET's og Center for Cybersikkerheds rapport har jeg taget oplysningerne om angrebets omfang og årsager til efterretning. Det er en alvorlig sag, og derfor er der behov for, at der ageres.

Derfor har jeg med tilfredshed noteret mig, at alle rapportens anbefalinger til dansk politi analyseres grundigt af Rigspolitiet, så man kan sikre, at samtlige anbefalinger vurderes og tages meget alvorligt.

Og når det gælder Center for Cybersikkerheds og Digitaliseringsstyrelsens rapport, vil jeg naturligvis opfordre til, at alle relevante myndigheder sætter sig grundigt ind i rapportens anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

For mit eget ministerområde kan jeg i hvert fald sige, at der er stor fokus på at sikre, at anbefalingerne efterleves.

7. Jeg sagde før, at CSC-sagen giver anledning til to mere overordnede spørgsmål. Det ene spørgsmål går på, om it-sikkerheden hos CSC har været god nok.

Det er det spørgsmål, som er temaet for den artikel, der er henvist til i samrådsspørgsmålet.

Og i lyset af de konklusioner, der er kommet frem om datakompromitteringen, må svaret i al sin enkelhed være nej. Sikkerheden har ikke været god nok.

Det er naturligvis ganske utilfredsstillende.

Hackeren opnåede så høje systemrettigheder, at han kunne afbryde logningen af sine aktiviteter. Det betyder på godt dansk, at hackeren her har kunnet gennemføre sine aktiviteter uden at efterlade nogen form for spor.

Det er selvfølgelig ikke godt nok, at sådan noget kan ske.

Jeg har forstået, at både CSC og Rigspolitiet har lagt en meget stor indsats i at lukke de sikkerhedshuller, som sagen har afsløret. Herudover har politiet også mere generelt taget skridt til at forbedre den elektroniske beskyttelse af sensitive data.

8. Det andet spørgsmål, jeg nævnte, går på, om myndighedernes efterfølgende håndtering af hackerangrebet har været god nok. Det er det, som andet led i samrådsspørgsmålet handler om.

9. For det første har der været kritik af, at politiet under efterforskningen af hackerangrebet lod sig assistere af CSC's teknikere i stedet for selvstændigt at foretage den fulde undersøgelse af det angrebne it-miljø.

Pressen har simpelthen rejst tvivl om, hvorvidt CSC har haft en reel interesse i, at angrebets fulde omfang blev afdækket.

Hvis den slags undersøgelser laves uden inddragelse af folk med indgående kendskab til de konkrete it-opsætninger, kan man simpelthen risikere systemnedbrud eller væsentlige driftsforstyrrelser. Og i denne sag ville det kunne have haft den konsekvens, at vigtige samfundskritiske systemer blev sat ud af drift.

Det er i øvrigt Københavns Politis opfattelse, at samarbejdet mellem teknikerne i politiet og CSC er foregået upåklageligt under hele forlø-

bet, og politiet har ikke på noget tidspunkt haft anledning til at sætte spørgsmålstegn ved de personer, som har udført undersøgelser hos CSC, eller måden, de har gjort det på.

Jeg lægger til grund, at politiet er dem, som bedst er i stand til at afgøre, hvordan en strafferetlig efterforskning skal tilrettelægges.

10. Rigspolitiet har tidligere oplyst, at der i efteråret 2012 var kontakt mellem svensk og dansk politi, men at det var i januar 2013, at dansk politi for første gang modtog data i form af logfiler, der viste, at CSC kunne være blevet kompromitteret ved et hackerangreb.

Det er også en oplysning, der blev videregivet til Folketinget, og som var baseret på Rigspolitiets viden på daværende tidspunkt.

Efter at de nævnte oplysninger kom frem under straffesagen, har politiet foretaget en fornyet gennemgang af materiale og oplysninger, som er modtaget fra det svenske Rigspoliti og den svenske efterretningstjeneste.

Og som jeg var inde på før, har det så vist sig, at der faktisk *har* været yderligere kontakt mellem svensk og dansk politi – altså ud over den kontakt, som Folketinget allerede er blevet orienteret om.

Dansk politi har således i løbet af 2012 modtaget mere konkrete oplysninger om forsøg på hacking af CSC, end hvad der hidtil er blevet oplyst, og politiets bidrag til besvarelsen af tidligere folketingsspørgsmål om sagen har derfor ikke været fuldt ud dækkende.

Dansk politi reagerede på henvendelserne fra svensk politi ved at indgå i en dialog med de svenske myndigheder, men det var som nævnt først i begyndelsen af 2013, at politiet iværksatte en egentlig efterforskning,

Det er sandt at sige utilfredsstillende, og Rigspolitiet har også været ude at beklage. Og andet er der ikke at sige til det.

11. Det her er uden tvivl en sag, som myndighederne skal tage ved lære af.

I den forbindelse har politiet og anklagemyndigheden taget initiativ til en samlet styrket indsats mod it-kriminalitet, herunder i form af etableringen af NC3 (Nationalt Cyber Crime Center) i Rigspolitiet.

Og jeg har da også tillid til, at Rigspolitiet – i lyset af erfaringerne med CSC-sagen – kan sikre den nødvendige beskyttelse af deres data hos CSC fremover.

12. Lad mig afslutningsvis lige opsummere de vigtigste pointer, jeg har været inde på:

- Der er tale om en rigtig kedelig sag, som har vist, hvor alvorligt it-sikkerhed skal tages.
- Sagen har vist, at sikkerheden hos CSC ikke har været god nok, og at Rigspolitiet og Politiets Efterretningstjeneste på daværende tidspunkt havde en efterforskningsmæssig kapacitet på cyberområdet, som må betegnes som ikke fuldt tilstrækkelig.
- Politiet og anklagemyndigheden har siden taget initiativ til en samlet styrket indsats mod it-kriminalitet.
- Rigspolitiet og Politiets Efterretningstjeneste har nu beklaget, at der ikke blev indledt egentlige efterforskningsmæssige tiltag i sagen på et tidligere tidspunkt.

Tak.