TALESEDDEL TIL FORSVARSMINISTEREN TIL BESVARELSE AF REU SAMRÅDSSPØRGSMÅL G OM HACKERANGREBET MOD CSC FREDAG DEN 28. NOVEMBER 2014

REU 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."

27. november 2014

Besvarelse af samrådsspørgsmål G

- Hackerangrebet mod CSC var uden tvivl et af de alvorligste hackerangreb, vi har set i Danmark, og jeg vil gerne understrege, at regeringen tager denne sag meget alvorligt. Derfor har regeringen også lagt stor vægt på at få analyseret hackerangrebet grundigt. Desuden er det meget vigtigt, at vi i staten aktivt bruger erfaringerne fra angrebet til at styrke it-sikkerheden.

- De rapporter, som omtales i spørgsmålet, har netop haft til formål at analysere hackerangrebet og komme med anbefalinger til styrkelse af it-sikkerheden. Analysen af angrebet er sket i et tæt samarbejde mellem Center for Cybersikkerhed og PET. De fremadrettede anbefalinger er udarbejdet af Center for Cybersikkerhed og Digitaliseringsstyrelsen.

- Som justitsministeren netop har forklaret, giver CSC-rapport II en detaljeret beskrivelse af sikkerhedsbruddet hos CSC, og det står klart, at it-sikkerheden hos CSC ikke

var i orden. Men de berørte myndigheder har efterfølgende gjort en stor indsats for at sikre, at it-sikkerheden er blevet styrket.

- Jeg vil nu komme nærmere ind på indholdet af den tredje rapport om CSC-sagen, som indeholder anbefalinger til en styrkelse af sikkerheden i statens outsourcede it-drift.

- For udover den konkrete indsats i forhold til it-sikkerheden i det pågældende it-system hos CSC er det i kølvandet på hackerangrebet mod CSC helt afgørende, at såvel offentlige myndigheder som private virksomheder lærer af de erfaringer, som kan udledes af angrebet.

- Det er baggrunden for, at Center for Cybersikkerhed og Digitaliseringsstyrelsen har udarbejdet en fælles rapport, som tager udgangspunkt i de ting, som gik galt ved sikkerhedsbruddet hos CSC og kommer med konkrete anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

- CSC-sagen har først og fremmest understreget, at der findes en reel og alvorlig trussel om cyberangreb imod danske myndigheders digitale systemer.

- En stor del af den statslige it-drift er outsourcet til eksterne leverandører, og vi har den seneste tid set flere andre alvorlige sikkerhedshændelser hos statens eksterne

it-leverandører, f.eks. utilgængeligheden af NemID i kortere perioder, samt den såkaldte Se og Hør-sag. Derfor er det særligt vigtigt, at der er stor fokus på sikkerheden i outsourcet it-drift.

- Den helt centrale anbefaling i rapporten er derfor, at myndighederne skal være mere opmærksomme på at stille passende sikkerhedsmæssige krav til deres leverandører – og at myndighederne løbende skal følge op på, om kravene fortsat er passende, og om leverandørerne efterlever kravene.

[CSC-rapport III – anbefalingerne]

- Rapportens anbefalinger fokuserer på fire områder:

  [1] For det første skal myndighederne kende de trusler, de står overfor, og de skal kende sårbarhederne i deres systemer:

  - Det betyder blandt andet, at myndighedernes ledelse skal vurdere konsekvenserne af, at data, som myndigheden behandler, bliver stjålet.

  - Ledelsen skal også kende til de aktuelle trusler og til de aktører, som kunne være interesseret i myndighedernes data og systemer.

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

- Det understreges i rapporten, at sikkerheden i systemerne er myndighedens ansvar. Det er derfor ikke nok, at myndigheden bare forlader sig på, at leverandøren nok har styr på tingene.

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

- Sikkerhedsbrud er meget dyre og betyder hver gang potentielle omkostninger eller anden ulempe – både for myndigheden og for borgere eller virksomheder. Samtidig taber den involverede myndighed anseelse, og offentligheden taber tillid til de digitale løsninger i samfundet.

- It-sikkerhed er derfor i høj grad et ledelsesspørgsmål.

[4] For det fjerde skal ministerierne koordinere og videndele på sikkerhedsområdet:

- Offentlige myndigheder står langt hen ad vejen med de samme udfordringer, og de kan derfor lære af hinanden – både om, hvad der gik galt, og om, hvad der bliver gjort rigtigt.

- Jeg er sikker på, at anbefalingerne vil blive studeret grundigt af myndighedernes ledelser, og at anbefalingerne vil være et godt grundlag for en styrkelse af it-sikkerheden i myndighederne og hos deres leverandører.

[Afslutning]

- Alt i alt mener jeg, at vi med de to rapporter har fået en grundig og meget brugbar bearbejdning af det alvorlige hackerangreb mod CSC. It-sikkerheden er allerede forbedret, og med de fremadrettede anbefalinger er der skabt gode forudsætninger for at forbedre sikkerheden yderligere.

- Regeringen har helt fra starten haft fokus på at styrke beskyttelsen mod cyberangreb. Et af de helt centrale tiltag har i den forbindelse været oprettelsen af Center for Cybersikkerhed, som altså også har spillet en helt central rolle i forbindelse med analysen af angrebet mod CSC og i forbindelse med udarbejdelse af de fremadrettede anbefalinger.

- Arbejdet med at forbedre sikkerheden fortsætter – både hos Center for Cybersikkerhed og hos de enkelte myndigheder. For lad mig understrege at det jo følger af det almindelige sektoransvarsprincip, at det er de enkelte

myndigheder, der har ansvaret for it-sikkerheden i deres egne systemer og i de systemer, som private leverandører driver for myndighederne.

- Regeringen har – bl.a. på baggrund af erfaringerne fra CSC-sagen – allerede iværksat en række umiddelbare, konkrete tiltag på cybersikkerhedsområdet, herunder etablering af fora, der kan sikre en bedre videndeling på området. Men vi vil også fremadrettet arbejde på yderligere at styrke sikkerheden i statens it-løsninger.

- Helt konkret formulerer regeringen en egentlig national strategi for cyber- og informationssikkerhed.

- Den nationale strategi skal sikre en målrettet indsats på sikkerhedsområdet med sigte på at opretholde tryghed og tillid til digitale løsninger. Det sker med deltagelse af en række ministerier, og strategien omsættes umiddelbart i en række konkrete initiativer, der skal være med til yderligere at styrke cyber- og informationssikkerheden i Danmark.