digitaliserings og ligestillingsministeriet

Digitaliseringsminister og minister for ligestilling Marie Bjerres talepapir

Anledning	DIU alm. del samråd G, som er stillet efter ønske fra Lisbeth Bech-Nielsen
Dato / tid	9. januar 2024 15:00-16:00
Sted	Folketingets digitaliserings- og it-udvalg
Talens varighed	10 minutter

Det talte ord gælder

Samrådsspørgsmål G:

”Vil ministeren i lyset af Rigsrevisionens beretninger og Statsrevisorernes kritik i beretning nr. 5 og 6 om sikkerheden på Statens it-servere og statens it-beredskab besvare følgende:

- Vil ministeren kommentere på det forhold, at Danmark er et af verdens mest digitaliserede lande, men at det offentlige it-sikkerhedsniveau medfører risici for samfundskritiske systemer og for borgernes følsomme personoplysninger og forretningskritiske data?
- Hvilke konkrete tiltag vil ministeren iværksætte for at bringe it-sikkerheden på Statens It’s servere i orden, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering, og så cyberangreb ikke kan sprede sig mellem servere og mellem myndigheder?
- Hvilke konkrete tiltag vil ministeren iværksætte i samarbejde med de relevante ministerier for at sikre, at alle samfundskritiske funktioner har et tilfredsstillende og stærkt it-beredskab, således at løsningen af samfundskritiske opgaver ikke trues i tilfælde af større it-nedbrud, hackerangreb mv.?
- Vil ministeren redegøre for, hvorfor man i lyset af forrige års kritik og den stigende cybersikkerhedstrussel ikke har sikret at styrke sikkerhedsniveauet?”

[Indledning]

- Tak for invitationen og tak til spørgeren for at bringe disse vigtige emner om it-beredskab og sikkerheden på Statens It's servere op.
- Samrådsspørgsmålet indeholder fire underspørgsmål: Det ene underspørgsmål omhandler forhold i Statens It mere specifikt, og de øvrige tre underspørgsmål vedrører mere generelt it-beredskabet i forhold til statslige samfundskritiske it-systemer.
- Det er aftalt med finansministeren og med udvalget, at jeg som digitaliseringsminister indleder med at svare på de tre underspørgsmål vedrørende it-beredskabet i staten.
- Herefter vil jeg give ordet til finansministeren, så han kan svare på underspørgsmålet om Statens It, som er en styrelse under Finansministeriet.

[Cyber- og informationssikkerhed i staten generelt]

- Som indledning til at besvare spørgsmålene vil jeg understrege, at cyber- og informationssikkerhed er områder, der har regeringens opmærksomhed.
- Og for mig som digitaliseringsminister er cyber- og informationssikkerhed et vigtigt område, fordi sikkerheden skal følge med i takt med den stigende digitalisering af den offentlige sektor og samfundet mere generelt.
- Vi har en offentlige sektor, der har været tidligt ude og anvendt de muligheder, der følger med digitaliseringen.
- Det har været medvirkende til at gøre Danmark til et af de meste digitaliserede lande.
- Men en høj grad af digitalisering giver også et behov for tilsvarende høj cyber- og informationssikkerhed.
- Skiftende regeringer har derfor siden 2014 udarbejdet nationale strategier for cyber- og informationssikkerhed. Den seneste blev lanceret for to år siden.
- Det gælder, at strategierne og arbejdet med cyber- og informationssikkerhed i Danmark er baseret på sektoransvarsprincippet.
- Det indebærer, at den myndighed, der har ansvaret for en opgave til daglig, bevarer ansvaret for opgaven under en større ulykke eller katastrofe.
- Ansvaret for cyber- og informationssikkerhed i den enkelte statslige myndighed ligger dermed i sidste ende hos den ansvarlige minister.

- Og det giver god mening at ansvaret ligger hos den enkelte myndighed.
- Blandt andet sikrer det lokale ansvar, at cyber- og informationssikkerhed ses i sammenhæng med den konkrete faglige opgaveløsning og ikke som en særskilt opgave.
- Det lokale ansvar hos de enkelte statslige myndigheder understøttes centralt med en række værktøjer, som særligt Digitaliseringsstyrelsen udvikler.

[Anonymisering af myndigheder og systemer]

- I forhold til de tre underspørgsmål, jeg vil svare på, udspringer de af Rigsrevisionens beretning 5 om statens it-beredskab.
- I beretningen er fire af syv undersøgte myndigheder anonymiserede. Det samme gælder alle de undersøgte samfundskritiske systemer.
- Anonymiseringen er sket af sikkerhedshensyn, og jeg kan derfor ikke udtale mig mere præcist om disse.

[Sikkerhedsniveauet i offentlige it-systemer]

- I det første underspørgsmål spørges til det forhold, at Danmark er et af verdens mest digitaliserede lande, men at det offentliges it-sikkerhedsniveau medfører risici for samfundskritiske systemer og for borgernes følsomme personoplysninger og forretningskritiske data.
- Jeg er glad for at få stillet det spørgsmål, for det giver mulighed for at tage en vigtig debat om it-sikkerhed og risikostyring.
- I spørgsmålet fremhæves det, at det nuværende sikkerhedsniveau medfører en risiko for systemerne og data. Og lige netop ordet ”risiko” vil jeg gerne tage fat i her.
- Virkeligheden er – desværre – at der altid vil være en risiko for, at et system går ned og ikke umiddelbart kan genoprettes, og at nødplanen ikke virker efter hensigten.
- Det kan skyldes fejl, naturkatastrofer eller bevidste, ondsindede handlinger.
- Men selv hvis alle samfundskritiske it-systemer lever op til alle kriterier for it-beredskab, som opstilles i beretningen, vil den risiko ikke kunne fjernes helt.
- Formålet med den risikostyring, som sikkerhedsstandarden ISO 27001 tager udgangspunkt i er, at den enkelte myndigheds ledelse bliver gjort

bekendt med de aktuelle risici og prioriterer ressourcerne derefter. Herved kan risici minimeres til et acceptabelt niveau.

- Deri ligger både en præmis om, at risici ikke kan fjernes helt - men kun kan minimeres, og at ressourcerne ikke er uendelige.
- Investeringer i it-sikkerhed fungerer groft sagt som mange andre investeringer: Man får meget sikkerhed for den første krone, der investeres, men man når også et punkt, hvor man får meget lidt ekstra sikkerhed for hver ekstra krone, der investeres.
- Den tilgang til it-sikkerhed genfindes i EU's nye cybersikkerhedsdirektiv. NIS2-direktivet.
- I NIS2-direktivet fremgår det bl.a., at der skal tages hensyn til gennemførelsesomkostningerne, når det skal vurderes, hvilke sikkerhedstiltag der skal iværksættes.
- Når der er tale om samfundskritiske it-systemer, mener jeg, at der skal investeres de nødvendige ressourcer for at opnå et højt sikkerhedsniveau.
- Som beretningen viser, er der områder, hvor it-beredskabet i staten skal forbedres i forhold til samfundskritiske it-systemer.
- Jeg finder det derfor positivt, at beretningen har givet anledning til justeringer i it-beredskabet hos de myndigheder, hvor Rigsrevisionen påpeger mangler.
- Sikkerhed er dog ikke det eneste, der er vigtigt i forhold til samfundskritiske it-systemer.
- Systemerne er sat i verden med et primært, fagligt formål – for at bidrage til en opgave, som skal løses.
- Samtidig skal de være brugervenlige, være tilgængelige for personer med handicap eller funktionsnedsættelse, og de skal drives økonomisk effektivt.
- De andre hensyn er ikke afspejlet i beretningen, og særligt indgår der ikke overvejelser om økonomiske hensyn og prioriteringer.
- Jeg synes også, at det er vigtigt at fremhæve, at beretningen omhandler it-beredskabet og ikke den samlede sikkerhed omkring de undersøgte statslige samfundskritiske it-systemer.
- It-beredskabet indgår som et vigtigt element i sikkerheden, men samtidig indgår der andre sikkerhedselementer, der skal forhindre angrebsforsøg i overhovedet at komme så vidt, at beredskabet bliver aktiveret.
- Det er vigtigt at holde sig for øje, inden der drages konklusioner om den samlede sikkerhed omkring statens samfundskritiske it-systemer.

[Konkrete tiltag]

- I forhold til spørgsmålet om, hvilke tiltag der vil blive iværksat i samarbejde med de relevante ministerier for at sikre et tilfredsstillede og stærkt it-beredskab vil jeg dels fokusere på den eksisterende indsats og dels det kommende arbejde.
- Digitaliseringsstyrelsen har udformet en række vejledninger og skabeloner til myndigheders it-beredskab.
- Digitaliseringsstyrelsen udbyder som en del af statens digitaliseringsakademi en række kurser om it-sikkerhed rettet mod både medarbejdere og ledere, og it-beredskabet indgår som en del af disse kurser.
- Digitaliseringsstyrelsen beder desuden hvert år alle statslige myndigheder følge op på deres anvendelse af ISO 27001, og Digitaliseringsstyrelsen afrapporterer herom til regeringen.
- En sammenfatning af resultaterne af den opfølgning offentliggøres.
- Det er samlet set min vurdering, at der fra Digitaliseringsministeriet gives gode forudsætninger for, at alle statslige myndigheder kan implementere et godt it-beredskab.
- Den vurdering understøttes af, at Rigsrevisionen i den første beretning om it-beredskabet i staten konkluderede, at Digitaliseringsstyrelsen på tilfredsstillende vis har vejledt de statslige myndigheder.
- I forhold til det kommende arbejde vil der som noget nyt med implementeringen af NIS2-direktivet blive ført proaktivt tilsyn med de omfattede statslige myndigheders arbejde med cyber- og informationssikkerhed.
- Den nærmere udformning af direktivet i dansk ret må afvente et kommende lovforslag, men af direktivet fremgår it-berdskabet også som et element, idet de omfattede enheder blandt andet skal have styr på reetablering og krisestyring.

[Handling siden sidste års kritik]

- I forhold til spørgsmålet om, hvorfor man i lyset af forrige års kritik og den stigende cybersikkerhedstrussel ikke har sikret at styrke sikkerhedsniveauet, er det min opfattelse, at der generelt arbejdes hårdt på at styrke sikkerheden i de enkelte myndigheder, og at it-sikkerhed har et stort fokus i staten.
- Det skyldes blandt andet, at de tekniske minimumskrav til de statslige myndigheder løbende er blevet tilpasset. Senest blev der i juni 2023

udvidet med nye krav, som myndighederne skal have implementeret senest d. 1. juli 2024.

- I forhold til hvorfor de undersøgte myndigheder ikke har imødekommet kritikken, vil jeg igen henlede opmærksomheden på sektoransvarsprincippet.
- Jeg kan derfor ikke svare på, hvad myndigheder uden for mit ministerium har gjort eller ikke har gjort i forhold til it-beredskabet for deres samfundskritiske it-systemer, men Digitaliseringsstyrelsen har løbende fokus på at komme med den rette vejledning.

- Det var mine svar på tre af de fire underspørgsmål.
- Nu vil jeg give ordet til finansminister Nicolai Wammen

[Finansministerens tale]

[Afrunding]

[MIN får ordet af finansministeren]

- Mange tak.
- Til sidst vil jeg også takke for ordet.