FINANSMINISTERIET

Finansministeriet · Christiansborg Slotsplads 1 · 1218 København K

Statsrevisorernes Sekretariat

Folketinget Christiansborg

ministersvar@ft.dk

09.02.2024

Til Statsrevisorerne

Ministerredegørelse til Statsrevisorernes beretning nr. 6/2023 om It-sikkerheden på Statens It's servere

Jeg har modtaget Statsrevisorernes bemærkninger fra den 4. december 2023 til Rigsrevisionens beretning nr. 6/2023 om it-sikkerheden på Statens It's servere. I det følgende redegøres for de overvejelser, som beretningen har givet anledning til. Redegørelsen forholder sig til såvel beretningens indhold og konklusioner samt Statsrevisorernes bemærkninger.

Indledningsvist vil jeg gerne kvittere for Statsrevisorernes bemærkninger og Rigsrevisionens beretning, som berører et vigtigt emne.

Statsrevisorerne udtaler i bemærkningerne til beretningen en kritik af sikkerheden på Statens It's servere. Statens It oplyser mig, at de har et stort fokus på at sikre Statens It's egen og kundernes it-sikkerhed. Henset til ansvarsfordelingen mellem Statens It og Statens It's kunder er det udfordrende at sikre, at alle servere kan sikkerhedsopdateres. Derfor tager jeg Rigsrevisionens undersøgelse af it-sikkerheden på Statens It's servere og Statsrevisorernes bemærkninger til efterretning.

Statsrevisorerne hæfter sig ved følgende undersøgelsesresultater:

1. 537 servere hos Statens It kan ikke længere sikkerhedsopdateres, da servernes levetid er udløbet. Dette svarer til ca. 10 % af de i alt 5.353 undersøgte servere, som Statens It varetager driften af på vegne af 46 myndigheder.

2. Den fortsatte brug af servere, der ikke længere kan sikkerhedsopdateres, gør, at der er risiko for, at et cyberangreb kan sprede sig mellem servere og mellem myndigheder, da sårbarheder hos én myndighed kan udsætte andre myndigheder for it-sikkerhedsmæssige risici.

3. For 178 servere mangler Statens It viden om servernes type, hvilket bevirker, at Statens It ikke efterlever kravene i ISO 27001 angående fuldstændigt overblik over serverporteføljen.

4. Statens It har ikke procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres. Samtidig har Statens It ikke etableret det fornødne samarbejde med myndighederne til, at serverne kan opgraderes eller nedlægges, hvis serverne ikke længere kan sikkerhedsopdateres. Statens It er bl.a. udfordret af, at serverne ikke altid kan opgraderes eller nedlægges, fordi de enkelte myndigheder ikke har sikret, at deres fagsystemer er kompatible med nye servere.

5. Statens It estimerede i marts 2022, at ca. 26 % af deres egne servere ikke kunne sikkerhedsopdateres.

Statens It har oplyst mig, at de er enige med Rigsrevisionen i, at løbende og rettidig opgradering af servere er vigtigt for it-sikkerheden. Statens It er sat i verden for bl.a. at sikre en sikker og stabil it-drift i staten, og Statens It tager derfor problemstillingen alvorligt.

Jeg hæfter mig ved, at Statens It ikke kan opdatere eller nedlægge servere, før myndighederne har sikret, at deres it-systemer er kompatible med opdaterede servere. Jeg har derfor noteret mig Rigsrevisionens anbefaling om, at Finansministeriet bør overveje, om arbejds- og ansvarsfordelingen mellem myndighederne og Statens It i forhold til servere er hensigtsmæssig. Problemstillingen skal løses igennem et tættere samarbejde mellem Statens It og myndighederne samt implementering af kompenserende foranstaltninger.

På den baggrund kan jeg oplyse, at Statens It har iværksat en række initiativer, der skal forbedre styringen af opdateringstilstanden på Statens It's servere og implementere supplerende, mitigerende foranstaltninger omkring serverne. I det følgende redegøres for fire konkrete initiativer.

- *Initiativ 1: Udarbejdelse af handleplaner og kontinuerlig opfølgning*
  Statens It vil intensivere dialogen med de myndigheder, der er tilknyttet Statens It. Myndighederne skal i regi af et nyt databehandlerparadigme udarbejde handleplaner for de it-systemer, der i dag ikke kan afvikles på opdaterede servere. Handlingsplanerne skal være på plads ved udgangen af 1. kvartal 2024.

  SIT vil have fokus på, at der sker en forankring af handleplanerne på et højt ledelsesmæssigt niveau. Statens It vil i den forbindelse etablere en fast opfølgningssystematik for handleplanerne.

- *Initiativ 2: Højne datakvaliteten vedrørende serveres opdateringstilstand*
  Statens It vil højne datakvaliteten vedrørende servernes opdateringstilstand, herunder udnytte eksisterende værktøjer bedre. Statens It vil derfor undersøge, hvilke eksisterende og nye værktøjer, der kan understøtte dette. Stillingtagen til værktøjerne vil foreligge inden udgangen af 2. kvartal 2024.

- *Initiativ 3: Kompenserende foranstaltninger*
  Statens It vil på baggrund af handleplanerne foretage en konkret vurdering af behovet for at implementere kompenserende foranstaltninger for serverne, dette fx gennem en stærkere filtrering af datatrafikken, så Statens It i højere grad kan afsondre uopdaterede servere fra opdaterede servere, således at sikkerheden specifikt for de uopdaterede servere styrkes. Vurderingen foretages i samarbejde med Statens It's kunder og vil være på plads ved udgangen af 2. kvartal 2024.

- *Initiativ 4: Segmenteringsprojekt*
  Endeligt har Statens It orienteret mig om, at de har igangsat et større infrastrukturprojekt, der segmenterer alle myndighedernes servere. En sådan segmentering vil reducere risikoen for spredning af et cyberangreb yderligere. Segmenteringsprojektet er ressourcekrævende og opdeles i flere faser. Første fase vedrører de servere, der i dag har størst risiko for spredning af et cyberangreb mellem myndigheder, og forventes færdigimplementeret ultimo 2024.

I perioden frem til implementering af ovenstående initiativer arbejder Statens It i samarbejdet med myndighederne på at nedbringe antallet af servere, der ikke kan sikkerhedsopdateres.

Afslutningsvist bemærker jeg, at Statens It selv har et mindre antal servere, der ikke kan sikkerhedsopdateres. Det skyldes samme problematik. Der har siden Rigsrevisionens påbegyndelse af revisionen været et skærpet fokus på disse servere hos Statens It og ved udgangen af januar 2024 er 18 servere nedlagt eller opdateret.

Finansministeriets departement følger Statens It's initiativer og fremdrift tæt.

Med ovenstående redegørelse håber jeg, at der er givet et fyldestgørende svar på Statsrevisorernes bemærkninger og Rigsrevisionens beretning om it-sikkerhed på Statens It's servere.

En kopi af denne redegørelse er sendt til Rigsrevisionen.

Med venlig hilsen

Nicolai Wammen