FOLKETINGET
RIGSREVISIONEN

Juni 2023

Rigsrevisionens notat om
beretning om

universiteternes beskyttelse af forskningsdata

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

2. juni 2023

RN 1407/23

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 notat til Statsrevisorerne af 11. april 2019 og af 3. maj 2022.

Universiteterne har forskningsdata af stor værdi. Derfor er universiteternes forskningsdata et potentielt mål for cyberangreb eller cyberspionage. Af Center for Cybersikkerheds seneste trusselvurdering fra februar 2023 fremgår det, at truslen fra cyberspionage mod universiteter er blevet hævet fra høj til meget høj. Center for Cybersikkerhed uddyber, at den øgede trussel kommer fra flere fremmede stater, og at der de seneste år er set flere forsøg på cyberangreb rettet mod danske universiteter. På grund af det høje trusselsniveau er det centralt, at universiteterne har en høj it-sikkerhed, der beskytter forskningsdata.

I notatet af 3. maj 2022 fandt Rigsrevisionen, henset til universiteternes høje trusselsniveau, at tempoet for arbejdet med at rette op på kritiske it-sikkerhedsbrister ikke havde været tilfredsstillende. Statsrevisorerne tilkendegav på deres møde den 16. maj 2022 ved behandlingen af notatet, at de ønskede en hurtig opfølgning på denne sag på grund af sagens alvorlige karakter.

Rigsrevisionen har som led i opfølgningen udført nye it-revisioner i 2022. Resultatet af disse har været i særskilt høring på universiteterne.

Dette notat omhandler de udestående punkter fra beretningen om opfølgning på landets 5 største universiteters risikoprofiler i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Endvidere omhandler notatet en særskilt it-revision af Københavns Universitets arbejde med it-sikkerhed i forhold til beskyttelse af forskningsdata.

Sagsforløb for en større undersøgelse

- Beretning
- Ministerredegørelse
- § 18, stk. 4-notat
- **Fortsat notat**
- Sagen afsluttes

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

Konklusion

Rigsrevisionen konstaterer på baggrund af en særskilt it-revision af Københavns Universitets arbejde med it-sikkerhed, at universitet har foretaget et stort arbejde for at forbedre beskyttelsen af forskningsdata. Det finder Rigsrevisionen tilfredsstillende og vurderer, at denne del af sagen kan afsluttes. Rigsrevisionen baserer denne konklusion på følgende:

- Københavns Universitets centrale it-afdeling og 3 udvalgte institutter opfylder Rigsrevisionens særskilte it-revisions kontrolmål for beskyttelse af forskningsdata.

Rigsrevisionen har videre foretaget en opfølgning på landets 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Ukendt it-udstyr kan fx være forskeres eget medbragte it-udstyr, som it-afdelingerne ikke er blevet orienteret om og dermed ikke har kendskab til.

Rigsrevisionen konstaterer på baggrund af opfølgningen på Københavns Universitet (KU), Aarhus Universitet (AU), Aalborg Universitet (AAU), Syddansk Universitet (SDU) og Danmarks Tekniske Universitet (DTU), at universiteterne har iværksat en række tiltag i forhold til at øge beskyttelsen af forskningsdata mod ukendt it-udstyr. Rigsrevisionen vurderer dog, at universiteterne endnu ikke er helt i mål med at nedbringe risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

Rigsrevisionen vil derfor fortsat følge udviklingen og orientere Statsrevisorerne om:

- resultatet af landets 5 største universiteters risikoprofiler i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr.

I. Baggrund

2. Rigsrevisionen afgav i januar 2019 en beretning om universiteternes beskyttelse af forskningsdata, som byggede på resultater fra Rigsrevisionens it-revision, der var udført i perioden marts-oktober 2018. I beretningen kortlagde Rigsrevisionen de 5 største danske universiteters, KU, AU, AAU, SDU og DTU, risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Rigsrevisionens kortlægning af de 5 universiteters risikoprofil omfattede undersøgelse af 6 risikofaktorer. Risikofaktorerne omfatter bl.a., om universiteternes ledelse forholder sig til risikoen ved ukendt it-udstyr, om universiteterne blokerer sine netværk mod ukendt hardware, samt om universiteterne tillader forskere lokaladministratorrettigheder og dermed kontrol over den computer, som medarbejderen arbejder ved, og selv kan installere software på. Dernæst gik beretningen i dybden med at undersøge, hvordan det største universitets, KU, centrale it-afdeling og 3 udvalgte institutter arbejdede med it-sikkerheden i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr.

3. Da Statsrevisorerne behandlede beretningen, fandt de det utilfredsstillende, at de 5 største universiteter i Danmark ikke beskyttede forskningsdata i tilstrækkelig grad, fx mod ukendt it-udstyr.

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

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.	Behandles i dette notat. Opfølgningspunktet adskiller sig fra nr. 3, idet ministeriet og universiteterne nu har identificeret it-sikkerhedsbrister. Denne opfølgning omhandler derfor kun, hvorvidt universiteterne har rettet op på it-sikkerhedsbristerne.

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

5. Vi redegør i dette notat for resultaterne af opfølgningen på ovenstående punkt.

I notatet af 3. maj 2022 anførte Rigsrevisionen bl.a., at Uddannelses- og Forskningsministeriets iværksatte initiativer i forhold til at få universiteterne til at rette op på kritiske it-sikkerhedsbrister var tilfredsstillende. Rigsrevisionen vurderede dog, at ministeriets bestræbelser endnu ikke havde ført til, at alle universiteterne havde rettet op på kritiske it-sikkerhedsbrister i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Denne opfølgning omhandler derfor ikke ministeriets initiativer og bestræbelser, som vi tidligere har fundet tilfredsstillende. Opfølgningen omhandler i stedet resultatet af universiteternes arbejde med at sikre beskyttelse af forskningsdata mod ukendt udstyr.

Opfølgningen er foretaget via:

- en særskilt it-revision af KU's opfyldelse af de kontrolmål, der var afrapporteret som ikke opfyldt (røde)- eller delvist opfyldt (gule) i notatet af 3. maj 2022
- en opfølgning på risikofaktorerne i kortlægningen af de 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr.

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

Ukendt it-udstyr
Ukendt it-udstyr er i dette notat en betegnelse for udstyr, der ikke bliver styret og kontrolleret af den centrale it-afdeling på universitetet. Den centrale it-afdeling har derfor ikke kendskab til og kontrol over sikkerheden af udstyret, herunder om systemet fx er sikkerhedsopdateret. Ukendt it-udstyr omfatter både diverse udstyr, som forskerne selv medbringer (Bring Your Own Device (BYOD)), og fx forsknings- og laboratorieudstyr indkøbt via universitetet for forskningsmidler.

II. Universiteternes initiativer

6. Rigsrevisionen har i perioden 2022-2023 fulgt op på universiteternes initiativer. Opfølgningen falder i 2 dele:

Opfølgningen på den særskilte it-revision af KU er foretaget hos den centrale it-afdeling på KU (KU-IT) og 3 udvalgte institutter (Biomedicinsk Institut på Det Sundhedsvidenskabelige Fakultet, Institut for Nordiske Studier og Sprogvidenskab på Det Humanistiske Fakultet og Niels Bohr Institutet på Det Natur- og Biovidenskabelige Fakultet). De 3 institutter er valgt for at dække så stor en del af KU's virksomhed som muligt, ligesom de er valgt ud fra en spredning på forskellige parametre. Fx havde Niels Bohr Institutet i 2018 og ved opfølgningen fra 2022 sin egen it-organisation i modsætning til de andre, der hører under KU's centrale it-afdeling (KU-IT). De 3 institutter er desuden valgt for at dække forskellige typer data, der er særligt væsentlige at beskytte, herunder særlige personoplysninger, data med høj økonomisk værdi og data underlagt kontraktuelle krav. Revisionen er baseret på revisionsbesøg og skriftlig dokumentation.

Opfølgningen på kortlægningen af KU's, AU's, AAU's, SDU's og DTU's risikoprofiler i forhold til beskyttelse af forskningsdata er baseret på revisionsbesøg hos universiteternes centrale it-afdelinger samt på skriftlig dokumentation. Resultaterne i det følgende er baseret på situationen ved afslutningen af revisionen primo maj 2023.

Opfølgning på KU's beskyttelse af forskningsdata

7. Beretningen gik i en særskilt it-revision i dybden ved at undersøge, hvordan landets største universitet, KU, arbejdede med it-sikkerheden i forhold til beskyttelse af forskningsdata. Undersøgelsen tog udgangspunkt i KU's centrale it-afdeling (KU-IT) og 3 udvalgte institutter.

Vi har fulgt op på de kontrolmål fra beretningen, som ikke var opfyldt eller var delvist opfyldt ved opfølgningen fra 2022. Vi har fulgt op ved at foretage særskilte it-revisioner hos KU-IT og hos de 3 udvalgte institutter. For selv om KU-IT leverer service til hovedparten af KU, så har hvert institut også et ansvar for at bidrage til beskyttelse af forskningsdata. Resultatet afrapporteres dog som tidligere i en samlet KU-vurdering.

Opfølgningen viser, at KU nu opfylder de kontrolmål, som ikke var opfyldt eller var delvist opfyldt, da Rigsrevision sidst behandlede sagen i notat af 3. maj 2022. Rigsrevisionens vurdering er baseret på, at KU-IT og de 3 institutter alle lever op til kravene.

Vi gennemgår KU's opfyldelse af de enkelte kontrolmål nedenfor.

Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU

8. Vi har fulgt op på KU's ledelsesmæssige opmærksomhed på styring af it-udstyr. Tabel 1 viser beretningens resultater sammenholdt med opfølgningen fra 2022 og 2023.

Tabel 1

Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU ved undersøgelsestidspunktet for beretningen sammenholdt med opfølgningen fra 2022 og 2023

	Beretningen	2022	2023
Universitetet har ledelsesgodkendt politik og retningslinjer for styring af it-udstyr (hardware og software)	●	●	-
Universitetet har vurderet trusler mod sin anvendelse af it og har dokumenteret trusselsvurderingen	●	●	●
Universitetet har vurderet risici ved at anvende it i forskningen og har dokumenteret risikovurderingen	●	●	●

Note: For hvert kontrolmål har Rigsrevisionen vurderet, om KU har opfyldt kontrolmålet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt). "-" angiver, at der ikke er foretaget en opfølgning på kontrolmålet i 2023, da kontrolmålet var opfyldt ("grøn") i 2022.

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgninger fra 2022 og 2023.

Det fremgår af tabel 1, at KU i denne opfølgning har vurderet trusler og risici ved at anvende ukendt it-udstyr i forskningen og har dokumenteret vurderingerne. Det finder Rigsrevisionen tilfredsstillende.

KU's beskyttelse af forskningsdata

9. Vi har fulgt op på, om KU sikrer, at data beskyttes i overensstemmelse med de ledelsesgodkendte politikker og retningslinjer. Tabel 2 viser beretningens resultater sammenholdt med opfølgningen fra 2022 og 2023.

Tabel 2

KU's beskyttelse af forskningsdata ved undersøgelsestidspunktet for beretningen sammenholdt med opfølgningen fra 2022 og 2023

	Beretningen	2022	2023
Universitetet sikrer, at klassificerede forskningsdata beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer herfor	●	●	●

Note: Rigsrevisionen har vurderet, om KU har opfyldt kontrolmålet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgninger fra 2022 og 2023.

Det fremgår af tabel 2, at KU sikrer, at klassificerede forskningsdata nu beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer herfor. Rigsrevisionen vurderer, at KU's tiltag samlet giver en bedre beskyttelse af forskningsdata. Det finder Rigsrevisionen tilfredsstillende.

KU's overblik over anvendt hardware

10. Vi har fulgt op på, om KU har fortegnelser over hardware, som forskerne på universitetet anvender. Derudover har vi undersøgt, om KU identificerer eventuelt ukendt hardware på netværket. Tabel 3 viser beretningens resultater sammenholdt med opfølgningen fra 2022 og 2023.

Tabel 3

KU's overblik over anvendt hardware ved undersøgelsestidspunktet for beretningen sammenholdt med opfølgningen fra 2022 og 2023

	Beretningen	2022	2023
Universitetet har en komplet og opdateret fortegnelse over hardware (servere og desktops), som har adgang til netværk, der indeholder systemer og data, som er vigtige for forskningen	🟡	🟡	🟢
Universitetet anvender en metode til at opdage ukendt hardware på netværk med forskningsdata	🔴	🟡	🟢

Note: For hvert kontrolmål har Rigsrevisionen vurderet, om KU har opfyldt kontrolmålet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgninger fra 2022 og 2023.

Det fremgår tabel 3, at KU nu har fortegnelser over KU-styret hardware (servere og desktops), der har adgang til netværk, og som indeholder systemer og data, der er vigtige for forskningen.

Opfølgningen viser videre, at KU har implementeret et nyt netværk, der medfører, at ukendt it-udstyr automatisk kun får adgang til internettet og dermed ikke adgang til netværk med forskningsdata. Endelig viser opfølgningen, at KU-IT som en ekstra sikkerhed foretager interne automatiserede, kontinuerlige scanninger af både kendt og ukendt it-udstyr/Bring Your Own Device (BYOD) på netværket. Det finder Rigsrevisionen tilfredsstillende.

KU's overblik over software og softwareopdatering

11. Vi har fulgt op på KU's overblik over software og softwareopdatering. Tabel 4 viser beretningens resultater sammenholdt med opfølgningen fra 2022 og 2023.

Tabel 4

KU's overblik over software og softwareopdatering ved undersøgelsestidspunktet for beretningen sammenholdt med opfølgningen fra 2022 og 2023

	Beretningen	2022	2023
Universitetet har overblik over anvendt software på pc'er, og om den anvendte software er opdateret	●	●	●
Universitetet har overblik over anvendt software på servere, og om den anvendte software er opdateret	●	●	-

Note: For hvert kontrolmål har Rigsrevisionen vurderet, om KU har opfyldt kontrolmålet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt). "-" angiver, at der ikke er foretaget en opfølgning på kontrolmålet i 2023, da kontrolmålet var opfyldt ("grøn") i 2022.

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgninger fra 2022 og 2023.

Det fremgår af tabel 4, at KU nu har overblik over anvendt software på pc'er, der styres af KU-IT, og at den anvendte software er opdateret. De pc'er, som ikke styres af KU-IT (dvs. ukendt it-udstyr), har kun adgang til internettet og dermed ikke adgang til forskningsdata, hvorfor risikoen er reduceret. Det finder Rigsrevisionen tilfredsstillende.

Opfølgning på kortlægning af de 5 største universiteters risikoprofiler

12. I Rigsrevisionens beretning blev der foretaget en kortlægning af de 5 største universiteters (KU, AU, AAU, SDU og DTU) risikoprofiler af beskyttelse af forskningsdata i forhold til 6 udvalgte risikofaktorer. Rigsrevisionen konstaterede ved opfølgningen fra 2022, at ikke alle universiteter var i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad.

13. Vi har derfor fulgt op på universiteternes risikoprofiler i forhold til de 6 udvalgte risikofaktorer:

- Forholder universitetets ledelse sig til risikoen ved ukendt it-udstyr?
- Tillader universitetet "Bring Your Own Device" (BYOD)?
- Er der fundet ukendt hardware (dvs. ukendt it-udstyr) på universitetets netværk?
- Blokerer universitetet sine netværk mod ukendt hardware (dvs. ukendt it-udstyr)?
- Tillader universitetet forskerne lokaladministratorrettigheder?
- Har der været hændelser på universitetet på baggrund af ukendt it-udstyr?

Vi har fulgt op på de risikofaktorer, som blev afrapporteret som "rød" eller "gul" i beretningen fra 2019 for de enkelte universiteter. Tabel 5 viser resultaterne fra opfølgningen på de 5 universiteter.

Tabel 5
Opfølgning på universiteternes risikoprofil i 2023

Risikofaktor	KU	AU	AAU	SDU	DTU
Forholder universitetets ledelse sig til risikoen ved ukendt it-udstyr?	●	-	●	-	●
Tillader universitetet "Bring Your Own Device" (BYOD)?	●	●	●	-	●
Er der fundet ukendt hardware (dvs. ukendt it-udstyr) på universitetets netværk?	●	●	●	●	●
Blokerer universitetet sine netværk mod ukendt hardware (dvs. ukendt it-udstyr)?	●	●	●	●	●
Tillader universitetet forskerne lokaladministratorrettigheder?	●	●	●	●	●
Har der været hændelser på universitetet på baggrund af ukendt it-udstyr?	●	-	-	●	-

Note: Rigsrevisionen har vurderet, om risikofaktoren øger (rød), delvist øger (gul) eller ikke øger (grøn) risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

"-" angiver, at der ikke er foretaget en opfølgning på risikofaktoren i 2023, da Rigsrevisionen i beretningen fra 2019 vurderede, at risikofaktoren ikke øgede risikoen for, at forskningsdata ikke blev beskyttet i tilstrækkelig grad mod ukendt it-udstyr.

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgning fra 2023.

Det fremgår af tabel 5, at universiteterne fortsat har nogle sikkerhedsbrister og derfor endnu ikke er helt i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

Vi gennemgår universiteternes risikoprofil i forhold til de 6 risikofaktorer nedenfor.

Forholder universiteternes ledelser sig til risikoen ved ukendt it-udstyr?
14. Det fremgik af beretningen fra 2019, at kun AU's og SDU's ledelser havde forholdt sig til risikoen ved ukendt it-udstyr i tilstrækkeligt omfang. KU's, AAU's og DTU's ledelser havde ikke forholdt sig til risikoen ved ukendt it-udstyr i tilstrækkeligt omfang.

Opfølgningen viser, at alle universiteternes ledelser nu aktivt har forholdt sig til risikoen ved ukendt it-udstyr. Det finder Rigsrevisionen tilfredsstillende.

Tillader universiteterne "Bring Your Own Device" (BYOD)?
15. Det fremgik af beretningen, at det kun var SDU og DTU, der ikke tillod forskere BYOD. I forbindelse med opfølgningen fra 2022 blev Rigsrevisionen dog bekendt med, at DTU alligevel tillod forskere at medbringe ukendt it-udstyr. SDU var således det eneste universitet, der ikke tillod forskere BYOD.

Opfølgningen viser, at KU, AU, AAU og DTU fortsat tillader forskere at medbringe ukendt it-udstyr. Dog har alle 4 universiteter implementeret kompenserende foranstaltninger, der delvist reducerer risikoen. Rigsrevisionen bemærker, at de kompenserende foranstaltninger ikke fuldt ud reducerer risikoen ved ukendt it-udstyr/BYOD.

Er der fundet ukendt hardware (dvs. ukendt it-udstyr) på universiteternes netværk?
16. Det fremgik af beretningen fra 2019, at der var fundet ukendt hardware på alle 5 universiteters netværk.

Opfølgningen viser, at der fortsat findes ukendt hardware på alle 5 universiteters netværk. Opfølgningen viser dog også, at alle 5 universiteter nu har implementeret kompenserende foranstaltninger, der reducerer risikoen ved ukendt hardware på universiteternes netværk. Det finder Rigsrevisionen tilfredsstillende.

Blokerer universiteterne deres netværk mod ukendt hardware?
17. 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 blokeret deres netværk mod ukendt hardware.

Opfølgningen viser, at AU nu – som det eneste af de 5 universiteter – har blokeret sit netværk mod ukendt hardware, men opfølgningen viser også, at blokeringen indeholder en teknisk svaghed, der gør, at blokeringen kan omgås. Opfølgningen viser videre, at KU, SDU og DTU fortsat delvist har blokeret deres kablede netværk mod ukendt hardware. Opfølgningen viser derudover, at AAU fortsat ikke har blokeret det kablede netværk mod ukendt it-udstyr. AAU har oplyst, at AAU i 2023 vil gå i gang med at blokere det kablede netværk mod ukendt udstyr. Rigsrevisionen konstaterer, at de 4 universiteter har en kompenserende foranstaltning, men Rigsrevisionen bemærker, at det ikke fuldt ud reducerer risikoen ved ukendt udstyr.

Alle 5 universiteter har i forbindelse med opfølgningen oplyst, at de vil implementere blokering mod ukendt it-udstyr på hele det kablede net, og AU vil få løst den tekniske svaghed, så blokeringen ikke kan omgås. Universiteterne har oplyst, at det er en omfattende opgave, og at de forventer at have færdigimplementeret blokering mv. mod ukendt udstyr inden for en tidshorisont fra efteråret 2024 og frem til udgangen af 2026.

Tillader universiteterne forskere lokaladministratorrettigheder?
18. Det fremgik af beretningen fra 2019, at alle 5 universiteter i et vist omfang tillod forskere at få lokaladministratorrettigheder, så de fx kunne installere software, selv om det udgjorde en sikkerhedsrisiko.

Opfølgningen viser, at KU og AAU nu ikke længere tillader forskere at have permanente lokaladministratorrettigheder på Windows-pc'er styret af universiteternes centrale it-delinger. For Mac-computere, hvor lokaladministratorrettighederne som udgangspunkt ikke kan begrænses, har KU og AAU i stedet sikret, at computerne er opdaterede, og har enten gennemtvunget opdateringer eller har låst Mac-computerne, så de ikke kan bruges. Det finder Rigsrevisionen tilfredsstillende.

Opfølgningen viser videre, at SDU og DTU som udgangspunkt heller ikke tillader lokaladministratorrettigheder for Windows-pc'er, der er styret af den centrale it-afdeling. Opfølgningen viser dog, at DTU ikke følger op på, om Mac-computere er opdaterede, og ikke gennemtvinger opdateringerne. SDU følger op på, om Mac-computere er opdaterede. SDU har siden februar 2023 kørt et projekt med henblik på enten at få opdateret eller skrottet alle gamle Mac-computere. SDU har således reduceret antallet af Mac-computere, der ikke har et acceptabelt patchniveau, markant og forventer at være i mål med det medio juni 2023.

Endelig viser opfølgningen, at AU fortsat tillader forskere at have lokaladministratorrettigheder. Det finder Rigsrevisionen utilfredsstillende. Rigsrevisionen bemærker dog, at AU har været i gang med at implementere en løsning, men AU fandt ud af, at løsningen ikke levede op til universitetets behov. AU vil derfor implementere en ny løsning.

Har der været hændelser på universiteterne på baggrund af ukendt it-udstyr?
19. Det fremgik af beretningen fra 2019, at KU og SDU havde oplevet sikkerhedshændelser, der kunne henføres til brug af ukendt it-udstyr, fx fordi forskerne ikke havde sikkerhedsopdateret deres it-udstyr eller havde anvendt andet it-udstyr og andre dataopbevaringsløsninger end dem, som universiteterne stillede til rådighed. AU, AAU og DTU havde ikke oplevet sådanne hændelser.

Opfølgningen viser, at KU ikke har oplevet sikkerhedshændelser på baggrund af ukendt it-udstyr i opfølgningsperioden (fra 2022 til primo 2023). SDU har oplevet sikkerhedshændelser på baggrund af ukendt it-udstyr, men SDU har, efter det oplyste, opdaget og håndteret hændelserne inden for få timer.

Sammenfatning om universiteternes arbejde i forhold til, at universiteterne får rettet op på kritiske it-sikkerhedsbrister

20. Rigsrevisionen finder det tilfredsstillende, at den særskilte it-revision af KU's centrale it-afdeling og 3 institutter viser, at universitetet har opfyldt Rigsrevisionens kontrolmål for beskyttelse af forskningsdata. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes.

Rigsrevisionen vurderer på baggrund af opfølgningen på kortlægningen af de 5 universiteters risikoprofiler, at universiteterne har foretaget et stort arbejde i forhold til at få rettet op på kritiske it-sikkerhedsbrister mod ukendt it-udstyr. Rigsrevisionen finder dog, at universiteterne fortsat har nogle it-sikkerhedsbrister og derfor endnu ikke helt er i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr. Det drejer sig primært om, at ingen af de 5 universiteter i tilstrækkelig grad har blokeret deres netværk mod ukendt it-udstyr.

Rigsrevisionen vil derfor fortsat følge resultatet af landets 5 største universiteters risikoprofiler i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr.

Birgitte Hansen