FOLKETINGET
RIGSREVISIONEN

April 2024

Rigsrevisionens notat om
beretning om

5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

Opfølgning i sagen om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden (beretning nr. 9/2021)

2. april 2024

RN 1404/24

I. Baggrund og konklusion

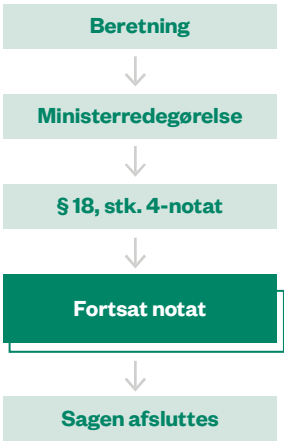
1. Rigsrevisionen følger i dette notat op på sagen om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden, som blev indledt med en beretning i 2022. Opfølgningen sker med henblik på at vurdere, om Statens It's (Finansministeriet), Kriminalforsorgens (Justitsministeriet), Energistyrelsens (Klima-, Energi- og Forsyningsministeriet), Fødevarestyrelsens (Ministeriet for Fødevarer, Landbrug og Fiskeri) og Sundhedsdatastyrelsens (Indenrigs- og Sundhedsministeriet) initiativer adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning. Rigsrevisionen følger i notatet også op på Finansministeriets (nu Digitaliserings- og Ligestillingsministeriet) arbejde med at vurdere, om enkelte af de 20 krav skal præciseres yderligere. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 22. april 2022.

2. Statslige myndigheder har siden 2020 skullet efterleve 20 tekniske minimumskrav for at sikre et højt niveau af cyber- og informationssikkerhed. Formålet med kravene er at beskytte statslige arbejdspladser mod cyberangreb og misbrug, fx uberettiget adgang til it-systemer samt hacker- og ransomwareangreb.

3. Da Statsrevisorerne behandlede beretningen, fandt de det utilfredsstillende, at hverken Statens It eller nogen af de 4 andre statslige myndigheder havde efterlevet alle de tekniske minimumskrav til it-sikkerheden i staten, på trods af at de var trådt i kraft 1-1½ år tidligere.

Statsrevisorerne konstaterede endvidere, at 4 minimumskrav var upræcise og havde givet anledning til fortolkning og tvivl om, hvordan myndighederne skulle efterleve kravene. Statsrevisorerne tilsluttede sig Rigsrevisionens anbefaling om, at Finansministeriet skulle konkretisere og uddybe de 4 minimumskrav.

Sagsforløb for en større undersøgelse



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

Konklusion

Rigsrevisionen finder det tilfredsstillende, at Statens It, Energistyrelsen og Fødevarestyrelsen nu efterlever alle de tekniske minimumskrav, der blev undersøgt i beretningen. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes for de 3 myndigheder.

Rigsrevisionens opfølgning viser, at Kriminalforsorgen fortsat ikke efterlever ét af kravene, og at Sundhedsdatastyrelsen ikke efterlever 6 af kravene.

Rigsrevisionens finder det ligeledes tilfredsstillende, at Digitaliserings- og Ligestillingsministeriet har vurderet, at enkelte krav skal præciseres, og at ministeriet i den forbindelse har udviklet nye, præciserede minimumskrav, som de statslige myndigheder skal efterleve pr. 1. juli 2024. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Kriminalforsorgens og Sundhedsdatastyrelsens efterlevelse af de tekniske minimumskrav.

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. De 5 myndigheders efterlevelse af de tekniske minimumskrav, der udestod, da Rigsrevisionen afgav beretningen til Statsrevisorerne.	Statens It, Energistyrelsen og Fødevarestyrelsen behandles og afsluttes i dette notat. Kriminalforsorgen og Sundhedsdatastyrelsen behandles i dette notat og følges fortsat.
2. Digitaliserings- og Ligestillingsministeriets arbejde med at vurdere, om enkelte krav skal præciseres yderligere.	Behandles og afsluttes i dette notat.

III. De 5 statslige myndigheders og Digitaliserings- og Ligestillingsministeriets initiativer

5. Vi gennemgår i det følgende Statens It's, Kriminalforsorgens, Energistyrelsens, Fødevarestyrelsens, Sundhedsdatastyrelsens og Digitaliserings- og Ligestillingsministeriets initiativer i forhold til de udestående opfølgningspunkter.

6. Opfølgningen er baseret på revisionsbesøg hos de 5 myndigheder, dokumentgennemgang samt redegørelser fra og møde med Digitaliserings- og Ligestillingsministeriet og Digitaliseringsstyrelsen.

7. Beretningen tog udgangspunkt i de 20 tekniske minimumskrav, som var gældende på undersøgelsestidspunktet. Digitaliseringsstyrelsen har efterfølgende præciseret minimumskravene i juni og november 2022. De præciserede krav skulle efterleves fra den 1. januar 2023. Vi har taget udgangspunkt i disse krav.

8. Statens It skal som myndighed selv efterleve minimumskravene til it-sikkerheden, men skal også som leverandør af it-services for en række statslige myndigheder sikre, at systemerne administreres i overensstemmelse med de tekniske minimumskrav.

På undersøgelsestidspunktet efterlevede Statens It alle minimumskravene for de systemer, som Statens It havde fået overdraget fra henholdsvis Energistyrelsen og Fødevarestyrelsen, som er kunder hos Statens It. I vores opfølgning er der derfor ikke fulgt op på de krav, som Statens It har ansvaret for på vegne af andre myndigheder. Vi har til gengæld fulgt op på de 2 krav, som Statens It ikke efterlevede i sin egen organisation på undersøgelsestidspunktet.

Det bemærkes, at sikkerhedsopdatering af servere, som blev behandlet i beretningen om it-sikkerheden på Statens It's servere fra december 2023, ikke er ét af de 20 tekniske minimumskrav.

Myndighedernes tiltag for at efterleve alle 20 minimumskrav

9. Statsrevisorerne fandt det utilfredsstillende, at ingen af de 5 statslige myndigheder havde efterlevet alle de tekniske minimumskrav til it-sikkerheden i staten.

10. Tabel 1 viser de 5 myndigheders efterlevelse af de 20 tekniske minimumskrav på undersøgelsestidspunktet (2021) og i forbindelse med vores opfølgning (2023-2024).

Tabel 1

Antal tekniske minimumskrav til it-sikkerheden, som de 5 statslige myndigheder efterlevede i 2021 og 2024

Myndighed	Status 2021	Status 2024
Statens It	18	20
Kriminalforsorgen	16	19
Energistyrelsen	15	20
Fødevarestyrelsen	17	20
Sundhedsdatastyrelsen	12	14

Note: Energistyrelsen manglede i 2021 at efterleve 4 krav, mens ét krav ikke var relevant.

Kilde: Rigsrevisionen.

Det fremgår af tabel 1, at Statens It, Energistyrelsen og Fødevarestyrelsen nu lever op til alle 20 minimumskrav.

Kriminalforsorgen er ikke helt i mål med at efterleve ét krav, mens Sundhedsdatastyrelsen mangler at efterleve 6 af de 20 minimumskrav.

De 5 statslige myndigheder

- Statens It (Finansministeriet)
- Kriminalforsorgen (Justitsministeriet)
- Energistyrelsen (Klima-, Energi- og Forsyningsministeriet)
- Fødevarestyrelsen (Ministeriet for Fødevarer, Landbrug og Fiskeri)
- Sundhedsdatastyrelsen (Indenrigs- og Sundhedsministeriet).

Kriminalforsorgen oplyser, at Kriminalforsorgen har igangsat et projekt med henblik på at sikre efterlevelsen af det sidste krav om sikkerhedsopdatering af applikationer. Kriminalforsorgen opfylder dele af kravet og arbejder målrettet med kravet.

Sundhedsdatastyrelsen har sikret efterlevelse af ét krav. Derudover er et af kravene blevet overdraget fra Sundhedsdatastyrelsen til Statens It.

Sundhedsdatastyrelsen oplyser, at styrelsen vil iværksætte en ny og styrket indsats for at leve op til de tekniske minimumskrav, som træder i kraft den 1. juli 2024.

Digitaliserings- og Ligestillingsministeriets arbejde med at præcisere enkelte minimumskrav

De 4 upræcise minimumskrav

- 6: Begrænset tildeling af lokaladministratorrettigheder
- 13: Regelmæssig opdatering af mobile enheder
- 14: Logning (krav 15 i beretningen)
- 20: Kryptering af kommunikation af hjemmesider (krav 18 i beretningen).

11. Statsrevisorerne konstaterede, at 4 minimumskrav var upræcise. Statsrevisorerne tilsluttede sig derfor Rigsrevisionens anbefaling om, at Finansministeriet (nu Digitaliserings- og Ligestillingsministeriet) skulle konkretisere og uddybe de 4 minimumskrav.

12. Vores opfølgning viser, at Digitaliserings- og Ligestillingsministeriet har arbejdet med at vurdere, om enkelte krav skulle præciseres yderligere. Ministeriet har sammen med Statens It, Politiets Efterretningstjeneste og Center for Cybersikkerhed evalueret de oprindelige 20 minimumskrav fra 2020. Ministeriet præciserede på baggrund heraf flere af kravene i 2022, herunder 3 af de 4 krav, som Statsrevisorerne fandt upræcise. Ministeriet oplyser, at det sidste upræcise krav (logning) er blevet præciseret i de nye minimumskrav, der skal efterleves pr. 1. juli 2024.

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

14. Bilag 1 viser Folketingets behandling af beretningen.

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
5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden (nr. 9/2021) 17-01-2022 **Minister-redegørelser:** Finansministeren: 11-03-2022 Sundheds-ministeren: 13-03-2022 Ministeren for fødevarer, landbrug og fiskeri: 16-03-2022 Klima-, energi- og forsynings-ministeren: 17-03-2022 Justitsministeren: 25-03-2022	Finansudvalget: 27-01-2022		Finansministeren: 28-04-2022 (285) 29-04-2022 (301)	Finansudvalget: 28-04-2022		