Bilag 1.Talepapir ved samråd i KOU den 8. oktober

Samrådsspørgsmål:

Finansministeren bedes redegøre for kritikken af sikkerheden omkring offentlige myndigheders IT-systemer i den seneste rapport om emnet fra Center for Cybersikkerhed og Digitaliseringsstyrelsen om sikkerhed og udliciteret it-drift samt oplyse, hvad regeringen agter at gøre for at sikre borgernes personfølsomme data i offentlige myndigheders varetægt bedre.

Svar:

[Indledning]

- Jeg vil gerne takke udvalget for at give mig mulighed for at komme her i dag. Først har jeg tænkt mig at tale om rapporten fra Center for Cybersikkerhed og Digitaliseringsstyrelsen, og dernæst vil jeg redegøre for regeringens tiltag på området.

[Afgrænse spørgsmålet]

- Der er spurgt ind til seneste rapport fra Center for Cybersikkerhed og Digitaliseringsstyrelsen med anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

- Rapporten er en opfølgning på CSC-sagen og giver generelle anbefalinger til myndighederne.

- CSC-sagen går helt kort ud på, at hackere i 2012 skaffede sig adgang til et mainframemiljø hos CSC.

- Der var tale om en kompromittering af de dele af CSC's mainframemiljø, som indeholder data fra politiet, CPR-kontoret, SKAT og Moderniseringsstyrelsen.

- Den igangværende retssag er nu ved at afklare de strafferetlige konsekvenser af sagen.

- Fra regeringen er der tidligere udarbejdet to andre rapporter om CSC-sagen, der er klassificeret til tjenestebrug. Derfor kan jeg ikke diskutere deres indhold på et åbent samråd.

- Både Retsudvalget og Kommunaludvalget blev på et møde d. 16. september i Justitsministeriet orienteret om indholdet i den anden rapport.

- Spørgsmål til disse to rapporter henvises til Justits- og Forsvarsministeren.

[Redegøre for kritikken]

- Rapport 3, der også hedder "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift" er udarbejdet af Center for Cybersikkerhed og Digitaliseringsstyrelsen efter ønske fra regeringen, for at sikre, at alle statslige myndigheder skal lære mest muligt fra CSC-sagen.

- Rapporten udgør således regeringens eget bud på, hvordan sikkerheden hos enkelte myndigheder i lyset af CSC-sagen kan styrkes. Rapportens centrale pointe i denne sammenhæng er, at det især er et potentiale til forbedring af håndteringen af sikkerheden i outsourcede it-løsninger.

- Anbefalingerne til styrkelse af sikkerheden i de outsourcede it-løsninger skal ses i lyset af, at CSC-sagen illustrerer, at netop styringen af de eksterne leverandører kan udgøre et svagt punkt i it-sikkerheden, hvis myndighederne ikke har fokus på denne opgave.

- Fra CSC-sagen fremgår det, at de angrebne outsourcede it-systemer på angrebstidspunktet var sårbare i en sådan grad, at det lykkedes angriberne at kompromittere fortroligheden af følsomme oplysninger, og at angriberne havde etableret et fodfæste i systemerne, så de potentielt kunne have forårsaget tab eller forvanskning af uerstattelige data.

- Rapport 3 har nu med baggrund i CSC-sagen også vist, at mere systematiske retningslinjer for, hvordan myndighederne skal arbejde med it-sikkerheden i outsourcede it-systemer, fremadrettet vil kunne sætte fokus på den type it-trusler, som CSC-sagen er et eksempel på.

- Jeg vil senere vende tilbage til at beskrive rapportens anbefalinger og regeringens øvrige fremadrettede indsats målrettet it-sikkerhed.

- Først er det dog væsentligt at pointere, at regeringen tager CSC-sagen meget alvorligt. Udviklingen i it-relaterede trusler går stærkt, og det er derfor afgørende, at den offentlige sektor lærer af sager, hvor sikkerheden ikke har været god nok og generelt opruster indsatsen for at imødekomme udfordringer på området.

- Det er også vigtigt at pointere, at vi aldrig kan opnå 100 pct. sikkerhed, uanset hvor mange ressourcer, vi bruger på det, da den digitale verden udvikler sig kontinuerligt, og der hele tiden opstår nye sikkerhedstrusler.

- It-sikkerhed er dynamisk og en afvejning mellem sikkerhed, brugervenlighed og økonomi. Indsatsen bør derfor være risikobaseret og dermed fokuseres, der hvor den giver mest værdi og effekt i forhold til sikkerhed.

- Den centrale udfordring er derfor at sikre et mere systematisk beredskab blandt myndighederne til at håndtere it-sikkerhedsrisici, forbedre myndighedernes viden om det aktuelle trusselsbillede og sikre et kontinuerligt arbejde i myndighederne med at løbende risikovurdere og følge op på egen og outsourcet it-sikkerhed.

[Regeringens hidtidige indsats]

- Arbejdet med at styrke it-sikkerheden har regeringen siden sin tiltrædelse prioriteret højt. Og en række af de tiltag, regeringen allerede har igangsat, er centrale for at få et billede af regeringens samlede indsats for at forbedre it-sikkerheden i staten.

- Helt konkret har regeringens fokus på sikkerheden resulteret i oprettelsen af Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste.

- Centeret arbejder med beskyttelse af samfundsvigtige funktioner mod avancerede cyberangreb gennem rådgivning og varsling. Centeret arbejder bredt med at understøtte en styrkelse af

cybersikkerheden i den infrastruktur, som danner grundlag for samfundsvigtige funktioner.

- Centeret kan også udføre sikkerhedsmonitorering og bistå i tilfælde af sikkerhedshændelser fra cyberangreb.

- Under Center for Cybersikkerhed ligger GovCERT, der medvirker til, at der i staten er overblik over trusler og sårbarheder i tjenester, netværk og systemer relateret til internettet. Dette inkluderer en varslingstjeneste, der sørger for at varsle statens it-leverandører omkring kritiske sårbarheder, således at disse kan udbedres.

- Med oprettelsen af Center for Cybersikkerhed har regeringen således skabt et organ, der løbende giver offentlige myndigheder rådgivning omkring cybersikkerhed samt kendskabet til trusler og sårbarheder. Hvilket forbedrer de offentlige myndigheders muligheder for at imødegå disse trusler.

- Ligeledes er Nationalt Cyber Crime Center (NC3) blevet oprettet under Rigspolitiet. Dette nationale center har bl.a. til opgave at efterforske og opklare it-kriminalitet, men har også et forebyggelseselement med henblik på at sikre, at it-kriminalitet ikke sker, fx hvad angår krænkelse af børn på nettet.

- Endvidere er alle statslige myndigheder forpligtet til at følge sikkerhedsstandarden ISO27001. Standarden er en internationalt anerkendt standard for sikkerhed og omfatter krav til risikovurdering, organisering af sikkerhedsarbejdet samt dokumentation og ledelsesinddragelse.

- ISO27001 standarden giver således de offentlige myndigheder et redskab til at arbejde mere systematisk med sikkerhed i deres organisationer.

- Alle statslige myndigheder er pt. ved at implementere den nye standard med vejledning og rådgivning fra Digitaliseringsstyrelsen.

[Regeringens fremadrettede tiltag]

- Udover de her gennemgåede hidtidige initiativer for at øge it-sikkerheden i det offentlige har regeringen taget en række yderligere fremadrettede tiltag, som skal supplere og styrke det igangværende arbejde.

- Dette arbejde indeholder initiativerne beskrevet i rapport 3, som spørgsmålet vedrører, men også andre tiltag er relevante at nævne i denne sammenhæng.

  Jeg vil i beskrivelsen af det fremadrettede arbejde derfor fremhæve tre elementer:

  1. Anbefalinger til statens outsourcede it-drift
  2. Strategi for Cyber- og Informationssikkerhed
  3. Arbejdsgruppe om beskyttelse af oplysninger ved elektroniske betalinger.

[1. Anbefalinger til statens outsourcede it-drift]

- Som indledningsvist nævnt har Center for Cybersikkerhed og Digitaliseringsstyrelsen vurderet, at en styrket og mere systematisk sikkerhedsmæssig styring af eksterne leverandører vil kunne styrke statslige myndigheders it-sikkerhedsarbejde og derved sikkerheden omkring borgernes følsomme persondata i offentlige myndigheders varetægt.

- På baggrund af CSC-sagen er der opstillet konkrete anbefalinger til, hvad myndighederne skal have fokus på, og hvilke krav, de skal stille til sine leverandører.

- Jeg vil gerne på et overordnet plan fremhæve fire områder fra rapporten, hvor der skal arbejdes med at forbedre it-sikkerheden:

- [1] For det første skal myndighederne kende de trusler, de står over for, og de skal kende sårbarhederne i deres systemer.

- [2] For det andet skal myndighederne som nævnt stille krav til it-sikkerheden hos leverandører og følge op på kravene.

- [3] For det tredje skal myndighedernes sikkerhedsorganisationer forankres i ledelsen.

- [4] For det fjerde skal ministerierne videndele på sikkerhedsområdet, så de kan lære af hinanden.

[2. Strategi for Cyber- og informationssikkerhed]

- Ud over anbefalingerne i rapport 3 har regeringen taget initiativ til udarbejdelsen af en strategi for cyber- og informationssikkerhed.

- Strategiens formål er at sikre, at it-sikkerhedsarbejdet bliver strategisk forankret og koordineret på tværs af staten. Samt at styrke informations- og cybersikkerheden med yderligere initiativer.

- Netop fordi arbejdet med it-sikkerhed har tværgående egenskaber og betydning for alle områder i staten, er en samlet strategi og koordination væsentligt for at sikre systematik og tværgående læring.

- Derfor er der af regeringen nedsat en tværministeriel arbejdsgruppe, som skal udarbejde en national strategi for cyber- og informationssikkerhed.

- Strategien udformes med milepæle for årene 2015 og 2016 og vil følges op med konkrete handlingsplaner, om hvordan de enkelte ministerområder vil sikre implementeringen på egne områder.

- Strategien lanceres i år.

[3. Arbejdsgruppe om beskyttelse af oplysninger ved elektroniske betalinger]

- Derudover ser regeringen på beskyttelse af oplysninger ved elektroniske betalinger. Dette sker i forlængelse af Se og Hør sagen, hvor der er blevet nedsat en arbejdsgruppe under Justitsministeriet, som har til opgave at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger mv.

- Arbejdsgruppen skal afklare, om der er grundlag for at gennemføre nye initiativer på området, herunder ændring af reglerne om behandlingssikkerhed (it-sikkerhed), skærpelse af straffen for

overtrædelse af persondataloven og anden relevant lovgivning, styrkelse af reaktionsmuligheder og tilsynsbeføjelser for Datatilsynet eller andre tilsynsmyndigheder samt ændring af grænsedragningen mellem tilsynsmyndighedernes kompetencer.

- Området er relateret til arbejdet med it-sikkerhed i staten, men ser bredere på databeskyttelsen af borgere, særligt i relation til kontrollen med finansielle institutioners arbejde med følsomme personoplysninger.

- Arbejdsgruppen vil afrapportere i år.

[Afslutning]

- Afslutningsvis vil jeg gerne runde af med at sige, at CSC-sagen indeholder en læring, som alle statslige myndigheder kan have nytte af.

- Regeringen har med rapport 3, som der spørges ind til, og med de øvrige initiativer, som jeg har gennemgået, iværksat en palette af initiativer, som samlet set skal sikre;

    - At myndighederne fremover har bedre redskaber til at arbejde systematisk med it-sikkerhed.
    - At de bedre kender det aktuelle trusselsbillede og har nemmere adgang til avanceret viden om, hvordan aktuelle trusler skal håndteres.
    - At der stilles yderligere krav til og sker en løbende risikovurdering af og opfølgning med eksterne leverandørers it-sikkerhedsarbejde.

- Jeg håber, at dette besvarede spørgerens spørgsmål om sikkerheden omkring offentlige myndigheders it-systemer i den seneste rapport om emnet fra Center for Cybersikkerhed og Digitaliseringsstyrelsen.

- Ligeledes håber jeg, at jeg har givet et klart billede af, hvad regeringen gør og agter at gøre fremadrettet for at sikre borgernes følsomme persondata i offentlige myndigheders varetægt.