FINANSMINISTERIET

Folketingets Udvalg for Digitalisering og It
Christiansborg

10. januar 2024

Svar på Udvalget for Digitalisering og Its spørgsmål nr. 78 (Alm. del) af 9. januar 2024

Spørgsmål
Ministeren bedes oversende sit talepapir fra samrådet den 9. januar 2024 om Rigsrevisionens beretninger og Statsrevisorernes kritik i beretning nr. 5 og 6 om sikkerheden på statens it-servere og statens it-beredskab, jf. DIU alm. del - samrådsspørgsmål G.

Svar
Nedenfor fremgår talepapiret fra samrådet den 9. januar 2024 om Rigsrevisionens beretninger og Statsrevisorernes kritik i beretning nr. 5 og 6 om sikkerheden på statens it-servere og statens it-beredskab.

Med venlig hilsen

Nicolai Wammen
Finansminister

Det talte ord gælder
[Afsnit 1: Indledning]

- Tak for ordet. Tak til Fru Lisbeth Bech-Nielsen for samrådsspørgsmålene, og tak til digitaliserings- og ligestillingsministeren for besvarelse af spørgsmål 1, 3 og 4.
- Jeg vil nu besvare spørgsmål 2 vedrørende it-sikkerheden på Statens It's servere, som i Rigsrevisionens beretning nr. 6 af 2023 med Statsrevisorernes bemærkninger vurderes som *utilfredsstillende*.

***

- Jeg vil starte med at sige, at cyber- og informationssikkerhed ligger regeringen meget på sinde, og det er naturligvis noget, vi tager yderst alvorligt.
- Ord som "hackerangreb" og "cyberkrig" er blevet en del af vores ordforråd. Det er uhyggeligt – og alvorligt – når kritiske it-systemer bliver angrebet af usynlige og virtuelle våben, og det er noget, vi i høj grad må indstille os på er dagens og fremtidens uorden.
- Derfor skal vi løbende tilpasse sikkerhedsniveauet i takt med, at flere trusler dukker op. Vi skal være på forkant og løbende håndtere de sikkerhedsflanker, der opstår.
- Det er vi grundlæggende gode til i Danmark, og blandt andet derfor er vi et digitalt foregangsland. Den del er jeg enig med spørgeren i.

- Jeg er også enig med spørgeren i, at det er utilfredsstillende, at der løbende opstår huller - også for servere. Når man finder et sikkerhedshul på en server, skal det lukkes med en sikkerhedsopdatering.
- Statens It samarbejder med de enkelte myndigheder omkring problemstillingen. Men det er også vigtigt at sige, at ansvaret for, at systemerne opdateres og kan løse de forretningskritiske opgaver, er ressortministeriernes.
- Statens It kan i princippet tvangsopdatere alle de uopdaterede servere. Men konsekvensen vil være, at forretningskritiske it-systemer hos danske myndigheder ikke længere vil virke, og det betyder, at vi her har en udfordring.
- Denne problemstilling gør sig gældende ved, at Statens It *reelt* ikke kan opdatere serverne, før de pågældende myndigheder har kodet deres it-systemer om, og derfor har man behov for, at de pågældende myndigheder får gjort dét.
- Den problemstilling bliver også kaldt for 'teknisk gæld', som anvendes ifm. forældede it-systemer, hvis software fx kun er brugbar på kort sigt. Problemstillingen er desværre kendt i den statslige it-portefølje.

[Afsnit 2: Tiltag og foranstaltninger]

- Man kan dog øge sikkerheden ved at iværksætte kompenserende tiltag og foranstaltninger.
- Statens It har fx allerede i dag en række sikkerhedsværn, som filtrerer al datatrafik, der går ind på serverne. Derved filtreres uønsket trafik fra. Det er Rigsrevisionens vurdering, at den nuværende filtrering ikke kompenserer for de uopdaterede servere.
- Jeg tager Rigsrevisionen og Statsrevisorernes kritik meget alvorligt.
- Derfor har Finansministeriet bedt Statens It om at komme med et oplæg til, hvordan man via kompenserende tiltag og foranstaltninger kan øge sikkerheden. Og det haster. Jeg forventer, at oplægget vil ligge umiddelbart efter vinterferien.
- Derudover ved jeg, at Statens It sideløbende arbejder på en permanent og mere moderne løsning, der kan skrue op for filtrering af datatrafikken imellem serverne. I praksis vil det betyde, at serverne isoleres fra hinanden. Med den løsning mindskes risikoen for spredning af et hackerangreb. Og derfor vil konsekvensen blive mindre omfattende. Statens It har oplyst mig, at denne løsning vil være klar ultimo 2024 for de servere, der i dag udgør en risiko for spredning af cyberangreb.

- I forhold til samarbejdet mellem Statens It og myndighederne er der behov for en endnu tættere koordinering. Derfor har jeg på baggrund af Statsrevisorernes kritik bedt Statens It om at følge kontinuerligt og intensivt op på de myndigheder med it-systemer, der ikke tåler opdatering af den tilhørende server.
- Den opfølgning, forventer jeg, er afsluttet inden udgangen af 1. kvartal, hvor der fra myndighedernes side bør foreligge handleplaner for opdatering af ældre it-systemer.

[Afsnit 3: Statens Its egne servere]

- Endelig har jeg noteret, at Statens It selv har et antal servere, der ikke er sikkerhedsopdateret. Det er utilfredsstillende. Det er klart, at Statens It har en bunden opgave i at opdatere eller nedlægge disse, hvilket Finansministeriet har meddelt Statens It.
- Statens It har oplyst mig, at antallet af deres egne uopdaterede servere falder løbende og vil være håndteret inden udgangen af 1. kvartal 2024. Det er aftalt, at der fra Finansministeriets side følges op på dette.
- Det var ordene. Tak.