FOLKETINGET
RIGSREVISIONEN

Oktober 2025

Rigsrevisionens notat om
beretning om

universiteternes beskyttelse af forskningsdata

Opfølgning i sagen om universiteternes beskyttelse af forskningsdata (beretning nr. 8/2018)

18. september 2025

RN 1405/25

I. Baggrund og konklusion

1. Rigsrevisionen følger i dette notat op på sagen om universiteternes beskyttelse af forskningsdata, som blev indledt med en beretning i 2019. Vi har tidligere behandlet sagen i notater til Statsrevisorerne af 11. april 2019, 3. maj 2022 og 2. juni 2023.

2. Universiteterne har forskningsdata af stor værdi, som kan være potentielle mål for cyberangreb eller cyberspionage. Formålet med undersøgelsen var derfor at vurdere, om universiteterne beskyttede forskningsdata i tilstrækkelig grad.

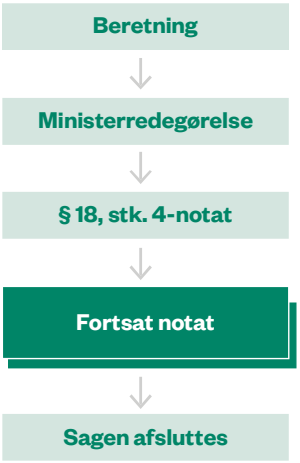
I beretningen kortlagde Rigsrevisionen, om Københavns Universitet (KU), Aarhus Universitet (AU), Aalborg Universitet (AAU), Syddansk Universitet (SDU) og Danmarks Tekniske Universitet (DTU) beskyttede forskningsdata i tilstrækkelig grad mod ukendt it-udstyr. Ukendt it-udstyr er udstyr, der ikke bliver styret og kontrolleret af den centrale it-afdeling, som derfor ikke har kendskab til og kontrol over sikkerheden af udstyret. Ukendt it-udstyr kan fx være udstyr, som forskerne selv medbringer, eller forsknings- og laboratorieudstyr, som er indkøbt via universitetet for forskningsmidler.

Vi undersøgte bl.a., om universiteternes ledelse forholdt sig til risikoen ved ukendt it-udstyr, om universiteterne blokerede deres netværk mod ukendt hardware, og om universiteterne tillod, at forskere havde lokaladministratorrettigheder og dermed kontrol over den computer, som medarbejderen arbejder ved og selv kan installere software på.

3. Da Statsrevisorerne behandlede beretningen, fandt de det utilfredsstillende, at de fem største universiteter ikke beskyttede forskningsdata i tilstrækkelig grad, fx mod ukendt it-udstyr.

4. Rigsrevisionen konstaterede i den seneste opfølgning i juni 2023, at universiteterne havde iværksat en række tiltag i forhold til at øge beskyttelsen af forskningsdata mod ukendt it-udstyr, men at de ikke var helt i mål med at nedbringe risikoen.

Sagsforløb for en større undersøgelse



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

Konklusion

KU, AU, AAU, SDU og DTU har siden opfølgningen i 2023 arbejdet videre med en række tiltag i forhold til at øge beskyttelsen af forskningsdata mod brug af ukendt it-udstyr. Selv om universiteterne har implementeret forskellige initiativer, konstaterer Rigsrevisionen, at ingen af de fem universiteter har nedbragt risikoen i tilstrækkelig grad. I lyset af den høje trussel fra cyberspionage og cyberkriminalitet mod danske universiteter finder Rigsrevisionen det utilfredsstillende, at universiteterne ikke har sikret, at forskningsdata er tilstrækkeligt beskyttet mod risikoen ved at tillade ukendt it-udstyr. Det drejer sig primært om, at ingen af de fem universiteter fuldt ud har blokeret deres netværk mod brug af ukendt it-udstyr.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- universiteternes initiativer i forhold til at sikre, at forskningsdata i tilstrækkelig grad beskyttes mod ukendt it-udstyr.

II. Status på sagen

5. 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. Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn.	Afsluttet i forbindelse med notat til Statsrevisorerne af 3. maj 2022.
2. Uddannelses- og Forskningsministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne.	Afsluttet i forbindelse med notat til Statsrevisorerne af 3. maj 2022.
3. Resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.	Afsluttet i forbindelse med notat til Statsrevisorerne af 3. maj 2022.
4. Resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får rettet op på kritiske it-sikkerhedsbrister.	Afsluttet i forbindelse med notat til Statsrevisorerne af 3. maj 2023 for den del, der vedrører Uddannelses- og Forskningsministeriets og universiteternes arbejde med at identificere kritiske it-sikkerhedsbrister. Følges fortsat for den del, der vedrører resultatet af landets fem største universiteters risikoprofiler i forhold til beskyttelse af forskningsdata – som vi i dette notat har omformuleret til "Universiteternes initiativer i forhold til at sikre, at forskningsdata i tilstrækkelig grad beskyttes mod ukendt it-udstyr".

III. Universiteternes initiativer

6. Vi gennemgår i det følgende de fem universiteters initiativer i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr.

7. Opfølgningen er baseret på skriftlige statusbeskrivelser og dokumentation fra de fem universiteter og møde med nogle af universiteternes centrale it-afdelinger. Resultaterne i det følgende beskriver situationen ved afslutningen af revisionen primo juni 2025.

Universiteternes initiativer i forhold til at sikre, at forskningsdata i tilstrækkelig grad beskyttes mod ukendt it-udstyr

8. Rigsrevisionens beretning fra 2019 kortlagde, om de fem største universiteter beskyttede forskningsdata i tilstrækkelig grad i forhold til seks udvalgte risikofaktorer. Vores opfølgning i 2023 viste, at universiteterne var kommet i mål med at beskytte forskningsdata i tilstrækkelig grad mod ukendt it-udstyr i forhold til tre af seks risikofaktorer.

9. Vi har derfor fulgt op på de tre risikofaktorer, hvor opfølgningen i 2023 viste, at forskningsdata ikke blev beskyttet i tilstrækkelig grad mod ukendt it-udstyr. De tre risikofaktorer er, om:

- universitetet tillader forskere at tage eget udstyr med
- universitetet blokerer sine netværk mod ukendt hardware (dvs. ukendt it-udstyr)
- universitetet tillader, at forskere har lokaladministratorrettigheder.

Tillader universiteterne, at forskere tager eget udstyr med?

10. Det fremgik af beretningen fra 2019 og Rigsrevisionens senere opfølgning, at SDU var det eneste universitet, der ikke tillod forskere at tage eget udstyr med.

Opfølgningen i 2023 viste, at KU, AU, AAU og DTU tillod forskere at medbringe ukendt it-udstyr, men at universiteterne havde implementeret kompenserende foranstaltninger. Rigsrevisionen bemærkede dengang, at de kompenserende foranstaltninger ikke fuldt ud reducerede risikoen ved ukendt it-udstyr.

Kompenserende foranstaltning
En kompenserende foranstaltning kan fx være opdateret informationssikkerhedspolitik.

11. Rigsrevisionen konstaterer, at de fire universiteter fortsat tillader, at forskere tager eget udstyr med, og at de kompenserende foranstaltninger stadig ikke fuldt ud reducerer risikoen herved.

Blokerer universiteterne deres netværk mod ukendt hardware/it-udstyr?
12. Det fremgik af beretningen fra 2019, at KU, SDU og DTU delvist havde blokeret deres netværk mod ukendt hardware, mens AU og AAU ikke havde.

Opfølgningen i 2023 viste, at AU havde blokeret sit netværk mod ukendt hardware/it-udstyr, men at blokeringen kunne omgås. KU, SDU og DTU havde delvist blokeret deres netværk, mens AAU ikke havde blokeret sine netværk. Alle fem universiteter havde kompenserende foranstaltninger, som ikke fuldt ud reducerede risikoen ved ukendt hardware/it-udstyr.

13. Rigsrevisionen konstaterer, at de fem universiteter er i gang med at implementere forskellige initiativer med henblik på at blokere deres netværk mod ukendt hardware/it-udstyr – eller sikre, at blokeringen ikke kan omgås. Vi konstaterer dog, at universiteterne er forsinkede med 1-5 år i forhold til planen. Det gælder særligt for DTU, som er forsinket med ca. 5 år og dermed forventer at have implementeret blokeringen i 2030. Rigsrevisionen anerkender, at der er tale om en omfattende opgave, men finder, at DTU's forsinkelse er meget stor. Rigsrevisionen konstaterer, at DTU's ledelse kender risikoen ved, at en blokering først er gennemført i 2030. Ligeledes har AAU har oplyst, at universitetets ledelse er opmærksom på risikoen ved, at blokeringen er forsinket.

Rigsrevisionen konstaterer, at universiteterne dermed fortsat er udsat for risikoen ved ukendt hardware/it-udstyr.

Tillader universiteterne, at forskere har lokaladministratorrettigheder?
14. Det fremgik af beretningen fra 2019, at alle fem universiteter i et vist omfang tillod forskere at få lokaladministratorrettigheder. Forskere med lokaladministratorrettigheder kan selv installere software på computere. Det medfører en risiko for, at den centrale it-afdeling ikke har et overblik over, hvilken software der installeres, eller ikke kan gennemtvinge opdateringer.

Opfølgningen i 2023 viste, at KU og AAU havde håndteret dette. Vores opfølgning i 2025 omfatter derfor AU, SDU og DTU. AU tillod ved vores opfølgning i 2023, at forskere havde lokaladministratorrettigheder. Opfølgningen viste også, at SDU og DTU som udgangspunkt ikke tillod lokaladministratorrettigheder for Windows-pc'er, men at universiteterne ikke fulgte op på, om Mac-computere var opdaterede, og at universiteterne ikke gennemtvang opdateringerne.

15. Vores opfølgning viser, at AU har inddraget permanente lokaladministratorrettigheder og implementeret et værktøj til at tildele forskere tidsbegrænsede lokaladministratorrettigheder på både Windows-pc'er og Mac-computere. Vi vurderer derfor, at dette punkt kan afsluttes for AU.

SDU følger nu op på, om Mac-computere er opdaterede, og blokerer for computere, der ikke opdateres. Vi vurderer derfor, at dette punkt kan afsluttes for SDU.

DTU følger fortsat ikke op på, om Mac-computere er opdaterede, og gennemtvinger eller låser heller ikke Mac-computere, som ikke er opdaterede.

Sammenfatning

16. Tabel 1 viser resultaterne fra opfølgningen på de fem universiteters initiativer. Vi har vurderet, om universiteternes initiativer for hver risikofaktor øger (rød), delvist øger (gul) eller ikke øger (grøn) risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

Tabel 1

Opfølgning på risikofaktorerne i 2025

Risikofaktor	KU	AU	AAU	SDU	DTU
Universitetet tillader forskere at tage eget udstyr med	🟡	🟡	🟡	-	🟡
Universitetet blokerer sine netværk mod ukendt hardware (dvs. ukendt it-udstyr)	🟡	🟡	🔴	🟡	🟡
Universitetet tillader, at forskere har lokaladministratorrettigheder	-	🟢	-	🟢	🟡

Note: "-" angiver, at Rigsrevisionen i beretningen fra 2019 eller i notatet af 2. juni 2023 vurderede, at universiteterne var kommet i mål med at beskytte forskningsdata i tilstrækkelig grad mod ukendt it-udstyr i forhold til den pågældende risikofaktor.

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgninger fra 2023 og 2025.

Det fremgår af tabel 1, at universiteterne endnu ikke er helt i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

17. Rigsrevisionen vil på baggrund af ovenstående fortsat følge universiteternes initiativer i forhold til at sikre, at forskningsdata i tilstrækkelig grad beskyttes mod ukendt it-udstyr.

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

Birgitte Hansen