Statsrevisorerne 2021-22
Beretning Nr. 9 Rigsrevisionens notat af 22. april 2022
Offentligt

FOLKETINGET
RIGSREVISIONEN

Maj 2022

Rigsrevisionens notat om
beretning om

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

Vedrører:

Statsrevisorernes beretning nr. 9/2021 om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

22. april 2022

RN 1406/22

Finansministerens redegørelse af 11. marts 2022
Sundhedsministerens redegørelse af 13. marts 2022
Ministeren for fødevarer, landbrug og fiskeris redegørelse af 16. marts 2022
Klima-, energi- og forsyningsministerens redegørelse af 17. marts 2022
Justitsministerens redegørelse af 25. marts 2022

1. Rigsrevisionen vurderer i dette notat de initiativer, som ministrene har iværksat og vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner.

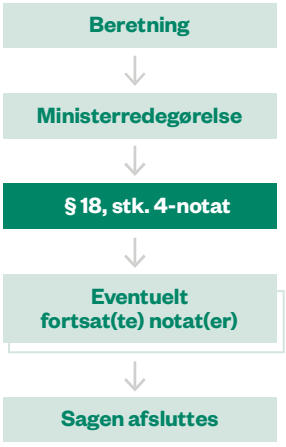
Konklusion

Ministrene tager generelt beretningen til efterretning og vil arbejde på at efterleve de tekniske minimumskrav, der udestod, da Rigsrevisionen afgav beretningen til Statsrevisorerne. Rigsrevisionen kan med tilfredshed konstatere, at der ifølge ministrenes redegørelser allerede er sket efterlevelse på flere områder.

Ministeren for fødevarer, landbrug og fiskeri oplyser, at Fødevarestyrelsen har sikret efterlevelse af de resterende 3 krav til it-sikkerheden. Finansministeren oplyser, at Statens It har sikret efterlevelse af de 2 krav, der udestod. Sundhedsministeren oplyser, at Sundhedsdatastyrelsen er i mål med efterlevelsen af 4 af de 8 krav, der manglede på revisionstidspunktet. På tilsvarende vis oplyser justitsministeren, at Kriminalforsorgen også er helt i mål med 2 af de 4 krav, som manglede efterlevelse, og at Kriminalforsorgen vil sikre efterlevelse af de resterende 2 krav i løbet af 2022. Klima-, energi- og forsyningsministeren oplyser, at Energistyrelsen allerede har sat tiltag i værk, og at arbejdet med opfyldelse af de resterende krav er i gang.

Finansministeren noterer sig endvidere Statsrevisorernes og Rigsrevisionens anbefaling om, at Finansministeriet konkretiserer og uddyber minimumskrav 6, 13, 15 og 18. Finansministeriet har derfor i regi af den nye nationale strategi for cyber- og informationssikkerhed igangsat et arbejde med at evaluere de eksisterende 20 minimumskrav, herunder vurdere, om enkelte krav skal præciseres yderligere. Finansministeriet vil samtidig se på muligheden for at udvide med nye krav for at styrke it-sikkerheden yderligere.

Sagsforløb for en større undersøgelse



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

Rigsrevisionen vil fortsat følge udviklingen og vil i 2023 orientere Statsrevisorerne om:

- de 5 myndigheders efterlevelse af de tekniske minimumskrav, der udestod, da Rigsrevisionen afgav beretningen til Statsrevisorerne
- Finansministeriets arbejde med at vurdere, om enkelte krav skal præciseres yderligere.

I. Baggrund

2. Rigsrevisionen afgav i januar 2022 en beretning om 5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden. Beretningen handlede om, hvorvidt Statens It (Finansministeriet), Kriminalforsorgen (Justitsministeriet), Sundhedsdatastyrelsen (Sundhedsministeriet), Energistyrelsen (Klima-, Energi- og Forsyningsministeriet) og Fødevarestyrelsen (Ministeriet for Fødevarer, Landbrug og Fiskeri) efterlever de 20 minimumskrav, da kravene har til formål at beskytte statslige arbejdspladser mod ondsindede cyber- og informationssikkerhedshændelser.

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 på daværende tidspunkt var trådt i kraft for 1-1½ år siden.

Statsrevisorerne konstaterede endvidere, at 4 minimumskrav er upræcise og har givet anledning til fortolkning og tvivl om, hvordan man efterlever kravene. Statsrevisorerne tilsluttede sig derfor Rigsrevisionens anbefaling om, at Finansministeriet konkretiserer og uddyber minimumskrav 6, 13, 15 og 18. Statsrevisorerne fandt desuden, at der er brug for, at Finansministeriet stiller sig i spidsen for vedvarende fokus på it-sikkerheden i staten.

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

II. Gennemgang af ministrenes redegørelser

Ministeriernes tiltag for at efterleve alle 20 minimumskrav

5. Statsrevisorerne fandt 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 på daværende tidspunkt var trådt i kraft for 1-1½ år siden.

Statsrevisorerne hæftede sig bl.a. ved, at Sundhedsdatastyrelsen havde efterlevet færrest minimumskrav (12 ud af 20 minimumskrav), mens Energistyrelsen havde efterlevet 15 krav, Kriminalforsorgen havde efterlevet 16 krav, og Fødevarestyrelsen havde efterlevet 17 krav. Statens It, som er en professionel aktør og leverandør af it-ydelser til 19 ministerområder, havde kun efterlevet 18 af de 20 minimumskrav.

6. Sundhedsministeren oplyser i sin redegørelse, at de sidste 2 års opgaver relateret til indsatsen mod COVID-19 har stillet hele ministerområdet, herunder også Sundhedsdatastyrelsen og ministeriets koncern-it-funktion, i en helt ekstraordinær situation. Alle resurser i koncernens it-funktion og i styrelserne har været sat ind for at sikre den nødvendige it-udvikling og it-understøttelse af COVID-19-indsatsen, og det har udfordret arbejdet med at sikre fuld målopfyldelse. Ministeren oplyser videre, at ministeren er helt enig med Statsrevisorerne og Rigsrevisionen i, at der netop er tale om minimumskrav, som offentlige myndigheder bør og skal leve op til. Ministeren oplyser i forlængelse heraf, at der på Sundhedsministeriets område arbejdes målrettet på at komme i mål med alle uopfyldte minimumskrav, og at ministeriet har gjort det løbende. På nuværende tidspunkt efterleves 16 af de 20 minimumskrav. Ministeren oplyser, at der er planer for, hvordan de sidste udestående opfyldes snarest muligt, og at Sundhedsdatastyrelsens vurdering er, at det sidste krav er opfyldt inden udgangen af 3. kvartal 2022.

Endelig oplyser sundhedsministeren, at arbejdet med it-sikkerheden og overholdelse af de 20 tekniske minimumskrav fremadrettet vil ske i et tæt samarbejde med Statens It, som helt eller delvist overtager ansvaret for målopfyldelse af kravene.

7. Ministeren for fødevarer, landbrug og fiskeri oplyser i sin redegørelse, at ministeren deler Statsrevisorernes og Rigsrevisionens opmærksomhed på it-sikkerheden og er enig i den fremsatte kritik. Ministeren oplyser, at Fødevarestyrelsen har fulgt op på kritikken i beretningen, og at styrelsen i sommeren 2021 har gennemført en transformation af hjemmesider hos Statens It og sikret, at kommunikation til hjemmesider fremadrettet er krypteret. Der er desuden foretaget udskiftning af alle forældede mobiltelefoner, sikret fremadrettet opdatering af mobile enheder og udarbejdet en plan for fremtidige opdateringer af servere. Ministeren oplyser, at Fødevarestyrelsen således har sikret efterlevelse af de udestående 3 krav til it-sikkerheden.

8. Klima-, energi- og forsyningsministeren oplyser i sin redegørelse, at ministeren sætter pris på beretningen og ser med alvor på, at de statslige myndigheder ikke fuldt ud efterlever de 20 tekniske minimumskrav til it-sikkerheden i staten. Ministeren oplyser videre, at Energistyrelsen fremadrettet vil sikre bedre styring og ledelsesforankring på området, og at styrelsen bl.a. har implementeret en styringsorganisation, der skal sikre en effektiv og ensartet forvaltning af domæneudvikling og idriftsættelse.

Klima-, energi- og forsyningsministeren oplyser i tilknytning hertil, at arbejdet er i gang, og de nye foranstaltninger skal sikre, at Energistyrelsen fremover efterlever alle de tekniske minimumskrav relateret til mail- og websikkerhed, som i beretningen er identificeret som værende ikke fuldt implementeret. Ministeren oplyser videre, at Energistyrelsen har skærpet proces og regelmæssig kontrol med bl.a. opdatering af mobile enheder. Ministeren nævner i den forbindelse konkrete tiltag som kvartalsvis dokumenteret gennemgang af opdatering af mobile enheder, ad hoc-procedure ved kritiske sikkerhedsopdateringer og øget awareness i organisationen via intranet m.m. Departementet vil ifølge ministeren følge Energistyrelsens arbejde gennem det departementale tilsyn. Ministeren påpeger i øvrigt vigtigheden af, at de tekniske minimumskrav bliver tydeligt defineret, og ministeren deler Rigsrevisionens og Statsrevisorernes syn på, at flere minimumskrav er upræcist beskrevet. Ministeren oplyser i forlængelse heraf, at der er behov for, at Finansministeriet konkretiserer og uddyber flere af minimumskravene.

9. Justitsministeren oplyser i sin redegørelse, at det er meget vigtigt, at myndighederne på Justitsministeriets område har iværksat foranstaltninger, der kan imødegå risici for cyberangreb og misbrug, og at kendte sikkerhedshuller og sårbarheder lukkes, så disse ikke kan udnyttes af ondsindede aktører. Ministeren oplyser i den forbindelse, at Justitsministeriet særskilt vil følge op på, at Kriminalforsorgen kommer i mål med implementeringen af de udestående krav. Ministeren oplyser desuden, at Kriminalforsorgen nu efterlever 2 af de 4 udestående krav, og at Kriminalforsorgen forventer at efterleve de resterende 2 krav i løbet af 2022.

10. Finansministeren oplyser i sin redegørelse, at ministeren er enig i beretningens konklusion og Statsrevisorernes bemærkning om, at det er utilfredsstillende, at ingen af de 5 undersøgte myndigheder har efterlevet alle 20 minimumskrav. Ministeren oplyser videre, at Statens It har et stort fokus på at sikre Statens It's egen og kundernes it-sikkerhed, og Finansministeriets fokus er dermed sammenfaldende med Rigsrevisionens formål med undersøgelsen.

Finansministeren oplyser i den forbindelse, at Statens It er enig med Rigsrevisionen i, at telefoners software skal opdateres rettidigt, og at Statens It derfor har implementeret en påmindelsesmail, der sendes til alle brugere, som ikke har opdateret til rette softwareversion. Rigsrevisionen forudsætter, at dette således også gælder opdatering af applikationer på de mobile enheder. Den nærmeste leder følger regelmæssigt op på denne awareness-mail, så det verificeres, at opdateringen finder sted. Ministeren oplyser, at med denne procedure vil Statens It leve op til kravet om regelmæssig opdatering af mobile enheder. Ministeren oplyser videre, at Statens It er enig med Rigsrevisionen i, at hjemmesider skal beskyttes med https. Fremadrettet vil Statens It derfor også lægge kryptering på tomme hjemmesider. Herved vil Statens It og kunderne også være sikret i tilfælde af utilstrækkelig koordinering.

11. Rigsrevisionen kan konstatere, at ministerierne har iværksat tiltag eller vil iværksætte tiltag, som skal sikre, at ministerierne efterlever de udestående minimumskrav. Statens It og Fødevarestyrelsen har oplyst, at de nu efterlever de krav, som udestod. Rigsrevisionen vil fortsat følge de 5 myndigheders efterlevelse af de tekniske minimumskrav, der udestod, da Rigsrevisionen afgav beretningen til Statsrevisorerne. Rigsrevisionen vil følge op herpå i 2023.

Finansministeriets tiltag for at konkretisere de upræcise minimumskrav

12. Statsrevisorerne fandt, at der er brug for, at Finansministeriet stiller sig i spidsen for vedvarende fokus på it-sikkerheden i staten. Statsrevisorerne tilsluttede sig endvidere Rigsrevisionens anbefaling om, at Finansministeriet konkretiserer og uddyber minimumskrav 6, 13, 15 og 18.

13. Finansministeren oplyser i sin redegørelse, at Finansministeriet løbende har fulgt op på myndighedernes implementering af minimumskravene, som også har vist, at mange myndigheder fortsat ikke er i mål med kravene. Derfor er det i regi af den nationale strategi for cyber- og informationssikkerhed besluttet, at myndighederne skal udarbejde handlingsplaner for de krav, som myndighederne ikke efterlever. Handlingsplanerne vil blive forelagt regeringen med henblik på at sikre en højere prioritering af arbejdet med minimumskravene i myndighederne.

Finansministeren oplyser desuden, at det er bevidst, at nogle af minimumskravene er formuleret med en vis fleksibilitet, da kravene skal passe til mange forskellige typer af myndigheder. De nuværende formuleringer giver nemlig en vis fleksibilitet i forhold til implementering af kravene. Ministeren oplyser videre, at ministeren har noteret sig Statsrevisorernes og Rigsrevisionens anbefaling, og nævner, at Finansministeriet i regi af den nye nationale strategi for cyber- og informationssikkerhed har igangsat et arbejde med at evaluere de eksisterende 20 minimumskrav, herunder vurdere, om enkelte krav skal præciseres yderligere. Der vil samtidig blive set på muligheden for at udvide med nye krav for at styrke it-sikkerheden yderligere.

Endelig oplyser finansministeren, at ministeren deler Statsrevisorernes holdning om, at Finansministeriet skal stille sig i spidsen for at sikre et vedvarende fokus på it-sikkerhed. Ifølge ministeren gør Finansministeriet det bl.a. ved løbende at følge op på myndighedernes implementering af ledelsestandarden ISO 27001 om informationssikkerhed og myndighedernes efterlevelse af de tekniske minimumskrav. I regi af den nye nationale strategi for cyber- og informationssikkerhed for perioden 2022-2024 vil ministeriet også afholde seminar for statslige topledere og gennemføre uddannelsesaktiviteter for både ledere og medarbejdere i staten. Sideløbende afvikles der også netværksaktiviteter for de statslige informationssikkerhedskoordinatorer, og der bliver løbende informeret til myndighederne om it-sikkerhed via hjemmesiden sikkerdigital.dk.

14. Rigsrevisionen finder det tilfredsstillende, at Finansministeriet i regi af den nye nationale strategi for cyber- og informationssikkerhed har igangsat et arbejde med at evaluere de eksisterende 20 minimumskrav. Rigsrevisionen vil fortsat følge ministeriets arbejde med at vurdere, om enkelte krav skal præciseres yderligere.

Lone Strøm