FOLKETINGET
RIGSREVISIONEN

September 2025

Rigsrevisionens notat om
beretning om

it-sikkerheden på Statens It's servere

Opfølgning i sagen om it-sikkerheden på Statens It's servere (beretning nr. 6/2023)

26. august 2025

RN C113/25

I. Baggrund og konklusion

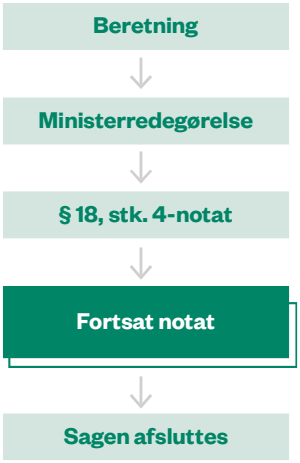
1. Rigsrevisionen følger i dette notat op på sagen om it-sikkerheden på Statens It's servere, som blev indledt med en beretning i 2023. Opfølgningen sker med henblik på at vurdere, om de initiativer, som finansministeren har stillet Statsrevisorerne i udsigt i lyset af Statsrevisorernes bemærkninger og Rigsrevisionens beretning, er gennemført. Vi har tidligere behandlet sagen i et notat til Statsrevisorerne af 4. marts 2024.

2. Beretningen handlede om, hvorvidt Statens It under Finansministeriet havde sikret, at Statens It's servere kan sikkerhedsopdateres, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering.

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

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

Sagsforløb for en større undersøgelse



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

Konklusion

Statens It har sikret, at alle myndigheder har udarbejdet en plan for, hvordan de vil håndtere it-systemer, der ikke kan afvikles på opdaterede servere. Statens It har fulgt op på planen og vil også fremadrettet følge systematisk op. Statens It har forbedret kvaliteten af data om servernes opdateringstilstand. Konkret har Statens It etableret et overblik over alle servere, de har ansvaret for, herunder servernes tilstand. Statens It har også håndteret i alt 578 servere, der ikke kunne opdateres, og sikret, at der ikke længere er servere hos Statens It selv, som ikke kan opdateres.

Rigsrevisionen vurderer på den baggrund, at disse dele af sagen kan afsluttes.

Statens It er i gang med at implementere et projekt, der skal reducere risikoen for spredningen af cyberangreb. Projektet er forsinket og følger dermed ikke den oprindelige tidsplan. Det finder Rigsrevisionen ikke tilfredsstillende.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Statens It's gennemførelse af et projekt, der skal reducere risikoen for spredning af cyberangreb.

II. Status på sagen

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. 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.	Behandles og afsluttes i dette notat.
2. Statens It's arbejde med at højne datakvaliteten vedrørende serveres opdateringstilstand.	Behandles og afsluttes i dette notat.
3. Statens It's arbejde med at implementere kompenserende foranstaltninger for servere, der ikke kan opdateres.	Behandles og afsluttes i dette notat.
4. Statens It's gennemførelse af et projekt, der skal reducere risikoen for spredning af cyberangreb.	Behandles i dette notat og følges fortsat.
5. Statens It's arbejde med at nedlægge eller opdatere egne servere, der ikke længere kan sikkerhedsopdateres.	Behandles og afsluttes i dette notat.

Kompenserende foranstaltning
Ved afsondring begrænses en servers mulighed for at kommunikere med andre servere. Dette mindsker risikoen for, at et cyberangreb spreder sig mellem serverne. Afsondring er derfor en kompenserende foranstaltning for servere, der ikke kan sikkerhedsopdateres.

III. Statens It's initiativer

5. Vi gennemgår i det følgende Statens It's initiativer i forhold til opfølgningspunkterne.

6. Opfølgningen er baseret på gennemgang af materiale fra Statens It, herunder en teknisk gennemgang.

Statens It's opfølgning på myndighedernes handlingsplaner

Statens It har sikret, at alle 47 myndigheder, der havde it-systemer, som ikke kunne afvikles på opdaterede servere, har udarbejdet en handlingsplan for, hvordan de vil håndtere dette. Statens It har løbende fulgt op på myndighedernes handlingsplaner og vil også fremadrettet sikre en fast systematik for opfølgning. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

7. Statsrevisorerne bemærkede, at Statens It ikke havde procedurer, der sikrede, at de løbende og rettidigt kunne opgradere eller nedlægge servere, der ikke længere kunne sikkerhedsopdateres. Samtidig havde Statens It ikke etableret det fornødne samarbejde med myndighederne til, at serverne kunne opgraderes eller nedlægges, hvis serverne ikke længere kunne sikkerhedsopdateres. Statens It var bl.a. udfordret af, at serverne ikke altid kunne opgraderes eller nedlægges, fordi de enkelte myndigheder ikke havde sikret, at deres fagsystemer var kompatible med nye servere.

8. Finansministeren oplyste i sin redegørelse til beretningen, at Statens It inden udgangen af 1. kvartal 2024 ville sikre, at alle myndigheder, der var tilknyttet Statens It, udarbejdede handlingsplaner for de it-systemer, der ikke kunne afvikles på opdaterede servere. Statens It ville desuden have fokus på, at der skete en forankring af handlingsplanerne på et ledelsesmæssigt niveau, og at der blev etableret en fast opfølgningssystematik på handlingsplanerne.

9. Vores opfølgning viser, at 47 myndigheder havde 578 servere hos Statens It, der ikke længere kunne opdateres pr. 1. kvartal 2024.

Statens It har sikret, at alle 47 myndigheder har udarbejdet handlingsplaner for de it-systemer, der ikke kan afvikles på opdaterede servere. Handlingsplanerne er godkendt af myndighedernes direktioner og var færdige ultimo februar 2024.

Statens It har to gange fulgt op på handlingsplanerne. Først i maj 2024 og senest i oktober 2024, hvor Statens It meldte ud, at hvis de ikke modtog dokumentation for, at myndighederne var i gang med at håndtere de servere, der ifølge handlingsplaner ville blive håndteret i 2024, ville de begynde at afsondre dem. Afsondring begrænser serveres mulighed for at kommunikere med andre servere, hvilket mindsker risikoen for, at et cyberangreb spreder sig mellem serverne. Afsondring er derfor en kompenserende foranstaltning for servere, der ikke kan sikkerhedsopdateres.

Statens It har også oplyst, at de fremadrettet vil følge op på myndighedernes planer på fire årlige statusmøder med myndighederne. Vi kan konstatere, at Statens It har afholdt langt hovedparten af de planlagte møder i 2025. Statens It vil kræve, at myndighederne udarbejder handlingsplaner for it-systemer, der ikke kan afvikles på opdaterede servere. Statens It vil afsondre serverne, hvis myndighederne ikke udarbejder handlingsplaner eller sikrer, at serverne kan opgraderes eller nedlægges.

Datakvaliteten vedrørende serveres opdateringstilstand

Statens It har videreudviklet deres rapport over opdateringstilstanden på deres servere. Det er Rigsrevisionens vurdering, at det har ført til bedre datakvalitet i forhold til servernes opdateringstilstand. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

10. Statsrevisorerne bemærkede, at Statens It ikke havde et fuldt overblik over de servere, de var ansvarlige for. Dette gjorde, at Statens It havde dårligere forudsætninger for at reagere hurtigt på cyberangreb og nye cybertrusler.

11. Finansministeren oplyste i sin redegørelse til beretningen, at Statens It ville højne datakvaliteten vedrørende servernes opdateringstilstand, herunder udnytte eksisterende værktøjer bedre. Statens It ville derfor undersøge, hvilke eksisterende og nye værktøjer der kunne understøtte dette. Stillingtagen til værktøjerne ville foreligge inden udgangen af 2. kvartal 2024.

Sårbarhedsscanning
En sårbarhedsscanning er et værktøj, der indsamler data om, hvad der er installeret på serverne, analyserer de indsamlede data og danner overblik over det aktuelle sikkerhedsniveau for serverne. Sårbarhedsscanningen rapporterer eventuelle kendte sårbarheder, der kan udgøre en sikkerhedsrisiko.

12. Vores opfølgning viser, at Statens It har opdateret og forbedret deres rapport over opdateringstilstanden på deres servere. Dermed har Statens It et overblik over alle de servere, de har ansvaret for, herunder deres tilstand. Statens it har anvendt forskellige værktøjer til at skabe dette overblik, bl.a. sårbarhedscanninger og Service Management System.

Kompenserende foranstaltninger for servere, der ikke kan opdateres

Statens It har håndteret de i alt 578 servere, der ikke kunne opdateres. 542 servere er enten blevet nedlagt eller opgraderet. Derudover har Statens It implementeret kompenserende foranstaltninger for 36 servere ved at afsondre dem. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Service Management System
Et Service Management System er et værktøj, der anvendes til at styre leveringen af services for it-systemer og bl.a. giver overblik over, hvilke systemer der er installeret på serverne.

13. Statsrevisorerne bemærkede, at den fortsatte brug af servere, der ikke længere kunne sikkerhedsopdateres, gjorde, at der var risiko for, at et cyberangreb kunne sprede sig mellem servere og mellem myndigheder, da sårbarheder hos én myndighed kunne udsætte andre myndigheder for it-sikkerhedsmæssige risici.

14. Finansministeren oplyste i sin redegørelse til beretningen, at Statens It på baggrund af handlingsplanerne ville foretage en konkret vurdering af behovet for at implementere kompenserende foranstaltninger for serverne. Vurderingen ville foreligge inden udgangen af 2. kvartal 2024.

15. Rigsrevisionens opfølgning viser, at Statens It i juli 2025 enten havde nedlagt eller opgraderet 542 servere ud af i alt 578 servere, der ikke kunne opdateres. De resterende 36 servere var blevet afsondret, dvs. servernes mulighed for at kommunikere med andre servere var blevet begrænset. Statens It oplyser, at der ikke er blevet etableret andre kompenserende foranstaltninger, da det er Statens It's vurdering, at afsondring opfylder det sikkerhedsmæssige behov for at reducere risikoen for spredning af cyberangreb. Rigsrevisionen er enig heri.

Statens It's arbejde med at reducere risikoen for spredning af cyberangreb

Statens It's implementering af det projekt, der skal reducere risikoen for cyberangreb, følger ikke den oprindelige tidsplan. Første fase af projektet er igangsat, men er ikke blevet færdigimplementeret. Det finder Rigsrevisionen ikke tilfredsstillende. Rigsrevisionen vil fortsat følge Statens It's arbejde med at implementere segmenteringsprojektet.

16. Det fremgik af beretningen, at Statens It havde en række foranstaltninger, som kunne reducere risikoen for, at cyberangreb kunne sprede sig. Der var dog stadig en risiko for, at cyberangreb kunne sprede sig mellem servere og mellem myndigheder.

17. Finansministeren oplyste i sin redegørelse til beretningen, at Statens It på den baggrund havde igangsat et projekt, der skulle segmentere alle myndighedernes servere. Segmenteringen af myndighedernes servere er iværksat for fremadrettet at reducere risikoen for, at cyberangreb kan sprede sig mellem myndighedernes servere. Segmentering er en langsigtet og strukturel foranstaltning til at minimere risikoen for spredning af cyberangreb, mens afsondring er en kortsigtet og kompenserende foranstaltning.

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

Første fase af projektet ville vedrøre de servere, hvor risikoen for spredning af et cyberangreb mellem myndigheder var størst. Ministeren oplyste, at første fase ville være implementeret ultimo 2024. Ministeren oplyste ikke, hvornår de resterende faser forventes at være implementeret.

18. Vores opfølgning viser, at Statens It i december 2024 har igangsat, men ikke færdigimplementeret, første fase af projektet. Statens It oplyser, at de forventer, at første fase vil være gennemført i løbet af 2025, og at projektet vil være endeligt færdigt i 2027. Statens It har desuden oplyst, at de vil håndtere servere, der ikke er opdaterede, gennem afsondring, indtil segmenteringsprojektet er fuldt implementeret.

Statens It's arbejde med at nedlægge eller opdatere egne servere

Statens It har nedlagt eller opgraderet alle 67 egne servere, der ikke kunne sikkerhedsopdateres. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

19. Statsrevisorerne bemærkede, at Statens It i marts 2022 estimerede, at ca. 26 % af deres egne servere, svarende til 67 servere, ikke kunne sikkerhedsopdateres.

20. Finansministeren oplyste i sin redegørelse til beretningen, at Statens It siden påbegyndelse af Rigsrevisionens undersøgelse har haft et skærpet fokus på disse servere, og ved udgangen af januar 2024 var 18 servere nedlagt eller opgraderet.

21. Vores opfølgning viser, at Statens It har nedlagt eller opgraderet de resterende servere. Således er alle 67 servere nu håndteret.

---

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

23. Bilag 1 viser Folketingets behandling af beretningen.

Birgitte Hansen

Bilag 1. Folketingets behandling af beretningen

Beretning (nr.), dato for Statsrevisorernes mødebehandling og ministerredegørelse(r)	Behandlet i udvalg	Gennemgang ved Statsrevisorerne og Rigsrevisionen	Udvalgsspørgsmål (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 **Ministerredegørelse:** Finansministeren: 09-02-2024	Udvalget for Digitalisering og It: 06-12-2023 Finansudvalget: 14-12-2023		Digitaliserings- og ligestillingsministeren: 09-01-2024 (77) Finansministeren: 09-01-2024 (78)	Udvalget for Digitalisering og It: 09-01-2024	Finansministeren og digitaliserings- og ligestillingsministeren: 22-02-2024	