FOLKETINGET
RIGSREVISIONEN

December 2021

Rigsrevisionens notat om

tilrettelæggelsen af en større undersøgelse af it-beredskabet i staten

Tilrettelæggelsen af en større undersøgelse af it-beredskabet i staten

26. november 2021

RN 1111/21

I. Indledning

1. Statsrevisorerne anmodede på deres møde den 15. oktober 2021 om en undersøgelse af it-beredskabet i staten, jf. rigsrevisorlovens § 8, stk. 1. Dette notat beskriver, hvordan en eventuel større undersøgelse vil kunne tilrettelægges.

Undersøgelsen kan gennemføres, så Rigsrevisionen kan afgive en beretning til Statsrevisorerne i 2. halvår 2022.

II. Baggrund

2. Størstedelen af offentlige myndigheder er afhængige af it-systemer for at kunne løse deres opgaver. Større it-nedbrud og tab af data i myndighedernes kritiske kerneopgaver og underliggende it-systemer kan have store konsekvenser for staten, borgere og virksomheder. Det er derfor afgørende, at myndighederne har et tilstrækkeligt it-beredskab på plads. Beredskabet skal sikre, at myndighederne hurtigt kan håndtere større it-nedbrud og datatab i it-systemerne og har planer for alternative forretningsprocesser og minimering af konsekvenserne, indtil man kan vende tilbage til normal it-drift.

3. Staten har ifølge Digitaliseringsstyrelsen samlet set ca. 3.433 it-systemer. Ca. 590 af de 3.433 it-systemer er vurderet som kritiske for statens virke eller for samfundet som helhed.

4. Offentlige myndigheder har siden 2016 skullet følge den internationale standard for informationssikkerhed ISO 27001. Herunder er det konkretiseret, hvad myndighederne skal gøre i forhold til it-beredskabet.

5. Statsrevisorernes og Rigsrevisionens beretning nr. 20/2020 om Skatteministeriets it-beredskab viste, at Skatteministeriets it-beredskab for kritiske forretningsprocesser var utilfredsstillende og utilstrækkeligt. Statsrevisorerne ønsker på den baggrund en undersøgelse af, hvordan it-beredskabet i staten mere generelt er.

6. Statsrevisorerne stillede følgende spørgsmål:

- Har staten generelt implementeret et tilfredsstillende it-beredskab i overensstemmelse med de internationale standarder for informationssikkerhed og it-beredskab? Hvem har tilsynsforpligtelsen hermed i de enkelte ministerier?
- Har statens myndigheder generelt taget stilling til, hvordan de vil implementere sikkerhedsforanstaltningerne, så de passer til den enkelte myndigheds risici og kritiske forretningsprocesser?
- Er statens vejledninger om implementering af it-beredskab tilfredsstillende, og sikres deling af viden på tværs af ministerierne?
- Hvilket tværministerielt it-beredskab kan sættes i værk, hvis flere af statens myndigheder rammes af it-sikkerhedshændelser på samme tid?

III. Tilrettelæggelsen af undersøgelsen

7. Vi forventer at udvælge et antal ministerier til at indgå i undersøgelsen, hvor vi vil undersøge it-beredskabet for udvalgte it-systemer. Vi vil udvælge ministerierne blandt de ministerområder, som har de mest kritiske it-systemer. Det kan fx være it-systemer, som håndterer store pengestrømme, it-systemer, som er centrale for ministeriets opgavevaretagelse, eller it-systemer, som understøtter samfundskritiske opgaver.

Vi vil derudover undersøge it-beredskabet i Statens It, som leverer it-ydelser til ca. 31.000 medarbejdere i staten og til 19 ministerområder. Statens It leverer bl.a. en it-arbejdsplads til statens medarbejdere, herunder hardware som computere og software, fx brugeradgangssystemer og Microsoft Office. Derudover drifter Statens It også nogle af de statslige institutioners it-fagsystemer. It-nedbrud eller datatab i it-systemerne i Statens It vil derfor påvirke mange af statens institutioner.

8. Rigsrevisionen forventer at opdele undersøgelsen i 3 dele.

I den *første del* af undersøgelsen vil vi undersøge, om de udvalgte institutioner har et tilfredsstillende grundlag for at etablere et dækkende it-beredskab. Her vil vi undersøge, om ministerierne har taget stilling til, hvordan de vil implementere ISO 27001-standarden.

Vi vil også undersøge, om ministerierne har kortlagt, hvilke it-systemer der er kritiske for ministeriets kerneopgaver, og om ministerierne har et overblik over det eksisterende it-beredskab. Derudover vil vi undersøge, om ministerierne anvender risiko- og konsekvensvurderinger til at tilrettelægge it-beredskabet.

Vi vil endvidere undersøge, hvordan arbejdet med at sikre implementeringen af et dækkende it-beredskab sker på ministerområderne. Herunder vil vi undersøge, om ministerierne fører tilsyn med, om ministeriernes institutioner har implementeret informationssikkerhed, herunder et tilfredsstillende it-beredskab.

9. I den *anden del* af undersøgelsen vil vi undersøge, om de udvalgte institutioner har udarbejdet it-beredskabsplaner for den interne krisehåndtering i institutionen, og om institutionerne har sikret, at der er udarbejdet tekniske planer for at reetablere it-systemerne efter et større nedbrud. Her vil vi undersøge, om it-beredskabsplanerne indeholder de mest centrale elementer, fx om planen beskriver, hvordan den aktiveres, om planen indeholder kontaktinformationer til centrale aktører, og om planen beskriver rolle- og ansvarsfordelingen mellem aktørerne. Vi vil også undersøge, om it-beredskabsplanerne er blevet testet årligt, og om testene indeholder de mest centrale elementer, fx om funktionaliteten af it-systemet er testet, og om reetableringen af it-systemet sker inden for den aftalte tidsperiode.

10. I den *tredje del* af undersøgelsen vil vi undersøge, om Digitaliseringsstyrelsen på tilfredsstillende vis har understøttet statens institutioner i at etablere et dækkende it-beredskab.

Digitaliseringsstyrelsen har en koordinerende rolle i forhold til at gennemføre informationssikkerhedsaktiviteter, udarbejde analyser og udvikle forskellige former for vejledningsmaterialer og hjælpeværktøjer om informationssikkerhed til den offentlige sektor. Styrelsen skal herunder understøtte myndighedernes implementering af it-beredskabet, bl.a. gennem vejledninger og kampagner. På hjemmesiden sikkerdigital.dk vejleder Digitaliseringsstyrelsen offentlige myndigheder og borgere om it-sikkerhed.

For det første vil vi om muligt undersøge, om Digitaliseringsstyrelsens vejledninger om implementering af it-beredskabet er tilfredsstillende. Her vil vi undersøge, om vejledningerne indeholder konkrete og relevante emner og anbefalinger, der kan understøtte ministeriernes arbejde med at implementere et dækkende it-beredskab. Det kan fx være vejledning om risikovurderinger, leverandørstyring, udarbejdelse af it-beredskabsplaner og kommunikation. Vi vil også undersøge, om Digitaliseringsstyrelsen har sikret, at vejledningsmaterialet er anvendeligt for brugerne.

For det andet vil vi undersøge, om Digitaliseringsstyrelsen har understøttet videndeling om it-beredskabet på tværs af statens institutioner.

Digitaliseringsstyrelsen driver forskellige råd og fora, der skal styrke koordinering, videndeling og håndtering af informationssikkerhedshændelser på tværs af de offentlige myndigheder og den private sektor. Fx driver Digitaliseringsstyrelsen *Statens netværk for informationssikkerhed*, hvor der deltager personer, som arbejder med informationssikkerhed på ministerområderne. Netværket skal understøtte videndeling og erfaringsudveksling inden for den praktiske håndtering af relevante emner inden for it-sikkerhed.

11. Vi vil i undersøgelsen afdække, om der er etableret et overordnet og tværgående beredskab, som kan sættes i værk ved fx større cyberangreb rettet mod samfundskritiske områder, som påvirker hele staten.

Vi vil undersøge, om der er udarbejdet overordnede beredskabsplaner, som kan anvendes i forbindelse med et større tværgående it-nedbrud eller cyberangreb i staten. Vi vil også undersøge, om der er udført tests eller øvelser af beredskabsplanerne.

12. Undersøgelsen er afgrænset til at afdække statens it-beredskab og inddrager dermed ikke regionernes it-beredskab, fx på hospitaler. Endvidere afgrænser vi os fra at se på forsyningssektoren, fx forsyning af el og gas, som har en særskilt lovgivning vedrørende it-beredskab. Undersøgelsen har derimod fokus på de statslige myndigheders implementering af ISO 27001-standarden, som alle offentlige myndigheder er forpligtede til at implementere.

13. Rigsrevisionen skal for god ordens skyld understrege, at der undervejs vil kunne ske ændringer i forhold til det skitserede oplæg.

Lone Strøm