FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

November 2022
– 3/2022

Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger

Statens it-beredskab

3/2022

Beretning om

statens it-beredskab

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 2022

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.

Ministrene afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.

På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i april 2023.

Ministrenes redegørelser, 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 2022, som afgives i februar 2024.

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

Yderligere eksemplarer kan købes ved henvendelse til:
Stibo Complete lager og logistik
Vandtårnsvej 83A
2860 Søborg

Tlf.: 4322 7300
kundeservice@stibocomplete.com
www.stibocomplete.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-777-4
ISBN online 978-87-7434-778-1

Statsrevisorernes bemærkning

Beretning om statens it-beredskab

Statsrevisorerne har anmodet om denne undersøgelse af, om staten har et tilfredsstillende it-beredskab.

Undersøgelsen viser, at it-beredskabet for 13 udvalgte samfundskritiske systemer er så utilfredsstillende, at det har været nødvendigt for Rigsrevisionen at afgive en fortrolig beretning herom til Statsrevisorerne og i forlængelse heraf denne korte beretning.

Statsrevisorerne kritiserer, at de undersøgte myndigheder ikke har et tilfredsstillende it-beredskab, der kan sikre, at en række samfundskritiske opgaver uforstyrret og fortsat kan løses, selv om der skulle ske større it-nedbrud eller datatab.

Statsrevisorerne finder det særdeles nødvendigt, at de undersøgte myndigheder hurtigst muligt får rettet op på de mangler i it-beredskabet, som Rigsrevisionen har påpeget. Det gælder ikke mindst udarbejdelse af tilfredsstillende reetableringsplaner, der kan sikre, at myndighederne hurtigt kan vende tilbage til normal drift i tilfælde af større it-nedbrud, hackerangreb, fysiske skader e.l.

Statsrevisorerne forventer, at alle de statslige myndigheder på baggrund af denne beretning undersøger og sikrer et effektivt it-beredskab. Statsrevisorerne vil desuden følge op med yderligere beretninger om it-beredskabet for andre samfundskritiske it-systemer.

Selv om ministeriernes svarfrist er lovbestemt til mindst 2 måneder, finder Statsrevisorerne, at de ansvarlige ministre bør komme med deres redegørelse hurtigst muligt og helst inden 1 måned, da Rigsrevisionen har konstateret meget alvorlige sikkerhedsbrister i de 13 samfundskritiske systemer.

Statsrevisorerne

4. november 2022

Mette Abildgaard
Leif Lahn Jensen
Troels Lund Poulsen
Sophie Løhde
Mikkel Irminger Sarbo
Serdal Benli

Indholdsfortegnelse

Undersøgelsen er en statsrevisoranmodning, og Rigsrevisionen afgiver derfor beretningen til Statsrevisorerne i henhold til § 8, stk. 1, og § 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 har i udkast været forelagt de undersøgte ministerier.

1. Indledning

1. Statsrevisorerne anmodede i oktober 2021 Rigsrevisionen om at undersøge statens it-beredskab. Rigsrevisionen har afsluttet undersøgelsen og har afgivet resultaterne i en fortrolig beretning til Statsrevisorerne, idet beretningen indeholder vurderinger af sikkerhedsmæssige procedurer i relation til samfundskritiske offentlige it-systemer. Rigsrevisionen offentliggør i forlængelse heraf denne korte beretning om statens it-beredskab, der ikke indeholder fortrolige oplysninger.

2. Rigsrevisionen forventer, at den korte beretning kan bidrage til, at både de myndigheder, der har været involveret i beretningen, og andre myndigheder får et øget fokus på it-beredskab.

2. Baggrund og hovedkonklusioner

Større it-hændelser, hvor myndighederne har brug for et it-beredskab

Større it-hændelser kan være situationer, hvor et it-system bliver utilgængeligt, fx ved hackerangreb, fysiske skader på datacentre eller fejl på servere.

Større it-hændelser kan også indebære tab af data i et it-system. Datatab kan opstå ved, at data ikke kan genskabes ud fra en backup, fx efter et it-nedbrud eller hackerangreb. Datatab kan også opstå ved, at fejlbehæftede data kopieres til flere servere eller it-systemer.

Typer af it-beredskabsplaner

- **Reetableringsplan:** Plan for, hvordan et it-system rent teknisk skal reetableres i en beredskabssituation.
- **Krisestyringsplan:** Plan for myndighedernes interne krisestyring i en beredskabssituation med større it-nedbrud.

3. Offentlige myndigheder er afhængige af it-systemer for at kunne løse deres opgaver. Større it-nedbrud og tab af data i myndighedernes samfundskritiske it-systemer kan have store konsekvenser for både staten, borgere og virksomheder. Det er derfor afgørende, at myndighederne har et tilstrækkeligt it-beredskab på plads, inden der sker et større it-nedbrud eller datatab, så myndighederne kan minimere konsekvenserne af nedbruddet.

4. Formålet med Rigsrevisionens undersøgelse er at vurdere, om staten har et tilfredsstillende it-beredskab for udvalgte samfundskritiske it-systemer, så staten kan opretholde samfundskritiske funktioner i tilfælde af større it-hændelser. Derudover har vi undersøgt Digitaliseringsstyrelsens vejledningsindsats vedrørende it-beredskab. Undersøgelsesperioden er 2019-2021.

5. Staten har ifølge Digitaliseringsstyrelsen ca. 4.200 it-systemer. Rigsrevisionen har undersøgt 13 samfundskritiske it-systemer, som understøtter vigtige opgaver for samfundet.

Undersøgelsen fokuserer på myndighedernes kortlægning af samfundskritiske it-systemer og udarbejdelse af risikovurderinger samt på 2 overordnede typer af it-beredskabsplaner, som skal håndtere forskellige opgaver inden for it-beredskabet:

- *reetableringsplaner* for, hvordan it-systemet skal reetableres ved datatab eller nedbrud på systemet
- *krisestyringsplaner* for myndighedernes interne håndtering af større it-hændelser.

Undersøgelsens hovedkonklusioner

De undersøgte myndigheder har ikke sikret et tilfredsstillende it-beredskab for de 13 udvalgte samfundskritiske it-systemer. Særligt er it-beredskabet utilfredsstillende for én af de undersøgte myndigheder, hvor undersøgelsen har omfattet flere it-systemer. Konsekvensen af manglerne i it-beredskabet er, at der er risiko for, at it-nedbrud og datatab medfører, at staten ikke kan opretholde eller markant får forstyrret samfundskritiske opgaver.

Der er dog forskelle i it-beredskabet inden for de undersøgte myndigheder.

Konklusionen baseres på følgende:

Grundlaget for it-beredskabet

Myndighederne har kortlagt, hvilke samfundskritiske it-systemer de har. Myndighederne har dog ikke for alle de udvalgte it-systemer et overblik over, hvilke andre it-systemer der er afgørende for, at de udvalgte it-systemer kan fungere. Det er vigtigt, at myndighederne har et overblik over disse afhængigheder, da et nedbrud på støttesystemer, platforme mv. også kan betyde, at de samfundskritiske it-systemer ikke fungerer.

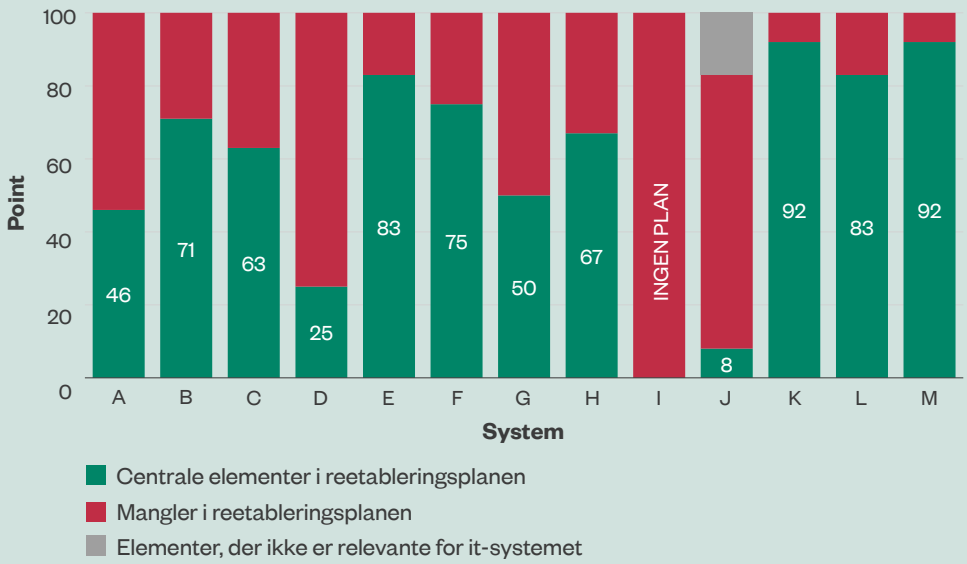
Myndighederne har udarbejdet risikovurderinger for 10 af de 13 udvalgte it-systemer. Det er vigtigt, at myndighederne risikovurderer de samfundskritiske it-systemer, så risikovurderingerne kan operationaliseres og anvendes til at håndtere de identificerede risici ved tilrettelæggelsen af it-beredskabet.

Reetableringsplaner for it-systemerne

Myndighederne har ikke sikret, at der er udarbejdet tilfredsstillende reetableringsplaner for de 13 udvalgte samfundskritiske it-systemer. Reetableringsplanerne skal sikre, at myndighederne hurtigst muligt kan vende tilbage til normal it-drift, hvis der sker et nedbrud på ét af it-systemerne. Det kræver, at myndighederne har reetableringsplaner, der indeholder en række centrale elementer, og at planerne er ajourført og testet.

Nogle af reetableringsplanerne har få mangler, mens størstedelen af planerne har flere mangler. For ét af de undersøgte it-systemer er der slet ingen reetableringsplan. Figur 1 viser Rigsrevisionens vurdering af reetableringsplanerne for de 13 udvalgte it-systemer.

Figur 1
Samlet vurdering af reetableringsplanerne for de 13 it-systemer



Kilde: Rigsrevisionen på baggrund af oplysninger fra de undersøgte myndigheder.

Ingen af reetableringsplanerne for de 13 udvalgte it-systemer er testet tilstrækkeligt, og 5 af systemerne er ikke blevet testet i perioden 2019-2021. Det betyder, at myndighederne for hovedparten af it-systemerne reelt ikke ved, om systemerne kan reetableres ved et totalt nedbrud, og hvor lang tid det vil tage at reetablere systemerne.

For de it-systemer, der driftes af eksterne leverandører, viser undersøgelsen, at myndighedernes leverandørstyring ikke er tilstrækkelig. Fx er der for under halvdelen af de eksternt driftede it-systemer stillet krav i kontrakten om, at leverandøren skal teste reetablering af it-systemet.

Krisestyringsplaner

De undersøgte myndigheders planer for den interne krisestyring er i overvejende grad tilfredsstillende. Myndighederne skal i deres krisestyringsplan bl.a. have klarlagt rolle- og ansvarsfordelingen, og hvordan myndigheden skal kommunikere i tilfælde af en større it-hændelse. Det er vigtigt, at disse forhold er på plads, før en større it-hændelse opstår, for at minimere eventuelle følgevirkninger af et større it-nedbrud eller datatab.

Størstedelen af myndighedernes krisestyringsplaner indeholder alle centrale elementer, som bør indgå i en krisestyringsplan. Dog er krisestyringsplanerne for enkelte af de undersøgte myndigheder ikke helt tilfredsstillende.

Alle myndigheder med undtagelse af én myndighed har testet deres krisestyringsplan i perioden 2019-2021. Det er vigtigt, at krisestyringsplanerne testes med jævne mellemrum for at sikre, at planerne er ajourført og understøtter en effektiv intern krisestyring.

Digitaliseringsstyrelsens vejledning om it-beredskabet
Digitaliseringsstyrelsen har på tilfredsstillende vis vejledt de statslige myndigheder i at implementere deres it-beredskab. Rigsrevisionen anbefaler dog, at Digitaliseringsstyrelsen fremadrettet systematisk undersøger myndighedernes behov for vejledning for bedre at kunne understøtte myndighederne i at implementere et tilfredsstillende it-beredskab.

3. Metode for Rigsrevisionens vurdering af it-beredskabet

Rigsrevisionens vurderinger af it-beredskabet er baseret på en række undersøgelsesspørgsmål, som kort præsenteres nedenfor.

Grundlaget for it-beredskabet

Vi har undersøgt følgende:

- Har myndighederne kortlagt, hvilke af deres it-systemer der er samfundskritiske?
  - Har myndighederne kortlagt, hvilke andre it-systemer, platforme mv. de samfundskritiske it-systemer er afhængige af for at kunne fungere?
- Har myndighederne udarbejdet risikovurderinger for de samfundskritiske it-systemer?
  - Har myndighederne nedskrevet en procedure for risikovurderingerne?
  - Indeholder risikovurderingerne en vurdering af trusler, sårbarheder, konsekvenser og sandsynligheder?
  - Er risikovurderingerne ajourført årligt?
- Har myndighederne taget stilling til, i hvilket omfang og hvordan myndighederne vil implementere ISO 27001-standardens kontrolmål for it-beredskabet?

Reetableringsplaner for de udvalgte samfundskritiske it-systemer

Vi har undersøgt følgende:

- Har myndighederne sikret, at der er udarbejdet reetableringsplaner for de samfundskritiske it-systemer?
  - Er reetableringsplanerne ajourført årligt?
  - Indeholder reetableringsplanerne 6 centrale elementer, som Rigsrevisionen vurderer, at en reetableringsplan som minimum bør indeholde?
    Se figur 2 på næste side.
- Har myndighederne sikret, at reetableringsplanerne er blevet testet?
  Vi har både set på, om der årligt er udført delvise tests (restore test), og om der jævnligt udføres fulde reetableringstests (disaster recovery test).
  - Har myndighederne sikret, at det er testet, om hele it-systemet kan reetableres på baggrund af den seneste backup på en tom server eller på ny hardware, fx i et testmiljø?
  - Indgår test af reetableringstiden (Recovery Time Objective) og test af it-systemets funktionalitet som en del af reetableringstesten?

- Har myndighederne sikret en tilfredsstillende leverandørstyring i forhold til reetableringsplaner?
  - Er der i kontrakterne med leverandørerne stillet krav til reetableringsplaner og til leverandørernes test af planerne?
  - Er der udarbejdet systemspecifikke revisorerklæringer?

Figur 2
Centrale elementer i en reetableringsplan

Kilde: Rigsrevisionen på baggrund af ISO 27001, Digitaliseringsstyrelsens vejledning om it-beredskab og Beredskabsstyrelsens vejledning om helhedsorienteret beredskabsplanlægning.

Myndighedernes krisestyringsplaner for de udvalgte samfundskritiske it-systemer

Vi har undersøgt følgende:

- Har myndighederne udarbejdet krisestyringsplaner for de udvalgte samfundskritiske it-systemer?
  - Er krisestyringsplanerne ajourført årligt?
  - Er krisestyringsplanerne fysisk tilgængelige?
  - Beskrives det, hvordan krisestyringsplanerne aktiveres?
  - Indeholder krisestyringsplanerne kontaktoplysninger på interne og eksterne nøglepersoner?
  - Indeholder krisestyringsplanerne en beskrivelse af rolle- og ansvarsfordelingen internt i myndigheden?
  - Beskriver krisestyringsplanerne, hvordan der kommunikeres til interne og eksterne aktører ved en større it-hændelse?
- Har myndighederne årligt testet krisestyringsplanerne?
  - Fremgår resultaterne af testen?
  - Beskriver testrapporten konkrete forbedringsforslag, og bliver der fulgt op på disse?