FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2023
– 6/2023

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

It-sikkerheden på Statens It's servere

6/2023

Beretning om

it-sikkerheden på Statens It's servere

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2023

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Finansministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.

På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i marts 2024.

Ministerens redegørelse, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2023, som afgives i februar 2025.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

ISSN 2245-3008
ISBN online 978-87-7434-827-6

Statsrevisorernes bemærkning

Beretning om it-sikkerheden på Statens It's servere

Center for Cybersikkerhed under Forsvarets Efterretningstjeneste vurderer, at truslen i Danmark fra cyberkriminalitet og cyberspionage er meget høj, og at truslen fra cyberaktivisme er høj.

Statens It har ansvaret for it-driften og it-sikkerheden for 151 myndigheder på tværs af 21 ministerområder. Statens It er ansvarlig for, at Statens It's servere løbende sikkerhedsopdateres, og at servere opgraderes, når serverens levetid er udløbet, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering.

Statsrevisorerne finder 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 dårligere forudsætninger for at reagere hurtigt på cyberangreb og nye cybertrusler.

Statsrevisorerne finder 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 finder det også bekymrende, at borgeres og virksomheders tillid til offentlige myndigheder kan blive svækket som følge deraf.

Statsrevisorerne

4. december 2023

Mette Abildgaard
Leif Lahn Jensen
Mikkel Irminger Sarbo
Serdal Benli
Lars Christian Lilleholt
Monika Rubin

Statsrevisorerne har bl.a. hæftet sig ved disse undersøgelsesresultater:

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

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

Indholdsfortegnelse

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionens mandat til at gennemføre undersøgelsen følger af § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen vedrører finanslovens § 7. Finansministeriet.

I undersøgelsesperioden 2010 - maj 2023 har der været følgende ministre:

Claus Hjort Frederiksen: april 2009 - oktober 2011
Bjarne Corydon: oktober 2011 - juni 2015
Claus Hjort Frederiksen: juni 2015 - november 2016
Kristian Jensen: november 2016 - juni 2019
Nicolai Wammen: juni 2019 -

Beretningen har i udkast været forelagt Finansministeriet, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om it-sikkerheden på Statens It's servere.

2. Servere er en vigtig del af statens it-infrastruktur. Servere bruges til mange forskellige opgaver, bl.a. til at huse it-systemer, som kan indeholde følsomme personoplysninger og forretningskritiske data.

En server har en begrænset levetid. Levetiden er den periode, hvor leverandøren forpligter sig til at udvikle sikkerhedsopdateringer, i takt med at sårbarheder opdages. I løbet af serverens levetid udgiver leverandøren jævnligt sikkerhedsopdateringer, der forbedrer og sikrer serverens it-sikkerhed ved at inddæmme sikkerhedsbrister og beskytte mod nye trusler. Ved udløbet af serverens levetid vil serveren ikke længere kunne sikkerhedsopdateres. En server, der ikke længere kan sikkerhedsopdateres, udgør en sikkerhedsrisiko. Serveren skal derfor opgraderes til en nyere servertype for at kunne sikkerhedsopdateres igen. Det vil i nogle tilfælde være muligt at tilkøbe levetidsforlængelse i en begrænset periode.

3. Center for Cybersikkerhed under Forsvarets Efterretningstjeneste vurderer, at truslen i Danmark fra cyberkriminalitet og cyberspionage er meget høj, og at truslen fra cyberaktivisme er høj. Brud på it-sikkerheden kan i yderste konsekvens medføre, at en del af statens it-systemer og data bliver ødelagt eller gjort utilgængelige, samt at fortrolige og følsomme oplysninger om danske borgere og virksomheder bliver misbrugt eller ødelagt.

Center for Cybersikkerhed anbefaler derfor, at al software, herunder software til servere, opdateres, når nye sikkerhedsopdateringer frigives fra leverandøren. Det fremgår også af sikkerhedsstandarden ISO 27001, som alle statslige myndigheder skal efterleve, at det skal forhindres, at tekniske sårbarheder bliver udnyttet.

4. Statens It er en styrelse under Finansministeriet. Ved etableringen i 2010 blev drift og support af it for en række statslige myndigheder samlet i Statens It. Formålet var at levere bedre, billigere og mere sikker it-drift og service til den danske stat. Siden etableringen er der kommet flere myndigheder til, og Statens It har i dag ansvaret for it-driften og it-sikkerheden for 151 myndigheder på tværs af 21 ministerområder. I forbindelse med etableringen blev it-medarbejdere overført fra de enkelte myndigheder til Statens It.

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 denne beretning bruger vi begrebet server om servernes operativsystem, som er den grundlæggende software på en server.

Cyberaktivisme
Cyberaktivisme drives typisk af ideologiske eller politiske motiver. Cyberaktivister kan fokusere på enkeltsager, personer eller organisationer, som de opfatter som modstandere af deres sag.

Statens It
Statens It er udelukkende finansieret via indtægter fra de myndigheder, der er kunder hos Statens It. Ydelserne prissættes efter princippet om fuld omkostningsdækning. Myndighedernes betaling skal dække udgifter til drift, vedligeholdelse, udvikling, support og rådgivning. I finansloven for 2023 har Statens It indtægter og udgifter for 774 mio. kr. Statens It havde 506 årsværk i 2022.

5. Formålet med undersøgelsen er at vurdere, om 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. Vi besvarer følgende spørgsmål i beretningen:

- Har Statens It opgraderet eller nedlagt servere for de 46 myndigheder, der indgår i undersøgelsen, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer?
- Har Statens It gennemført kompenserende foranstaltninger for servere, der ikke længere kan sikkerhedsopdateres?
- Har Statens It etableret procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres?

Statens It's kunder
Statens It's kunder er myndigheder som departementer, styrelser og selvejende institutioner.

Rigsrevisionen har selv taget initiativ til undersøgelsen i marts 2023. Undersøgelsen er igangsat på baggrund af en it-revision, som Rigsrevisionen gennemførte i november 2022. It-revisionen omfattede 2 myndigheder, som har servere hos Statens It, og viste, at de 2 myndigheder havde flere servere hos Statens It, der ikke længere kunne sikkerhedsopdateres. Denne undersøgelse tager udgangspunkt i 46 myndigheder, herunder Statens It selv. Det er ca. en tredjedel af alle de myndigheder, der er kunder hos Statens It.

6. Beretningen er udarbejdet med henblik på offentliggørelse, og nogle resultater er derfor beskrevet på et overordnet niveau. Analysen indeholder detaljer om sårbarheder i it-sikkerheden hos Statens It. Da beskrivelsen af sårbarhederne ifølge Finansministeriet potentielt kan udgøre en risiko for statens sikkerhed, gengiver vi ikke disse detaljer i beretningen.

Hovedkonklusion

Statens It under Finansministeriet har ikke sikret, at alle Statens It's servere kan sikkerhedsopdateres. Det skyldes dels, at Statens It ikke har opgraderet eller nedlagt servere, der ikke længere kan sikkerhedsopdateres, dels at de har et ufuldstændigt overblik over myndighedernes servere. Dette finder Rigsrevisionen utilfredsstillende. Konsekvensen er, at der er risiko for, at hackere kan få adgang til følsomme personoplysninger og forretningskritiske data, og at disse oplysninger og data kan blive misbrugt eller ødelagt.

Statens It har ikke opgraderet eller nedlagt servere, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer

537 servere hos Statens It kan ikke længere sikkerhedsopdateres, da deres levetid er udløbet. Det er ca. 10 % af de i alt 5.353 undersøgte servere, som Statens It varetager driften af på vegne af de 46 myndigheder, inkl. Statens It selv. Statens It har ikke sikret, at serverne er blevet opgraderet eller nedlagt. Statens It har desuden et ufuldstændigt overblik over serverne, hvilket har forringet muligheden for at reagere hurtigt på cyberangreb og nye cybertrusler. Statens It har løbende siden undersøgelsens start arbejdet med dels at forbedre overblikket over serverne, dels at opgradere og nedlægge servere, der ikke længere kan sikkerhedsopdateres.

Statens It har ikke gennemført tilstrækkelige kompenserende foranstaltninger for de servere, der ikke længere kan sikkerhedsopdateres

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. Statens It har i forlængelse af undersøgelsen igangsat et initiativ, der skal begrænse muligheden for, at cyberangreb kan sprede sig mellem myndigheder.

Statens It har ikke procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres

Statens It har ansvaret for serverne og deres sikkerhed. Det følger af kongelige resolutioner. Myndighederne har dog i de fleste tilfælde ansvaret for driften af de fagsystemer, som ligger på serverne. Statens It har oplyst, at de ikke kan opgradere eller nedlægge serverne, fordi myndighederne ikke har opfyldt deres ansvar for at sikre, at myndighedernes fagsystemer er kompatible med nye servere. Hvis Statens It ikke kan opgradere eller nedlægge servere, uden at det får konsekvenser for myndighedernes brug af fagsystemerne, bør Statens It - som har det overordnede ansvar og kender de sikkerhedsmæssige risici - kontinuerligt rette henvendelse til myndighederne, indtil problemet er løst. Statens It har i 2018 og 2020 indgået aftaler med nogle af myndighederne om, hvad myndighederne skal gøre, før Statens It kan opgradere eller nedlægge serverne. Statens It har dog ikke etableret det fornødne samarbejde med myndighederne til, at serverne kan opgraderes eller nedlægges rettidigt. Statens It har oplyst, at de i 2023 vil tage et nyt paradigme i brug for aftaler med myndighederne, der gør det muligt at følge op på aftalerne. I den forbindelse vil Statens It iværksætte, at opfølgningen på aftalerne sker med en fast kadence.

For de servere, som er Statens It's egne og derfor ikke kræver aftaler med myndighederne, har Statens It heller ikke sikret en rettidig opgradering eller nedlæggelse. Statens It har oplyst, at de forventer at have opgraderet eller nedlagt egne servere, der ikke længere kan sikkerhedsopdateres, i 1. kvartal 2024.

Rigsrevisionen konstaterer, at det nuværende setup ikke er tilstrækkeligt til at løse problemet, og anbefaler derfor, at Finansministeriet tager stilling til, om der er den rigtige arbejds- og ansvarsfordeling mellem Statens It og myndighederne i forhold til serverne, så Statens It kan løfte deres ansvar for it-sikkerheden i statens it-infrastruktur.

1.2. Baggrund

7. Danmark er et af de mest digitaliserede lande i verden, og cybertrusler er derfor et grundvilkår for danske myndigheder. Cyberangreb foregår typisk ved, at hackere udnytter svagheder i it-sikkerheden til at skaffe sig uautoriseret adgang. Det kan foregå ved at udnytte menneskelige fejl, fx ved at snyde medarbejdere til at åbne links i mails og downloade ondsindet kode. Det er også i nogle tilfælde muligt at angribe computere og servere direkte. Når først sikkerheden er kompromitteret, er det muligt for hackere at åbne nye adgange til senere brug. Cyberangreb kan have til formål at ødelægge data og systemer, at spionere eller at tjene penge ved at sælge oplysninger og data. Det kan være svært at opdage, hvis sikkerheden er kompromitteret.

Boks 1 viser eksempler på cyberangreb i nyere tid.

Boks 1

Eksempler på cyberangreb i nyere tid

Cyberangreb på dansk kritisk infrastruktur
I maj 2023 blev 22 selskaber, som driver dele af den danske energiinfrastruktur, kompromitteret i et koordineret angreb. Angriberne udnyttede en kendt sårbarhed i en netværksenhed. Angrebene var mulige, fordi de enheder, der blev angrebet, ikke havde fået installeret de nyeste sikkerhedsopdateringer. Angriberne opnåede adgang til nogle af selskabernes kontrolsystemer, og flere selskaber måtte bl.a. frakoble sig internettet. På baggrund af angrebet anbefaler forsyningssektorens cybersikkerhedscenter bl.a., at processerne for sikkerhedsopdatering af enheder er på plads, og at det sikres, at der er overblik over alle enheder på netværket, så de bliver sikkerhedsopdateret.

Cyberangreb forårsagede nedbrud i togdrift
Et cyberangreb mod en underleverandør til DSB betød i oktober 2022, at mange af DSB's tog måtte holde stille i 4 timer.

Udnyttelse af sårbarhed hos Den Internationale Røde Kors Komité
Den Internationale Røde Kors Komité (ICRC) opdagede i januar 2022, at hackere i 70 dage havde udnyttet en sårbarhed i software, som endnu ikke var blevet sikkerhedsopdateret, til at skaffe sig uautoriseret adgang til følsomme personoplysninger om mere end 515.000 personer. Data kom fra Røde Kors' *Restoring Family Links*-program, som arbejder på at finde savnede personer og personer, der er blevet skilt fra familien, i forbindelse med væbnede konflikter og naturkatastrofer.

Angreb på 12 af 16 norske ministerier
I juli 2023 informerede den norske regering om et omfattende cyberangreb på "Departementenes sikkerhets- og serviceorganisasjon". Angrebet kompromitterede 12 ud af Norges i alt 16 ministerier. Hackerne udnyttede en sårbarhed i softwaren på både computere og servere, som kan udnyttes til at give adgang til brugeres personoplysninger og lave ændringer på serverne. Sårbarheden var endnu ikke blevet opdaget, og der var derfor ikke udviklet sikkerhedsopdateringer til at inddæmme den.

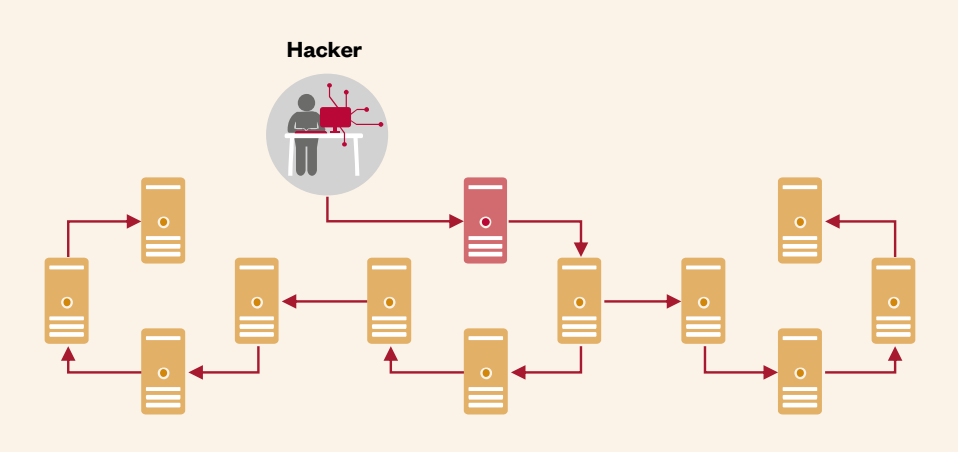
Note: Eksemplerne skyldes ikke nødvendigvis udnyttelse af sårbarheder i servere, der ikke kan sikkerhedsopdateres. Eksemplerne viser de problemer, der kan opstå, hvis en myndighed bliver ramt af et cyberangreb, og dermed vigtigheden af, at alle dele af offentlige myndigheders it-sikkerhed er god.

Kilde: Rigsrevisionen.

8. En sårbarhed på en server kan udgøre en risiko for både den pågældende server og for andre servere i det samme netværk. Hvis en hacker udnytter sårbarheden til at få uautoriseret adgang, kan det være muligt at få adgang til andre servere og it-systemer på tværs af netværket, også selv om disse servere er sikkerhedsopdaterede.

Figur 1 viser, hvordan et cyberangreb kan sprede sig mellem servere i et åbent netværk.

Figur 1
Spredning af et cyberangreb mellem servere i et fiktivt åbent netværk



Kilde: Rigsrevisionen.

9. Det er et kendt problem, at der er forældet it i den statslige it-portefølje, herunder også hos de myndigheder, der får varetaget deres basale it-drift hos Statens It. Rigsrevisionen har i beretningen om porteføljestyring af statens kritiske it-systemer gennemgået statslige myndigheders oplysninger til Statens It-råd. I Statens It-råds statusrapport for 2022 har 41 statslige myndigheder vurderet deres systemportefølje. 28 % af myndighedernes systemer har utilfredsstillende eller meget utilfredsstillende teknisk tilstand. 18 % af myndighederne har enten ikke implementeret alle relevante sikkerhedsopdateringer eller ved ikke, om de har det.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

10. Formålet med undersøgelsen er at vurdere, om 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.

11. I undersøgelsens første del undersøger vi, om Statens It har opgraderet eller nedlagt servere for de 46 myndigheder, der indgår i undersøgelsen, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer. Det gør vi ved at undersøge, om Statens It har servere, der ikke længere kan sikkerhedsopdateres.

12. I undersøgelsens anden del undersøger vi, om Statens It har gennemført kompenserende foranstaltninger for servere, der ikke længere kan sikkerhedsopdateres.

13. I undersøgelsens tredje del undersøger vi, om Statens It har etableret procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres. Det gør vi ved at undersøge, om Statens It har taget initiativ til i samarbejde med myndighederne at opgradere eller nedlægge de af myndighedernes servere, der ikke længere kan sikkerhedsopdateres. Vi undersøger også, om Statens It har taget initiativ til at opgradere eller nedlægge egne servere, der ikke længere kan sikkerhedsopdateres.

14. Vi baserer undersøgelsen på, at det er en grundlæggende del af en god it-sikkerhed at holde servere opdaterede. Vi lægger til grund, at det fremgår af den internationale sikkerhedsstandard ISO 27001, at myndigheder løbende skal iværksætte passende foranstaltninger for at håndtere risici ved tekniske sårbarheder. Vi lægger også til grund, at Center for Cybersikkerhed i "*Cyberforsvar der virker*" anbefaler, at al software, herunder servere, skal opdateres, når nye versioner eller sikkerhedsopdateringer frigives fra leverandøren.

"Cyberforsvar der virker"
Center for Cybersikkerheds grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb udkom første gang i 2013. Den seneste udgave udkom i juli 2023.

Metode

15. Undersøgelsens resultater er baseret på Rigsrevisionens egne analyser og it-revision og på gennemgang af materiale fra Statens It. For en nærmere beskrivelse af metoden henviser vi til bilag 1.

16. I undersøgelsen har vi inddraget cybersikkerhedsekspert Jacob Herbst. Jacob Herbst er teknisk chef (CTO) og partner i cybersikkerhedsfirmaet Dubex og er medlem af Cybersikkerhedsrådet. Jacob Herbst har bl.a. gennemgået beretningen og har rådgivet os om de mulige konsekvenser af resultaterne, herunder alvorsgraden af undersøgelsens resultater.

17. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

18. Undersøgelsen er afgrænset til de i alt 46 myndigheder, inkl. Statens It selv, som ved undersøgelsens start i marts 2023 ifølge Statens It brugte servere, der ikke længere kunne sikkerhedsopdateres.

19. Undersøgelsen omhandler servernes tilstand, i forhold til om de kan sikkerhedsopdateres, og Statens It's kompenserende foranstaltninger for servere, der ikke længere kan sikkerhedsopdateres. Vi har ikke undersøgt andre aspekter af servernes it-sikkerhed, fx fysisk sikkerhed eller logisk sikkerhed (fx adgangskoder).

20. Undersøgelsesperioden er fra 2010, hvor Statens It blev oprettet, og frem til maj 2023, hvor undersøgelsens datagrundlag er udtrukket.

21. Undersøgelsens resultater er baseret på udtræk fra Statens It's serverportefølje foretaget i maj 2023. Dataindsamlingen er afsluttet med dette udtræk. Statens It har efterfølgende haft mulighed for at komme med supplerende oplysninger.

2. Indsatsen over for servere, der ikke længere kan sikkerhedsopdateres

22. Dette kapitel handler om, hvorvidt Statens It under Finansministeriet, har sikret, at deres servere kan sikkerhedsopdateres, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering.

2.1. Servere, der ikke længere kan sikkerhedsopdateres

23. Vi har undersøgt, om Statens It har opgraderet eller nedlagt servere for de 46 myndigheder, der indgår i undersøgelsen, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer.

24. Undersøgelsen viser for det første, at 537 servere hos Statens It ikke længere kan sikkerhedsopdateres, da deres levetid er udløbet. Det er ca. 10 % af de i alt 5.353 undersøgte servere, som Statens It varetager driften af på vegne af de 46 myndigheder. Heraf er flere servere Statens It's egne, dvs. servere, som benyttes af Statens It til tværgående og intern it-drift, fx til fælles systemer, som tilgås af flere myndigheder.

Statens It har oplyst, at 98 af de 537 servere løbende er blevet opgraderet eller nedlagt siden undersøgelsens start. Dertil er 62 servere løbende påbegyndt opgraderet eller nedlagt i forbindelse med undersøgelsen. Statens It har endvidere oplyst, at der efter undersøgelsens start er kommet yderligere én myndighed til, som har servere, der ikke længere kan sikkerhedsopdateres.

For en større andel af de servere, der ikke længere kan sikkerhedsopdateres, har Statens It haft mulighed for at tilkøbe levetidsforlængelse for en begrænset periode. Det har de gjort for ca. halvdelen af disse servere.

25. Undersøgelsen viser for det andet, at Statens It ikke har et fuldstændigt overblik over serverporteføljen, hvilket man skal have ifølge ISO 27001. For 178 servere mangler Statens It viden om servernes type. Statens It har derfor i løbet af undersøgelsen løbende gennemgået serverne manuelt for at fremskaffe oplysninger.

Statens It's overblik er baseret på et digitalt værktøj, som trækker informationer fra alle servere, der har en agent installeret. En agent er et stykke software, som installeres på en server, hvor den opsamler og leverer information om serveren til en database. Undersøgelsen viser dog, at flere af Statens It's servere ikke har en agent installeret. Dette gælder bl.a. servere, der er så gamle, at agenten ikke kan installeres. Statens It har oplyst, at manglende agenter på serverne har skabt et ufuldstændigt overblik over serverne, og at de arbejder på at forbedre datakvaliteten.

Endelig har Statens It oplyst, at der – ud over de 46 myndigheder, der indgår i undersøgelsen – er yderligere 3 myndigheder, som har servere, hvor Statens It ikke har viden om behovet og muligheden for sikkerhedsopdateringer på serverne.

26. Konsekvenserne af det ufuldstændige overblik er, at Statens It har svært ved at vurdere behovet og muligheden for at holde serverne sikkerhedsopdaterede. Samtidig har Statens It dårligere forudsætninger for at reagere hurtigt på cyberangreb og nye cybertrusler og implementere nye tiltag for at imødekomme sårbarheder.

27. Rigsrevisionen bemærker, at servere, der ikke længere kan sikkerhedsopdateres, udgør en sikkerhedsrisiko, da de er udsat for sårbarheder, som er offentligt kendte, og som hackere kan udnytte. En sårbarhed udgør både en risiko for den pågældende server, men også for andre servere hos Statens It, da der er risiko for, at cyberangreb kan sprede sig til andre servere i samme netværk. Det er derfor vigtigt, at Statens It foretager kompenserende foranstaltninger for at reducere risikoen og konsekvenserne ved at have servere, der ikke længere kan sikkerhedsopdateres.

2.2. Kompenserende foranstaltninger

28. Vi har undersøgt, om Statens It har gennemført kompenserende foranstaltninger for de servere, der ikke længere kan sikkerhedsopdateres.

En kompenserende foranstaltning kan fx være at isolere serveren mest muligt på netværket, når den ikke længere kan sikkerhedsopdateres. Det vil mindske risikoen for, at et cyberangreb kan sprede sig til andre servere på tværs af netværket. Ifølge Statens It's egne interne procedurer er det et krav, at servere, der ikke længere kan sikkerhedsopdateres, isoleres mest muligt, så der ikke er adgang til andre servere. En anden kompenserende foranstaltning kan være at iværksætte tiltag, der generelt begrænser risikoen for succesfulde cyberangreb på de servere, der ikke længere kan sikkerhedsopdateres.

29. Undersøgelsen viser, at Statens It har en række foranstaltninger, som kan reducere risikoen for, at cyberangreb kan sprede sig. Foranstaltningerne består af en række netværks- og sikkerhedsværn, bl.a. firewalls og overvågning. Statens It har oplyst, at den generelle infrastruktur er designet, så risikoen for spredning på tværs og for kompromittering i almindelighed minimeres. Efter Rigsrevisionens vurdering er der 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. Statens It har i forlængelse af undersøgelsen igangsat et initiativ, der skal begrænse muligheden for, at cyberangreb kan sprede sig mellem myndigheder.

2.3. Procedurer for opgradering eller nedlæggelse af servere

30. Vi har undersøgt, om Statens It har etableret procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres. Statens It er ansvarlige for, at infrastrukturen er sikker, og at serverne er sikkerhedsopdaterede, uanset om der er tale om deres egne servere eller servere, som Statens It varetager driften af for andre myndigheder. Vi har undersøgt følgende:

- om Statens It har taget initiativ til i samarbejde med myndighederne at opgradere eller nedlægge de af myndighedernes servere, der ikke længere kan sikkerhedsopdateres
- om Statens It har taget initiativ til at opgradere eller nedlægge deres egne servere, der ikke længere kan sikkerhedsopdateres.

Initiativer til at opgradere eller nedlægge myndighedernes servere

31. Statens It er i nogle tilfælde afhængige af, at myndighederne udskifter eventuelle forældede fagsystemer, før de kan opgradere serverne. Selv om opgaven med at opgradere servere dermed ikke kan løses af Statens It alene, har Statens It initiativforpligtelsen i kraft af deres ansvar for serverne.

32. Når en myndighed bliver kunde hos Statens It, overgår ressortansvaret for it-driften af det overdragne område ved kongelig resolution til Finansministeriet. Ressortoverførslen betyder, at ansvaret påhviler Statens It, herunder ansvaret for it-sikkerhed og vedligeholdelse.

Boks 2 viser et eksempel på en kongelig resolution for overdragelse af en myndigheds it-drift.

Boks 2

Eksempel på ressortoverførsel ved kongelig resolution

§ 1. Ressortansvaret for alle opgaver, kontrakter og serviceaftaler vedrørende basal it-drift af interne datacentre, netværk, servere og storage, drift af operativsystemer, standard it-arbejdsplads, servicedesk og brugeradministration, informationssikkerhedsopgaver vedrørende foranstående samt kontrakter og leverandørstyringsopgaver vedrørende outsourcet it-drift, der vedrører Sundhedsministeriets departement, Sundhedsdatastyrelsen, Statens Serum Institut, Sundhedsstyrelsen, Styrelsen for Patientsikkerhed, Styrelsen for Patientklager, Fællessekretariatet for Det Etiske Råd og National Videnskabsetisk Komité samt Nationalt Genom Center, i henhold til nærmere aftale mellem sundhedsministeren og finansministeren overføres fra sundhedsministeren til finansministeren pr. 15. september 2021.

Note: Ressortoverførslerne kan have forskellig ordlyd.

Kilde: Bekendtgørelse nr. 1845 af 23. september 2021.

Som det fremgår af resolutionen, har Statens It overtaget ansvaret for it-driften, herunder for serverne. Det fremgår også, at der indgås nærmere aftaler mellem Statens It og myndighederne. I forlængelse af de kongelige resolutioner har Statens It derfor indgået kundeaftaler med myndighederne, hvori ansvarsfordelingen mellem Statens It og den enkelte myndighed aftales nærmere. Ansvar og opgaver fordeles i aftalerne pr. system ud fra forskellige driftsmodeller. Statens It har i alle driftsmodeller – i overensstemmelse med ressortoverdragelsen – ansvaret for at sikkerhedsopdatere serverne og for at have overblik over, hvornår serverne ikke længere kan sikkerhedsopdateres og derfor skal opgraderes. I de fleste driftsmodeller er det myndighederne, der har ansvaret for de fagsystemer, der benytter serverne. Det fremgår af Statens It's kundeaftaler, at ansvaret for sikkerhedsopdateringer vil overgå til myndigheden, hvis Statens It ikke kan sikkerhedsopdatere en server på grund af myndighedens forhold, fx hvis sikkerhedsopdateringer ikke er kompatible med myndighedens fagsystemer.

33. Statens It har oplyst, at forældede fagsystemer er den primære årsag til, at de ikke kan opgradere eller nedlægge servere, der ikke længere sikkerhedsopdateres. Hvis et fagsystem ikke er kompatibelt med en nyere servertype, kan serveren ikke opgraderes, uden at det hindrer driften af fagsystemet, medmindre fagsystemet også bliver opdateret og eventuelt opgraderet. Statens It har desuden oplyst, at det er en forholdsvis lille udgift for Statens It at opgradere eller nedlægge en server, der ikke længere kan sikkerhedsopdateres, men at det kan være en stor udgift for myndigheden at opgradere selve fagsystemet, så det er kompatibelt med en nyere server. Boks 3 viser et fiktivt eksempel på problemstillingen.

Boks 3

Fiktivt eksempel på afhængigheden mellem fagsystemer og servere

En myndighed har et fagsystem på en server hos Statens It. Myndigheden bruger fagsystemet til at løse vigtige opgaver, og serveren kan fx indeholde følsomme personoplysninger eller forretningskritiske data. Fagsystemet fungerer, men det er gammelt. Derfor virker fagsystemet også kun på en ældre servertype, fra da systemet blev udviklet. Det er en servertype, som ikke længere kan sikkerhedsopdateres, fordi dens levetid er udløbet, og serveren er derfor udsat for kendte sårbarheder. Statens It kan dog ikke opgradere serveren, da fagsystemet så ikke længere vil virke. Statens It er derfor afhængige af, at myndigheden opdaterer eller eventuelt udskifter fagsystemet, før Statens It kan løse deres opgave med at opgradere eller nedlægge serveren.

Kilde: Rigsrevisionen.

Hvis Statens It ikke kan opgradere eller nedlægge servere, uden at det får konsekvenser for myndighedernes brug af deres fagsystemer, bør Statens It kontinuerligt rette henvendelse til myndighederne, indtil problemet er løst. Statens It har været vidende om, at servere, der ikke længere kan sikkerhedsopdateres, udsætter den pågældende myndighed, Statens It og de øvrige myndigheder for en risiko. Statens It har desuden selv tilkendegivet, at de ikke lever op til deres vedligeholdelsesansvar, så længe, de har servere, der ikke kan sikkerhedsopdateres.

34. Statens It har i 2014, 2017 og 2022 skrevet til myndighederne om problemstillingen og risiciene forbundet med servere, der ikke længere kan sikkerhedsopdateres. Statens It har oplyst, at myndighederne også orienteres løbende gennem bilaterale kundemøder og via tværgående kundefora. Rigsrevisionen har gennemgået møderefferater for udvalgte myndigheder i 2022. Det fremgår af referater og dagsordener, at problemstillingen har været drøftet enkelte gange. Statens It har i 2017 udviklet en rapportløsning, hvor myndighederne selv kan tilgå informationer om deres servere, herunder om servertype og levetid. Rigsrevisionen bemærker, at rapportløsningen er baseret på Statens It's ufuldstændige overblik over servere. Rapporterne giver således i flere tilfælde ikke et fyldestgørende billede af myndighedernes servere og servernes levetid – særligt for de ældste servere.

35. Undersøgelsen viser, at Statens It har indgået aftaler med de fleste af myndighederne om opgradering eller nedlæggelse af servere, der ikke længere kan sikkerhedsopdateres. Undersøgelsen viser også, at det varierer, hvor konkrete aftalerne er. Hovedparten af aftalerne er indgået i 2018 og 2020, mens enkelte er indgået i 2021 og 2022. På undersøgelsestidspunktet havde Statens It indgået aftaler med 38 myndigheder, mens der manglede aftaler for 7 myndigheder. Efterfølgende har Statens It i løbet af 2023 indgået aftaler med 6 af de 7 myndigheder. Statens It har således indgået aftaler med 44 af de 45 myndigheder.

Vores gennemgang af aftalerne med myndighederne viser, at aftalerne ikke altid indeholder alle relevante oplysninger, fx navn på servere eller systemer samt tidsfrister for, hvornår serverne skal være opgraderet eller nedlagt. Det er dermed ikke klart, hvad Statens It har aftalt med myndighederne, ligesom aftalerne ikke giver et godt grundlag for opfølgning. Tabel 1 viser en opsummering af Statens It's aftaler med myndighederne.

Tabel 1

Opsummering af Statens It's aftaler med myndighederne

	Antal
Myndigheder i alt	**45**
heraf myndigheder, som Statens It ikke har indgået aftale med	1
heraf myndigheder, hvor de indgåede aftaler ikke navngiver servere eller systemer	13
heraf myndigheder, hvor de indgåede aftaler navngiver servere eller systemer	31

Kilde: Rigsrevisionen på baggrund af oplysninger fra Statens It.

Det fremgår af tabel 1, at Statens It har indgået aftaler med 44 af de 45 myndigheder. I 31 af de 44 aftaler med myndighederne er navngivne servere eller systemer, mens der i 13 aftaler ikke er navngivne servere eller systemer.

Vi har undersøgt resultaterne af de aftaler med myndighederne, som har navngivne servere, og som er indgået i perioden 2018-2022. Undersøgelsen viser, at der fortsat ikke er foretaget opgradering eller nedlæggelse af serverne for ca. en tredjedel af disse servere på trods af aftalerne mellem Statens It og myndighederne.

Statens It har oplyst, at de fra 4. kvartal 2023 vil tage et nyt paradigme i brug for aftaler om opgradering eller nedlæggelse af servere. I den forbindelse vil Statens It iværksætte, at opfølgningen på aftalerne sker med en fast kadence, og at aftalerne skal opdateres hvert år. Der er også fastsat krav til, hvilke oplysninger der skal indgå i aftalerne, bl.a. tidsfrister, servernavn og systemnavn.

36. Undersøgelsen viser desuden, at Statens It i december 2022 har igangsat et projekt med det formål at nedlægge servere, der ikke længere kan sikkerhedsopdateres. Projektet skal intensivere samarbejdet med myndighederne og sikre, at der afsættes de fornødne resurser hos myndigheden og Statens It, så nedlæggelsen af servere sker hurtigst muligt. Projektet er igangsat i forlængelse af Rigsrevisionens it-revision. Projektet omfatter alle kendte servertyper, der ikke længere kan sikkerhedsopdateres. Statens It forventede ifølge projektbeskrivelsen at have nedlagt alle myndighedernes servere i projektet ved udgangen af 1. kvartal 2024. Statens It har i september 2023 oplyst, at det ikke længere er forventningen at være i mål med alle servere med udgangen af 1. kvartal 2024. Rigsrevisionen bemærker hertil, at hvis Statens It ikke får opgraderet eller nedlagt serverne løbende, kan efterslæbet vokse sig større, i takt med at nyere servertypers levetid udløber.

Initiativer til at opgradere eller nedlægge Statens It's egne servere

37. Statens It har et betydeligt antal egne servere, som ikke længere kan sikkerhedsopdateres. Statens It er ikke afhængige af, at andre myndigheder opdaterer forældede fagsystemer, før disse servere kan opgraderes. Serverne bruges bl.a. 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.

38. Undersøgelsen viser, at Statens It ikke har sikret en rettidig opgradering eller nedlæggelse af egne servere, der ikke længere kan sikkerhedsopdateres. Statens It har i marts 2022 igangsat et internt projekt med det formål at opgradere Statens It's egne servere. Ved projektets begyndelse estimerede Statens It, at ca. 26 % af deres egne servere ikke kunne sikkerhedsopdateres. Det fremgår af Statens It's projektbeskrivelse, at projektet blev igangsat på baggrund af Center for Cybersikkerheds interesse for tilstanden af Statens It's egne servere. Det fremgår af projektbeskrivelsen, at Statens It vil skabe overblik over deres egne serveres levetid og udarbejde opgraderingsplaner, så de mest kritiske servere opgraderes eller nedlægges først. Projektet er endnu ikke afsluttet. Statens It har oplyst, at de forventer at have opgraderet eller nedlagt deres egne servere i 1. kvartal 2024.

Rigsrevisionen, den 23. november 2023

Birgitte Hansen

/Michala Krakauer

Bilag 1. Metodisk tilgang

Undersøgelsen bygger på en gennemgang af dokumenter og analyse af data.

Derudover har vi holdt møder med Statens It for at få indsigt i området. Finansministeriets departement har deltaget i møderne.

I undersøgelsen har vi inddraget cybersikkerhedsekspert Jacob Herbst. Jacob Herbst er teknisk chef (CTO) og partner i cybersikkerhedsfirmaet Dubex og er medlem af Cybersikkerhedsrådet. Jacob Herbst har bl.a. gennemgået beretningen og har rådgivet os om de mulige konsekvenser af resultaterne, herunder alvorsgraden af undersøgelsens resultater.

Nedenfor beskrives vores kvalitetssikring, data og metode i flere detaljer.

Kvalitetssikring

Denne undersøgelse er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos den reviderede samt ledelsesbehandling og sparring på forskellige tidspunkter i undersøgelsesforløbet med chefer og medarbejdere i Rigsrevisionen med relevante kompetencer.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- regler og vejledninger om it-sikkerhed for offentlige myndigheder
- korrespondance mellem Statens It og myndighederne
- referater af udvalgte møder mellem Statens It og myndighederne
- kundekontrakter mellem Statens It og myndighederne
- materiale fra Statens It's projekter vedrørende servere, der ikke længere kan sikkerhedsopdateres
- Statens It's interne vejledninger og retningslinjer
- systemporteføljerapporter
- databehandleraftaler.

Formålet med gennemgangen af dokumenterne har været at besvare undersøgelsens revisionskriterier.

Analyse af data

Undersøgelsens første del er baseret på en dataanalyse af udtræk fra Statens It's oversigter over servere. Udtrækkene er modtaget fra Statens It i maj 2023. Undervejs i undersøgelsen har Statens It fremsendt yderligere oplysninger om serverne.

Udtrækkene udgør et datasæt med én række for hver af Statens It's servere for de 46 myndigheder. Datasættet vedrører alle servere for de 46 myndigheder, der indgår i undersøgelsen. Vi har kun gennemgået data for de 46 myndigheder, som Statens It ved undersøgelsens start kunne konstatere brugte servere, der ikke længere kunne sikkerhedsopdateres.

For hver server har vi bl.a. modtaget informationer om følgende:

- **Servernavn.** Serverens navn.
- **Servertype.** Serverens operativsystem.
- **System.** Angivelse af, hvilket fagsystem der ligger på serveren.
- **Kunde.** Angivelse af, hvilken myndighed der betaler for Statens It's drift af serveren. Nogle servere er ejet af Statens It selv og bruges til at betjene flere myndigheder eller delte services.
- **Driftsmodel.** Angivelse af, hvilken af Statens It's driftsmodeller det pågældende fagsystem er underlagt.
- **Levetidsforlængelse.** Angivelse af, om der er tilkøbt levetidsforlængelse.

På baggrund af data har vi optalt antallet af servere med servertyper, der ikke længere kan sikkerhedsopdateres, og hvilke myndigheder serverne tilhører.

Analysen er kvalitetssikret hos Statens It, som har modtaget vores behandlede datasæt til kontrol.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision herunder standarderne for større undersøgelser (SOR 3). Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).