FOLKETINGET
RIGSREVISIONEN

Marts 2024

Rigsrevisionens notat om
beretning om

it-sikkerheden på Statens It's servere

Vedrører:

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

4. marts 2024

RN 302/24

Finansministerens redegørelse af 9. februar 2024

1. Rigsrevisionen gennemgår i dette notat de initiativer, som finansministeren har iværksat som følge af Statsrevisorernes bemærkninger og beretningens konklusioner. Dette sker med henblik på at vurdere, om initiativerne adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning.

Konklusion

Finansministeren tager Rigsrevisionens undersøgelse og Statsrevisorernes bemærkninger til efterretning og oplyser, at Statens It er enig i, at løbende og rettidig opgradering af servere er vigtig for it-sikkerheden.

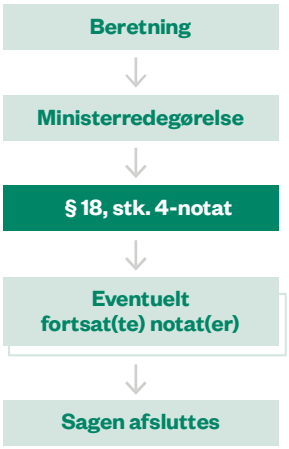
Finansministeren hæfter sig ved, at Statens It ikke kan opdatere eller nedlægge servere, før myndighederne har sikret, at deres it-systemer kan fungere på opdaterede servere. Ministeren har derfor noteret sig Rigsrevisionens anbefaling om, at Finansministeriet bør overveje, om arbejds- og ansvarsfordelingen mellem myndighederne og Statens It i forhold til servere er hensigtsmæssig. Ministeren oplyser, at problemstillingen skal løses gennem et tættere samarbejde mellem Statens It og myndighederne samt ved implementering af kompenserende foranstaltninger.

Finansministeren oplyser, at Statens It har iværksat en række initiativer, der skal forbedre styringen af tilstanden på Statens It's servere og implementere supplerende, mitigerende foranstaltninger.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Statens It's opfølgning på myndighedernes handlingsplaner for de it-systemer, der ikke kan afvikles på opdaterede servere, herunder etablering af en fast systematik for opfølgning
- Statens It's arbejde med at højne datakvaliteten vedrørende serveres opdateringstilstand
- Statens It's arbejde med at implementere kompenserende foranstaltninger for servere, der ikke kan opdateres

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

- Statens It's gennemførelse af et projekt, der skal reducere risikoen for spredning af cyberangreb
- Statens It's arbejde med at nedlægge eller opdatere egne servere, der ikke længere kan sikkerhedsopdateres.

I. Baggrund

Server
En server er en computer, som indgår i it-infrastrukturen og indeholder funktionalitet, der benyttes af andre computere. Servere bruges fx til opbevaring og styring af filer, databaser og programmer. Servere består både af hardware og software og kan være både fysiske og virtuelle. I dette notat bruger vi begrebet server om servernes operativsystem, som er den grundlæggende software på en server.

2. Rigsrevisionen afgav i december 2023 en beretning om it-sikkerheden på Statens It's servere. Beretningen handlede om, hvorvidt Statens It under Finansministeriet har sikret, at Statens It's servere kan sikkerhedsopdateres, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering.

Servere er en vigtig del af statens it-infrastruktur. En server har en begrænset levetid. Ved udløbet af serverens levetid kan serveren ikke længere sikkerhedsopdateres.

3. Da Statsrevisorerne behandlede beretningen, fandt de det utilfredsstillende, at Statens It ikke har sikret, at alle Statens It's servere kan sikkerhedsopdateres. Statens It har ikke opgraderet eller nedlagt servere, i takt med at serverne ikke længere kan sikkerhedsopdateres, og Statens It har ikke et fuldt overblik over de servere, de er ansvarlige for. Dette gør, at Statens It har dårlige forudsætninger for at reagere hurtigt på cyberangreb og nye cybertrusler.

Statsrevisorerne fandt det bekymrende, at Statens It's utilstrækkelige sikkerhedsopdateringer og utilstrækkelige kompenserende foranstaltninger indebærer risiko for, at borgeres og virksomheders personoplysninger og forretningskritiske data kan blive misbrugt eller ødelagt. Statsrevisorerne fandt det også bekymrende, at borgeres og virksomheders tillid til offentlige myndigheder kan blive svækket som følge heraf.

4. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

5. Bilag 1 viser Folketingets behandling af beretningen.

II. Gennemgang af ministerens redegørelse

Procedurer for opgradering eller nedlæggelse af servere

6. Statsrevisorerne bemærkede, at Statens It ikke har 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.

Statsrevisorerne var enige i Rigsrevisionens anbefaling om, at Finansministeriet bør overveje, om arbejds- og ansvarsfordelingen mellem myndighederne og Statens It er hensigtsmæssig i forhold til servere.

7. Finansministeren oplyser i sin redegørelse til beretningen, at Statens It vil intensivere dialogen med de myndigheder, der er tilknyttet Statens It. Myndighederne skal udarbejde handleplaner for de it-systemer, der i dag ikke kan afvikles på opdaterede servere. Handleplanerne skal være på plads ved udgangen af 1. kvartal 2024.

Finansministeren oplyser desuden, at Statens It vil have fokus på, at der sker en forankring af handleplanerne på et højt ledelsesmæssigt niveau, og at Statens It i den forbindelse vil etablere en fast systematik for opfølgning på handleplanerne.

8. Rigsrevisionen finder Statens It's initiativer relevante. Rigsrevisionen vil fortsat følge Statens It's opfølgning på myndighedernes handlingsplaner for de it-systemer, der ikke kan afvikles på opdaterede servere, herunder etablering af en fast systematik for opfølgning.

Statens It's overblik over serverne

9. Statsrevisorerne bemærkede, at Statens It for 178 servere mangler viden om servernes type, hvilket bevirker, at Statens It ikke efterlever kravene i ISO 27001 i forhold til fuldstændigt overblik over serverporteføljen.

Det fremgik også af beretningen, at Statens It ikke har et fuldstændigt overblik over serverne. Statens It's overblik er baseret på et digitalt værktøj, som trækker informationer fra alle servere, hvor der er installeret en agent. Flere af Statens It's servere har dog ikke en agent installeret. Dette gælder bl.a. servere, der er så gamle, at agenten ikke kan installeres. Statens It oplyste, at manglende agenter på serverne har skabt et ufuldstændigt overblik over serverne, og at Statens It arbejder på at forbedre datakvaliteten. Statens It har i løbet af undersøgelsen løbende gennemgået serverne manuelt for at fremskaffe oplysninger.

Agent
En agent er et stykke software, som installeres på en server, hvor den opsamler og leverer information om serveren til en database.

10. Finansministeren oplyser i sin redegørelse, at 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. En stillingtagen til værktøjerne vil foreligge inden udgangen af 2. kvartal 2024.

11. Rigsrevisionen finder det positivt, at Statens It vil højne datakvaliteten vedrørende servernes opdateringstilstand. Rigsrevisionen vil fortsat følge Statens It's arbejde hermed.

Kompenserende foranstaltninger

12. Det fremgik af beretningen, at Statens It ikke har gennemført tilstrækkelige kompenserende foranstaltninger for de servere, der ikke længere kan sikkerhedsopdateres.

13. Finansministeren oplyser i sin redegørelse, at Statens It på baggrund af handleplanerne vil foretage en konkret vurdering af behovet for at implementere kompenserende foranstaltninger for serverne, så Statens It i højere grad kan afsondre uopdaterede servere fra opdaterede servere, således at sikkerheden specifikt styrkes for de uopdaterede servere. Vurderingen foretages i samarbejde med Statens It's kunder og vil være på plads ved udgangen af 2. kvartal 2024.

14. Rigsrevisionen finder det positivt, at Statens It vil iværksætte en række kompenserende foranstaltninger for de servere, der ikke længere kan sikkerhedsopdateres. Rigsrevisionen vil fortsat følge Statens It's arbejde hermed.

Segmentering af servere

15. Det fremgik af beretningen, at Statens It har en række foranstaltninger, som kan reducere risikoen for, at cyberangreb kan sprede sig. Der er dog stadig risiko for, at cyberangreb kan sprede sig mellem servere og mellem myndigheder. Sårbarheder hos én myndighed kan derfor udsætte andre myndigheder for it-sikkerhedsmæssige risici.

Segmentering
Ved segmentering opdeles netværket i 2 eller flere uafhængige miljøer. Formålet er, at en hacker eller virus ikke har adgang til hele netværket samtidigt.

16. Finansministeren oplyser i sin redegørelse, at Statens It har igangsat et infrastrukturprojekt, der segmenterer alle myndighedernes servere. Ministeren oplyser, at dette vil reducere risikoen for spredning af et cyberangreb yderligere.

Projektet er ifølge finansministeren resursekrævende 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.

17. Rigsrevisionen finder det positivt, at Statens It har igangsat et projekt, der skal reducere risikoen for, at cyberangreb kan sprede sig. Rigsrevisionen vil fortsat følge Statens It's arbejde hermed.

Statens It's egne servere

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

Det fremgik af beretningen, at disse servere bl.a. bruges til intern drift i Statens It, men også af myndigheder, der er kunder hos Statens It, fx gennem brug af tværgående it-systemer i staten. Det fremgik også af beretningen, at Statens It forventede at have opgraderet eller nedlagt deres egne servere, der ikke kan sikkerhedsopdateres, i 1. kvartal 2024.

19. Finansministeren oplyser i sin redegørelse, at Statens It siden Rigsrevisionens opstart af undersøgelsen har haft et skærpet fokus på disse servere, og ved udgangen af januar 2024 er 18 servere nedlagt eller opdateret.

20. Rigsrevisionen finder det positivt, at Statens It er i gang med at opgradere og nedlægge egne servere. Rigsrevisionen vil fortsat følge Statens It's arbejde med at nedlægge eller opdatere de servere, der ikke længere kan sikkerhedsopdateres.

Birgitte Hansen

Bilag 1. Folketingets behandling af beretningen

Beretning (nr.), dato for Statsrevisorernes mødebehandling og minister-redegørelse(r)	Behandlet i udvalg	Teknisk gennemgang ved Statsrevisorerne og Rigsrevisionen	Udvalgs-spørgsmål (nr.)	Indkaldt til samråd	Statsrevisorerne har holdt møde med ministeren	§ 20-spørgsmål
It-sikkerheden på Statens It's servere (nr. 6/2023) 04-12-2023 **Minister-redegørelse:** Finansministeren: 09-02-2024	Udvalget for Digitalisering og It: 06-12-2023 Finansudvalget: 14-12-2023		Digitaliserings- og ligestillings-ministeren: 09-01-2024 (77) Finansministeren: 09-01-2024 (78)	Udvalget for Digitalisering og It: 09-01-2024	Finansministeren og digitaliserings- og ligestillings-ministeren: 22-02-2024	