FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Januar 2026
– 8/2025

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

Statens It's beskyttelse af lokalt netværksudstyr hos statslige myndigheder

8/2025

Beretning om

Statens It's beskyttelse af lokalt netværksudstyr hos statslige myndigheder

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 2026

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 april 2026.

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 2025, som afgives i februar 2027.

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 978-87-7434-882-5

Statsrevisorernes bemærkning

Beretning om Statens It's beskyttelse af lokalt netværksudstyr hos statslige myndigheder

Statens It under Finansministeriet har ansvaret for it-driften hos statslige myndigheder fordelt på 23 ministerier og mere end 800 lokationer. Statens It har bl.a. ansvaret for sikkerheden på de statslige myndigheders lokale netværksudstyr.

Hvis en hacker får adgang til en myndigheds lokale netværk, er der risiko for, at driften på netværket kan forstyrres, og at hackeren kan bruge adgangen som springbræt til Statens It's centrale netværk, som indeholder en række fortrolige informationer om staten, virksomheder og borgere. Sandsynligheden for succesfulde angreb på myndighedernes lokale netværk er lav, men konsekvensen kan være stor. Styrelsen for Samfundssikkerhed vurderer, at truslen fra cyberspionage er meget høj, og anbefaler, at netværksudstyr løbende sikkerhedsopdateres.

Formålet med undersøgelsen er at vurdere, om Statens It har sikret en tilfredsstillende beskyttelse af netværksudstyret hos de statslige myndigheder.

Statsrevisorerne finder Statens It's beskyttelse af netværksudstyret hos de statslige myndigheder ikke helt tilfredsstillende, idet der mangler implementering af sikkerhedsopdateringer og en tilstrækkelig risikovurdering af sårbarhederne på udstyret. Samtidig har Statens It ikke et fuldstændigt overblik over netværksudstyret hos de statslige myndigheder, som Statens It skal beskytte.

Statsrevisorerne

19. januar 2026

Mette Abildgaard
Leif Lahn Jensen
Serdal Benli
Mikkel Irminger Sarbo
Lars Christian Lilleholt
Mohammad Rona

Statsrevisorerne har hæftet sig ved disse undersøgelsesresultater:

- Statens It har ikke implementeret de sikkerhedsopdateringer, som producenterne frigiver. Det gælder også sikkerhedsopdateringer, der skal fjerne sårbarheder, som producenterne af udstyret betegner som kritiske. Stort set alt udstyret har ifølge producenterne kritiske sårbarheder. Statens It har i stedet igangsat et program, der skal modernisere de lokale netværk. Programmet vil være implementeret i 2032.
- Statens It har foretaget en overordnet risikovurdering af de kritiske sårbarheder på myndighedernes netværksudstyr, men forholder sig ikke løbende til de enkelte kritiske sårbarheder ved netværksudstyret. Statens It vurderer, at sandsynligheden for, at sårbarhederne på de lokale netværk kan udnyttes, er lav.
- Statens It har ikke et fuldstændigt overblik over netværksudstyr hos de statslige myndigheder, som Statens It skal beskytte. Der kan dermed være udstyr med kritiske sårbarheder, som Statens It ikke kender til.
- Statens It har implementeret en teknisk adgangskontrol, der skal sikre, at kun godkendte enheder kan få adgang til myndighedernes kablede netværk. Dog har Statens It ikke inden for undersøgelsesperioden kunnet dokumentere et fuldt overblik over, at denne adgangskontrol var tilstrækkeligt implementeret.

Statsrevisorerne er enige i Rigsrevisionens anbefaling om, at Statens It bør forholde sig konkret til de enkelte sårbarheder, i takt med at de udmeldes. Statsrevisorerne anbefaler også, at Statens It skaber et tilstrækkeligt fuldstændigt overblik over det netværksudstyr, som de har ansvaret for at beskytte.

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 rigsrevisorlovens § 2, stk. 1, nr. 1.

Beretningen vedrører finanslovens § 7. Finansministeriet.

I undersøgelsesperioden februar-august 2025 har der været følgende ministre:

Nicolai Wammen: juni 2019 -

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

1. Indledning

1.1. Formål og konklusion

1. Denne beretning handler om beskyttelse af netværksudstyret på de statslige myndigheders lokale netværk.

2. Et netværk kan kun fungere ved hjælp af *netværksudstyr*, der består af forskellige tekniske enheder. Det kan være wi-fi-enheder eller enheder, der via et kabel og et stik i væggen giver adgang til netværket.

3. De statslige myndigheders lokale netværk er de netværk, som medarbejderne kobler deres arbejdscomputere til. Netværkene er nødvendige for, at medarbejderne kan dele dokumenter og data med hinanden, sende e-mails, holde videomøder mv. Myndighedernes netværk kommunikerer med Statens It's centrale netværk.

Statens It's centrale netværk
Statens servere og data findes på Statens It's centrale netværk. Her ligger myndighedernes fagsystemer og gemte filer. Det centrale netværk er beskyttet af flere lag, end de statslige myndigheders lokale netværk er.

Rigsrevisionen har tidligere undersøgt dele af Statens It's centrale netværk i beretning nr. 6/2023 om it-sikkerheden på Statens It's servere. Statens data opbevares i Statens It's centrale netværk, og det er derfor mere risikofyldt, hvis uvedkommende får direkte adgang til Statens It's servere end adgang til myndighedernes lokale netværk.

I denne beretning undersøger vi de lokale netværk i form af netværksudstyr rundt omkring hos ministerierne.

4. Rigsrevisionen har i to tidligere it-revisioner i 2019 og 2023 bl.a. undersøgt og vurderet, at Statens It ikke havde implementeret hensigtsmæssige procedurer for sikkerhedsopdatering og vedligeholdelse af netværksudstyr. Denne undersøgelse handler om de samme typer af netværksudstyr, som indgik i de to it-revisioner.

Netværksudstyret hos de statslige myndigheder er ifølge Statens It placeret, hvor uvedkommende ikke har fysisk adgang, fx på gangarealer, i kontorer og i aflåste skabe eller rum. Det betyder, at sårbarheder kun kan udnyttes via ureglementeret fysisk adgang, som i de fleste tilfælde også vil kræve omgåelse af alarmer og vagter. Rigsrevisionen bemærker dog, at myndighederne også omfatter fx uddannelsesinstitutioner, hvor der er relativt fri adgang for offentligheden. Herudover vil udnyttelse af sårbarheder kræve omgåelse af Statens It's øvrige sikkerhedsforanstaltninger, fx firewalls. Derfor er der ifølge Statens It en lav sandsynlighed for, at sårbarhederne på de lokale netværk kan udnyttes.

Hvis det lykkes en hacker at få adgang til en myndigheds lokale netværk, er der risiko for, at hackeren kan forstyrre driften på netværket og dermed gøre det sværere for myndigheden at løse deres opgaver. Herudover kan der være risiko for, at hackeren kan opsnappe den kommunikation, der foregår på netværket, og fx se de dokumenter, som medarbejderne sender til printerne.

Der kan også være risiko for, at hackeren kan bruge adgangen som et springbræt til at få adgang til Statens It's centrale netværk og dermed bl.a. til fortrolig information om staten, virksomheder og borgere. Dette vil dog kræve, at hackeren også kan omgå en række af Statens It's øvrige sikkerhedsforanstaltninger. Derfor vurderer Statens It, at risikoen er lav.

5. Boks 1 viser et eksempel, hvor en hackergruppe har udnyttet sårbarheder på netværksudstyr.

Boks 1

Eksempel på angreb gennem sårbarheder på netværksudstyr

En formodet russisk, statsstøttet hackergruppe har specialiseret sig i at bryde ind i netværksudstyr. De går især efter gammelt og dårligt opdateret udstyr med kendte sårbarheder. Når de først har fået adgang, arbejder de sig gradvist videre ind i organisationens systemer ved at overtage mere udstyr. Undervejs kan de ændre opsætninger på udstyr og opsnappe datatrafik. Ved at ændre i selve softwaren i udstyret kan de have skjult adgang og spionere i årevis uden at blive opdaget. Angrebene har bl.a. været rettet mod myndigheder, teleselskaber og uddannelsesinstitutioner i Nordamerika og Europa, herunder også kritisk infrastruktur i Ukraine.

Kilde: Rigsrevisionen på baggrund af Cisco Talos (https://blog.talosintelligence.com/static-tundra/).

Der er kun få kendte eksempler på den type angreb, som er angivet i boks 1, og Rigsrevisionen er ikke bekendt med eksempler i Danmark.

Rigsrevisionen har i forbindelse med denne undersøgelse fået rådgivning fra en ekstern ekspert, som vurderer, at sandsynligheden for denne type angreb er lav, men at konsekvensen kan være stor. Statens It vurderer, at både sandsynligheden for succesfulde angreb på myndighedernes lokale netværk er lav, og at konsekvensen vil være lille, fordi angrebet vil blive opdaget af Statens It's øvrige foranstaltninger.

Selv om truslen i flere år har været alvorlig, ændrer den løbende karakter, ligesom hackerne hele tiden tager nye værktøjer og metoder i brug. Styrelsen for Samfundssikkerhed vurderer, at truslen fra cyberspionage er meget høj.

Styrelsen for Samfundssikkerhed anbefaler, at netværksudstyr løbende sikkerhedsopdateres. Beskyttelsen kan herudover fx ske ved en teknisk adgangskontrol, der betyder, at kun godkendte enheder, fx computere leveret af Statens It, kan få adgang til netværkene. Herudover er der andre lag, der beskytter oplysningerne på netværkene, fx kryptering af data.

6. Finansministeriet har ansvaret for it-driften hos statslige myndigheder fordelt på 23 ministerier og mere end 800 lokationer i både Danmark og udlandet. It-driften varetages af Statens It, der er en styrelse under Finansministeriet. Statens It har dermed også ansvaret for sikkerheden på de statslige myndigheders lokale netværksudstyr. Det er myndighederne, der har ansvaret for den fysiske adgangskontrol til lokationen.

Statslige myndigheder, som ikke indgår i undersøgelsen

Statens It varetog på undersøgelsestidspunktet ikke it-driften for Skatteministeriet og Forsvarsministeriet. Herudover er der enkelte myndigheder under de øvrige ministerier, hvor Statens It heller ikke har ansvaret for it-driften, bl.a. politiet.

7. Statens It køber netværksudstyr hos private producenter. Producenterne finder løbende ud af, at udstyret har sårbarheder, der kan gøre netværket usikkert. Når producenterne har fundet sårbarheder, frigiver de opdateringer, der kan fjerne sårbarhederne. Det er implementeringen af disse opdateringer, som Styrelsen for Samfundssikkerhed anbefaler.

8. Formålet med undersøgelsen er at vurdere, om Statens It har sikret en tilfredsstillende beskyttelse af netværksudstyret hos de statslige myndigheder. Vi besvarer følgende spørgsmål i beretningen:

- Har Statens It løbende implementeret de sikkerhedsopdateringer, som producenten frigiver?
- Har Statens It foretaget en tilstrækkelig risikovurdering af myndighedernes netværksudstyr?

Rigsrevisionen har selv taget initiativ til undersøgelsen i juni 2025.

9. Beretningen er udarbejdet med henblik på offentliggørelse. Efter aftale med Finansministeriet har vi af hensyn til statens sikkerhed ikke oplistet eller givet eksempler på sårbarheder hos navngivne myndigheder.

Konklusion

Statens It har ikke sikret en helt tilfredsstillende beskyttelse af netværksudstyret hos de statslige myndigheder. Det skyldes, at Statens It ikke har foretaget en tilstrækkelig risikovurdering af sårbarhederne på netværksudstyret og samtidig ikke har et fuldstændigt overblik over alt det udstyr, som de skal beskytte.

Statens It har ikke løbende implementeret de sikkerhedsopdateringer, som producenten frigiver, men Statens It har oplyst, at de i stedet har igangsat et program, der skal modernisere de lokale netværk.

Statens It har foretaget en overordnet risikovurdering, hvori de vurderer, at risikoen ved kritiske sårbarheder på myndighedernes netværksudstyr er lav. Risikovurderingen forholder sig dog ikke løbende til de enkelte kritiske sårbarheder ved netværksudstyret, i takt med at producenten har udmeldt dem, herunder hvilke risici sårbarhederne udgør for myndighedernes lokale netværk. Statens It har desuden ikke et fuldstændigt overblik over netværksudstyret hos de statslige myndigheder og dermed, hvad Statens It skal beskytte. Det betyder, at der kan være netværksudstyr med sårbarheder, som Statens It ikke kender til.

Statens It har herudover implementeret en teknisk adgangskontrol, der har til formål at sikre, at kun godkendte enheder, fx computere leveret af Statens It, kan få adgang til en myndigheds kablede netværk. Statens It havde på undersøgelsestidspunktet ikke fuldt overblik over, om adgangskontrollen i tilstrækkelig grad var implementeret på det relevante netværksudstyr. Rigsrevisionen har primo januar 2026 modtaget materiale, der ifølge Statens It dokumenterer, at adgangskontrollen i høj grad er implementeret. Rigsrevisionen har på grund af det sene tidspunkt ikke haft mulighed for at vurdere dokumentationen.

Rigsrevisionen anbefaler, at Statens It forholder sig konkret til de enkelte sårbarheder, i takt med at de udmeldes. Statens It bør desuden få skabt et fuldstændigt overblik over det netværksudstyr, som de har ansvaret for at beskytte.

1.2. Vurderingskriterier, metode og afgrænsning

Vurderingskriterier

10. Vores undersøgelse udspringer af to tidligere revisioner af it-sikkerhed, som er gennemført i 2019 og 2023. Vores vurdering af, om Statens It har sikkerhedsopdateret netværksudstyret, og om de har foretaget en tilstrækkelig risikovurdering, er baseret på de internationale standarder for informationssikkerhed ISO 27001 og ISO 27002. Det har siden 2016 været obligatorisk for statslige myndigheder at følge ISO 27001. ISO 27002 er en vejledning hertil. Herudover fremgår det af en vejledning fra Styrelsen for Samfundssikkerhed, at netværksudstyr bør opdateres, når producenterne frigiver opdateringer.

Metode

11. Undersøgelsen er baseret på en gennemgang af dokumenter og på analyser af data fra Statens It. Undersøgelsens metode er uddybet i bilag 1.

12. Cybersikkerhedsekspert Jacob Herbst, som er teknisk chef i cybersikkerhedsfirmaet Dubex og forperson for Cybersikkerhedsrådet, har rådgivet os om de mulige konsekvenser af undersøgelsens resultater, herunder alvorsgraden heraf. Indholdet i beretningen, herunder resultater og vurderinger, er alene Rigsrevisionens ansvar.

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

Afgrænsning

14. Vi har undersøgt de tre væsentligste typer af lokalt netværksudstyr, som fremgår af bilag 1. Det drejer sig om i alt ca. 11.600 stykker lokalt netværksudstyr fra den producent, der er hovedleverandør til Statens It.

Undersøgelsen omfatter netværksudstyr hos statslige myndigheder i de 23 ministerier, hvor Statens It pr. 21. august 2025 havde ansvaret for it-driften.

Undersøgelsen omfatter både det trådløse og det kablede netværk. Når vi undersøger Statens It's tekniske adgangskontrol, er undersøgelsen dog afgrænset til det kablede netværk. Det skyldes, at det er Rigsrevisionens erfaring fra andre it-revisioner, at netværksudstyret på det kablede netværk oftest er af ældre dato og dermed har de største svagheder.

Undersøgelsen af Statens It vedrører statslige myndigheder i Danmark, Grønland og på Færøerne samt danske repræsentationer i udlandet.

15. Undersøgelsen sætter fokus på de statslige myndigheders lokale netværksudstyr, som Statens It har ansvaret for. Vi har ikke undersøgt sikkerheden på Statens It's centrale netværk. Rigsrevisionen har i forbindelse med beretning nr. 6/2023 om it-sikkerheden på Statens It's servere undersøgt dele af Statens It's centrale netværk.

2. Beskyttelse af netværksudstyret

16. Dette kapitel handler om:

- Statens It's sikkerhedsopdateringer af netværksudstyret (afsnit 2.1)
- Statens It's risikovurdering af sårbarheder ved netværksudstyret (afsnit 2.2).

2.1. Sikkerhedsopdateringer af netværksudstyret

17. Det er Statens It's opgave at beskytte de statslige myndigheders netværk, så uvedkommende ikke kan få adgang.

Det fremgår af de internationale ISO-standarder for informationssikkerhed, at netværk og netværksudstyr skal være sikret for at beskytte informationer. Det fremgår også af Styrelsen for Samfundssikkerheds vejledning *Cyberforsvar der virker*, at netværksudstyr bør opdateres, når producenterne frigiver opdateringer.

Det fremgår af vejledningen, at de rette tekniske tiltag kan reducere risikoen for at blive ramt af et cyberangreb markant. Styrelsen for Samfundssikkerhed anbefaler derfor, at myndigheder og virksomheder prioriterer implementering af tekniske tiltag højt. Styrelsen har udarbejdet en liste med ti områder, som alle bør implementeres som en del af et cyberforsvar, der virker. Ét af de tekniske tiltag er at foretage sikkerhedsopdateringer.

Producenter af netværksudstyr offentliggør løbende nye sårbarheder ved udstyret og frigiver opdateringer, der kan fjerne sårbarhederne. Producenterne kategoriserer nogle af sårbarhederne som kritiske. Det kan være, fordi sårbarhederne er forholdsvis lette at udnytte, eller fordi udnyttelsen af sårbarhederne kan have alvorlige konsekvenser. Kritiske sårbarheder skal derfor ifølge producenterne håndteres hurtigt. Producenterne tager dog ikke højde for, i hvilket omfang kunderne har kompenserende foranstaltninger, der mindsker sårbarhederne.

18. Vi har undersøgt, om Statens It løbende har implementeret de sikkerhedsopdateringer, som producenten frigiver.

Rigsrevisionen har to gange tidligere haft bemærkninger til Statens It's beskyttelse af netværksudstyr. Ved en it-revision i 2019 fandt vi bl.a. eksempler på udstyr, der ikke var blevet opdateret i 10 år. I 2023 konkluderede vi, at Statens It ikke havde implementeret hensigtsmæssige procedurer for sikkerhedsopdatering og vedligeholdelse af netværksudstyr.

På baggrund af en risikovurdering har Statens It ikke implementeret de sikkerhedsopdateringer af netværksudstyr, som producenten frigiver.

Statens It har i forbindelse med denne undersøgelse oplyst, at de har prioriteret at igangsætte et moderniseringsprogram af myndighedernes lokale netværk i stedet for at opdatere myndighedernes netværksudstyr.

Moderniseringsprogrammet er påbegyndt i 2025 og forventes at tage 7 år at gennemføre. Statens It har oplyst, at programmet har til formål at modernisere netværket gennem en udstrakt grad af standardisering, harmonisering og automatisering. Dette skal bl.a. medvirke til at beskytte de lokale netværk.

Rigsrevisionens eksterne ekspert har oplyst, at det kan være sikkerhedsmæssigt forsvarligt ikke straks at sikkerhedsopdatere netværksudstyr. Det forudsætter ifølge eksperten en ordentlig risikovurdering, en løbende opfølgning og passende kompenserende kontroller. Netværksudstyret bør dog opdateres inden for rimelig tid, og det er som udgangspunkt bedste praksis og generelt anbefalet at opdatere udstyret hurtigst muligt efter, at producenterne har frigivet sikkerhedsopdateringerne. Derved får man adresseret kendte sårbarheder og løst kendte fejl, der kan forstyrre driften på netværket.

Vores gennemgang af i alt 11.616 stykker netværksudstyr viser, at stort set alt udstyret ifølge producenten har kritiske sårbarheder. De kritiske sårbarheder findes i netværksudstyret hos alle 23 ministerier.

Gennemgangen viser også, at det er muligt for Statens It at sikkerhedsopdatere 91 % af netværksudstyret, fordi producenten fortsat frigiver nye opdateringer. For de sidste 9 % af udstyret frigiver producenten ikke længere opdateringer. Det betyder, at Statens It kun kan fjerne de kritiske sårbarheder ved at udskifte udstyret. For størstedelen af netværksudstyret er det altså muligt for Statens It at fjerne sårbarhederne ved at opdatere udstyret. I nogle tilfælde vil det dog kræve, at Statens It betaler producenten for at forlænge licensen for netværksudstyret.

19. Statens It har oplyst, at de ikke forlænger de 3-årige licenser, som myndighedernes netværksudstyr leveres med som standard, da de har accepteret de risici, som manglende opdatering af netværksudstyr indebærer. Det skyldes, at Statens It vurderer, at risikoen for angreb er lav, og at konsekvensen ved et angreb er lille. Statens It har også oplyst, at hvis det lokale netværk bliver forstyrret, kan medarbejderne logge på det centrale netværk via deres mobiltelefon og dermed fortsætte opgaveløsningen.

Rigsrevisionen er enig i, at der kan være en række forhold, som gør det vanskeligt for en hacker at få adgang til at udnytte kendte sårbarheder i netværksudstyret som følge af manglende opdateringer. Løbende opdateringer af netværksudstyret vil dog give Statens It bedre muligheder for at begrænse skaderne, hvis en hacker rent faktisk får adgang til netværket.

2.2. Risikovurdering af sårbarheder ved netværksudstyret

20. Som nævnt har Statens It ikke foretaget sikkerhedsopdateringer på baggrund af en risikovurdering.

21. Ifølge de internationale ISO-standarder for informationssikkerhed er arbejdet med it-sikkerhed risikobaseret. Det betyder, at den ansvarlige myndighed skal indhente informationer om tekniske sårbarheder i de anvendte systemer og evaluere sårbarhederne. Når en potentiel teknisk sårbarhed er identificeret, bør myndigheden identificere de afledte risici og de handlinger, der skal udføres. På baggrund af risikovurderingen skal myndigheden iværksætte passende tiltag.

For at kunne foretage risikovurderingen er det nødvendigt for Statens It at have et overblik over alt det netværksudstyr hos de statslige myndigheder, som Statens It har ansvaret for. Det fremgår af ISO-standarderne, at den ansvarlige institution bør have en fortegnelse over aktiver som en forudsætning for en effektiv styring af tekniske sårbarheder.

22. Vi har undersøgt, om Statens It har et samlet overblik over myndighedernes netværksudstyr, og om de har foretaget en tilstrækkelig risikovurdering af udstyret. Desuden har vi undersøgt Statens It's anvendelse af en teknisk adgangskontrol, der ifølge Statens It er et væsentligt tiltag for at beskytte myndighedernes netværk.

Vores undersøgelse viser, at Statens It fører en fortegnelse over netværksudstyr hos de statslige myndigheder, men at fortegnelsen ikke er fuldstændig. Det betyder, at der kan være netværksudstyr med kritiske sårbarheder, som Statens It ikke kender til. Dermed er forudsætningen for at foretage en tilstrækkelig risikovurdering ikke fuldt til stede.

Vi har sammenholdt det netværksudstyr, som Statens It har registreret, med en adresseliste over de statslige myndigheder, hvor Statens It har ansvaret for it-driften. På nogle af adresserne har Statens It registreret netværksudstyret i et så begrænset omfang, at myndighedernes netværk ikke kan fungere alene med det registrerede netværksudstyr. Det har af ressursemæssige årsager ikke været muligt for os at afdække omfanget af uregistreret netværksudstyr på de mere end 800 lokationer.

Statens It er enige i, at de ikke har et fuldstændigt overblik over netværksudstyret.

23. Undersøgelsen viser også, at Statens It har foretaget en risikovurdering af netværksudstyr. Risikovurderingen er dog overordnet, og Statens It har ikke risikovurderet de enkelte kritiske sårbarheder, i takt med at producenten har udmeldt dem.

Rigsrevisionen skal bemærke, at det fremgår af ISO-standarderne, at der skal indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, at organisationens eksponering for sådanne tekniske sårbarheder skal evalueres, og at der skal igangsættes passende tiltag. Dette understøttes af vores eksterne ekspert, som har oplyst, at man bør forholde sig til de sikkerhedsopdateringer, som producenterne løbende frigiver. Derfor er det ikke tilstrækkeligt med en overordnet risikovurdering.

Rigsrevisionen bemærker, at en overordnet risikovurdering begrænser Statens It's muligheder for at vurdere sandsynligheden for og konsekvensen af, at de enkelte kendte sårbarheder i myndighedernes netværksudstyr bliver udnyttet af hackere. En risikovurdering skal gøre en ansvarlig ledelse i stand til at reagere og prioritere blandt mulige foranstaltninger for at opnå den påkrævede sikkerhed.

Rigsrevisionen anbefaler, at Statens It i lyset af ovenstående fremover forholder sig til risikoen ved de enkelte kritiske sårbarheder.

24. Vi har undersøgt Statens It's anvendelse af en teknisk adgangskontrol på i alt 2.930 stykker netværksudstyr på det kablede netværk. Adgangskontrollen har til formål at sikre, at kun godkendte enheder, fx computere leveret af Statens It, kan få adgang til en myndigheds kablede netværk.

Vores undersøgelse viser, at den tekniske adgangskontrol er fuldt implementeret på 808 ud af de 2.930 stykker netværksudstyr, dvs. at adgangskontrollen omfatter alle ind- og udgange på udstyret. For de resterende 2.122 stykker netværksudstyr har Statens It i større eller mindre grad implementeret adgangskontrollen. Statens It havde på undersøgelsestidspunktet dog ikke fuldt overblik over, om adgangskontrollen var implementeret på alle relevante ind- og udgange på udstyret.

Statens It har efterfølgende oplyst, at adgangskontrollen er implementeret på 94 % af de i alt 2.930 stykker netværksudstyr.

Rigsrevisionen har primo januar 2026 modtaget materiale, der ifølge Statens It dokumenterer, at adgangskontrollen i høj grad er implementeret. Vi har på grund af det sene tidspunkt for modtagelsen ikke haft mulighed for at vurdere dokumentationen.

25. Statens It har oplyst, at de også har andre tiltag, der kan reducere eller fjerne risikoen for og konsekvenserne af, at en hacker kan udnytte sårbarheder i det lokale netværksudstyr hos myndighederne.

Rigsrevisionen er enig i, at andre foranstaltninger kan bidrage til at reducere risikoen for, at sårbarheder i en myndigheds netværk bliver udnyttet. Det er summen af de forskellige lag af beskyttelse, der tilsammen skal beskytte myndighedens netværk bedst muligt. Rigsrevisionen bemærker, at disse foranstaltninger bør være dokumenteret.

Rigsrevisionen, den 9. januar 2026

Birgitte Hansen

/Kristian Brink og Vicky la Cour

Bilag 1. Metodisk tilgang

Undersøgelsen bygger på en gennemgang af dokumenter og på analyser af data. Derudover har vi holdt møder med Statens It og Finansministeriet for at få indsigt i området.

I undersøgelsen har vi inddraget cybersikkerhedsekspert Jacob Herbst, som er teknisk chef i cybersikkerhedsfirmaet Dubex og forperson for Cybersikkerhedsrådet. Jacob Herbst har rådgivet os om de mulige konsekvenser af undersøgelsens resultater, herunder alvorsgraden heraf.

Nedenfor beskriver vi vores kvalitetssikring, data og metode i flere detaljer.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- ISO 27001 fra 2023 og ISO 27002 fra 2022
- kontrakter mellem Statens It og myndighederne
- Statens It's interne vejledninger og retningslinjer
- materiale fra Statens It vedrørende opbygningen af myndighedernes netværk
- materiale fra Statens It vedrørende sikring af myndighedernes netværk
- materiale fra Statens It vedrørende graden af opdatering af netværksudstyret på myndighedernes netværk
- en redegørelse fra Statens It om opfølgning på Rigsrevisionens tidligere afrapporteringer om netværkssikkerhed.

Dataanalyser af de statslige myndigheders netværksudstyr

Undersøgelsens afsnit 2.1 og dele af afsnit 2.2 er baseret på analyser af et datasæt fra Statens It, som indeholder oplysninger om de statslige myndigheders netværksudstyr pr. 21. august 2025. Vi har ikke foretaget fysiske inspektioner hos myndighederne for at validere data fra Statens It. Vi har afgrænset vores analyse til at omfatte tre typer af netværksudstyr: switches, access points og routere. Disse typer af netværksudstyr er forudsætninger for, at der er et netværk. Vi undersøger således både netværksudstyr på det kablede og det trådløse netværk.

Datasættet indeholder netværksudstyr fra den producent, der er hovedleverandør til Statens It. Ud fra Statens It's overblik over netværksudstyr er det Statens It's vurdering, at ca. 99 % af netværksudstyret hos de statslige myndigheder er fra hovedleverandøren. Vores undersøgelse er derfor afgrænset til netværksudstyr fra hovedleverandøren. Rigsrevisionen har ikke undersøgt det resterende netværksudstyr, svarende til ca. 1 %.

Undersøgt netværksudstyr

Switch

En switch bruges fx til at forbinde computere og printere i et netværk, så medarbejderne kan sende filer til udskrivning fra deres computer. Switchen fungerer som en "postcentral", der videresender pakker af data og information fra en enhed til den relevante modtagerenhed.

Access point

Et access point er en enhed, der giver enheder (fx computere) trådløs adgang til et netværk.

Router

En router bruges til at sende data mellem forskellige netværk, fx mellem myndighedens lokale netværk og Statens It's centrale netværk, hvor myndighedens sagsbehandlingssystemer og filer ligger.

For hver af de tre typer af netværksudstyr viser datasættet:

- hvilken model netværksudstyret er
- hvilken version netværksudstyret er opdateret til
- den fysiske lokation for hvert stykke netværksudstyr.

Undersøgelsens afsnit 2.1 er baseret på oplysninger fra den producent af netværksudstyr, der er hovedleverandør til Statens It. Oplysningerne om opdateringer af netværksudstyret og kritiske sårbarheder kommer fra producentens hjemmeside. Vi har sammenholdt disse oplysninger med Statens It's datasæt om myndighedernes netværksudstyr pr. 21. august 2025.

Vi har undersøgt, om producenten stadig frigiver opdateringer til det netværksudstyr, som fremgår af Statens It's liste. Det har vi gjort ved at se på, om den dato, som producenten angiver som "End of Vulnerability/Security Support" på det enkelte netværksudstyr, er overskredet, dvs. om datoen ligger før den 21. august 2025.

For det netværksudstyr, hvor producenten stadig frigiver opdateringer, har vi undersøgt, om udstyret på Statens It's liste har kritiske sårbarheder ifølge producenten.

Undersøgelsens afsnit 2.2 er baseret på en sammenholdelse af Statens It's liste over adresser for de statslige myndigheder med en liste over netværksudstyr fordelt på adresser. Vi har herudover bedt Statens It om at dokumentere deres risikovurdering af de enkelte kritiske sårbarheder på netværksudstyret.

I undersøgelsens afsnit 2.2 har vi desuden gennemgået brugen af en teknisk adgangskontrol på netværksudstyret på det kablede netværk, som skal sikre, at kun godkendte enheder, fx en computer leveret af Statens It, kan få adgang. Vi har herudover bedt Statens It om at dokumentere, at adgangskontrollen er implementeret på alle relevante ind- og udgange på netværksudstyret.

Kvalitetssikring

Undersøgelsen er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos de reviderede samt ledelsesbehandling og sparring med chefer og medarbejdere i Rigsrevisionen.

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).