DET TALTE ORD GÆLDER
Samråd den 23. maj 2014

[**Samrådsspørgsmål A**
Ministeren bedes redegøre for, om statsrevisorernes beretning nr. 3/2013 fra den 9. oktober 2013 om forebyggelse af hackerangreb giver ministeren anledning til at iværksætte nye politiske tiltag i forhold til de arbejdsopgaver, som Center for Cybersikkerhed har ansvaret for?]

# Taleseddel samrådsspørgsmål A

- Cybersikkerhed er et højt prioriteret fokusområde for regeringen, og det er godt, at Rigsrevisionen også har fokus på dette vigtige område.

- Jeg synes, at Rigsrevisionen i sin beretning fra oktober 2013 kommer med nogle centrale anbefalinger, og jeg har i den forbindelse noteret, at Rigsrevisionen – som det også fremgår af beretningen – har indhentet ekspertviden hos Center for Cybersikkerhed.

- Rigsrevisionens beretning indeholder tre anbefalinger. For det første at alle statslige virksomheder forholder sig aktivt til risikoen for et cyberangreb. For det andet at Finansministeriet præciserer opgavesplittet mellem Statens It og virksomhederne, hvad angår sikring mod hackerangreb fra internettet. For det tredje at Finansministeriet eller Forsvarsministeriet udarbejder en vejledning til statslige virksomheder om nyttige sikringstiltag.

- For så vidt angår Forsvarsministeriets område, så oprettede Regeringen som bekendt Center for Cybersikkerhed i december 2012. Det skete for at styrke vores beskyttelse mod cyberangreb.

- Og for så vidt angår Rigsrevisionens anbefaling vedrørende udarbejdelse af en vejledning om sikringstiltag, så har Center for Cybersikkerhed og Digitaliseringsstyrelsen i november måned 2013 udarbejdet en fælles vejledning – "Cyberforsvar der virker".

- Vejledningen beskriver de mest centrale sikringstiltag, som myndigheder og virksomheder bør gennemføre for at imødegå

den stadigt stigende risiko for alvorlige cyberangreb og kommer med anbefalinger på både leder-, teknisk-, og brugerniveau.

- Hvis jeg skal nævne de vigtigste punkter fra vejledningen, kan der nævnes vigtigheden af opbakning og prioritering fra topledelsen; nødvendigheden af den rette tekniske kompetence til at imødegå cybertruslen og opmærksomheden fra den enkelte bruger om truslen fra cyberspace i form af f.eks. emails.

- Helt konkret omtaler vejledningen en "top fire" af tiltag, som drastisk minimerer risikoen for cyberangreb i virksomheder. "Top fire" løser ikke problemet alene, men de løfter angrebsbyrden til et niveau, hvor færre modstandere kan være med.

- Helt lavpraktisk handler "top fire"-tiltagene om, at virksomheden udarbejder en liste over godkendt software, der må benyttes; at programmerne holdes jævnligt opdateret samt at virksomhederne begrænser antallet af brugerkonti med domæne- eller lokaladministratorrettigheder.Rigsrevisionen har oplyst, at den i de kommende it-revisioner vil have fokus på, om Center for Cybersikkerheds anbefalinger fra vejledningen bliver fulgt.

- Med oprettelsen af Center for Cybersikkerhed i december 2012 blev Danmarks beskyttelse mod cyberangreb forøget.

- Regeringen vil med det fremsatte forslag til lov om Center for Cybersikkerhed yderligere styrke beskyttelsen mod cyberangreb.

- Lovforslaget vil give centeret nye og bedre redskaber til at undersøge cyberangreb, bl.a. gennem øget samarbejde med myndigheder og private virksomheder, så centeret i større omfang end i dag kan få de nødvendige informationer, der skal bruges til at afklare, hvilke angrebsværktøjer og metoder, der anvendes ved cyberangreb.

- De nye muligheder vil også styrke forebyggelsen af nye og tilsvarende hændelser med behørig respekt for retssikkerheden og den personlige frihed.

- Jeg vil også fremhæve, at styrkelsen af den forebyggende indsats på cybersikkerhedsområdet desuden omfatter en øget vejledningsindsats fra Center for Cybersikkerhed over for både myndigheder og virksomheder.

- Regeringen har særligt fokus på at styrke cybersikkerheden, fordi det er et område, der er i konstant udvikling. Dem, der angriber vores digitale infrastruktur, bliver hele tiden bedre og får mere avancerede værktøjer – og derfor skal vi selvfølgelig også fortsætte med at udvikle både vores forebyggende indsats og vores evne til at imødegå angrebene, når de sker.

- Med Center for Cybersikkerhed har vi for første gang fået en særskilt national it-sikkerhedsmyndighed i Danmark. Det sikrer, at der er stor fokus på at beskytte den kritiske ikt-infrastruktur, som understøtter samfundsvigtige funktioner.

- En meget vigtig opgave for den nationale it-sikkerhedsmyndighed er at bistå andre myndigheder med både at forebygge og håndtere sikkerhedsbrud.

- Som et konkret eksempel kan jeg nævne, at Center for Cybersikkerhed har en central rolle i at klarlægge omfanget af det meget omtalte hackerangreb mod CSC. For det er selvfølgelig vigtigt, at vi får en detaljeret viden om, hvad der skete, og her arbejder Center for Cybersikkerheds it-eksperter tæt sammen med politiet, som selvsagt varetager efterforskningen af sagen. Jeg forventer, at den afsluttende rapport om hackerangrebet mod CSC kan oversendes til Folketinget om kort tid.

- Men det er også vigtigt, at vi i staten lærer af erfaringerne fra de forskellige former for sikkerhedsbrud, som vi ser.

- Derfor glæder jeg mig over, at vi nu har en national it-sikkerhedsmyndighed, som kan komme med fremadrettede anbefalinger til, hvordan vi kan blive bedre til at sikre statens it-systemer, og hvordan vi bliver bedre til at håndtere it-sikkerheden, når for eksempel driftsopgaver overlades til eksterne leverandører.

- Netop den erfaringsopsamling – og omsætningen af erfaringerne til konkrete anbefalinger – ser jeg som et område, der også fremover skal styrkes yderligere. Og med oprettelsen af Center for Cybersikkerhed er rammerne for det arbejde på plads.

- Center for Cybersikkerhed vil endvidere som led i sin virksomhed løbende udgive en række vejledninger, der skal hjælpe myndigheder og virksomheder på forskellige områder, hvor erfaringerne viser, at der er behov for at styrke it-sikkerheden.

- Statens IT spiller en central og kritisk rolle som it-leverandør til en lang række statslige myndigheder. Der er i dag derfor allerede en tæt og regelmæssig dialog mellem Center for Cybersikkerhed og Statens IT.

- Det drøftes i øjeblikket mellem de to parter, hvordan det daglige samarbejde kan styrkes for at øge cybersikkerheden, bl.a. ved at gennemføre pilotforsøg, der har til formål at teste nye sikkerhedsmekanismer hos Statens IT.

- En stor fordel ved at have et samlet kompetencecenter for cybersikkerhed i staten er, at Center for Cybersikkerhed i forebyggelses- og rådgivningsarbejdet kan trække på den helt konkrete viden om cyberangreb, som hele tiden indsamles i de

civile og militære netsikkerhedstjenester for internettrusler, der også er placeret i centeret.

- Her arbejder man med at opdage, varsle om og imødegå cyberangreb, og der udsendes løbende situationsbilleder og konkrete varslinger om trusler og sårbarheder i tjenester, net og systemer.

- Til slut vil jeg nævne, at der i øjeblikket arbejdes på en national strategi for cyber- og informationssikkerhed. Strategien vil indeholde anbefalinger om konkrete initiativer over en bred front, der vil kunne medvirke til at øge cybersikkerheden i Danmark.

- Jeg forventer, at strategien kan præsenteres senere i år. Så det er endnu et eksempel på, at cybersikkerheden er et område, som regeringen prioriterer højt, og at vi løbende vil følge udviklingen, så vi sikrer, at vi altid har de rette værktøjer til både at forebygge og imødegå cyberangreb.

- Tak.