FOLKETINGET
RIGSREVISIONEN

Maj 2019

Rigsrevisionens notat om
beretning om

universiteternes beskyttelse af forskningsdata

Vedrører:

Statsrevisorernes beretning nr. 8/2018 om universiteternes beskyttelse af forskningsdata

11. april 2019

RN 1404/19

Uddannelses- og forskningsministerens redegørelse af 18. marts 2019

1. Rigsrevisionen vurderer i dette notat de initiativer, som uddannelses- og forskningsministeren vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner.

Konklusion

Uddannelses- og forskningsministeren redegør i sin ministerredegørelse for de overvejelser og foranstaltninger, som beretningen har givet Uddannelses- og Forskningsministeriet anledning til. Ministeren oplyser, at Rigsrevisionen med beretningen har sat fokus på it- og informationssikkerhed og beskyttelse af forskningsdata på universiteterne, og at ministeriet og universiteterne finder, at høj it- og informationssikkerhed, der beskytter forskningsdata, er vigtigt og skal have høj prioritet.

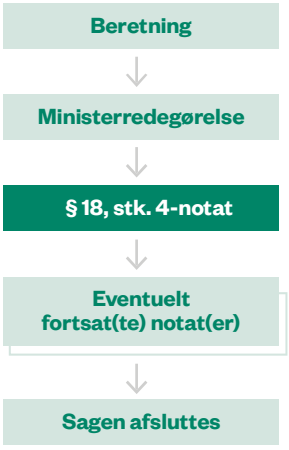
Uddannelses- og forskningsministeren oplyser videre, at Uddannelses- og Forskningsministeriet vil inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn i 2019. Derudover vil ministeriet i samarbejde med universiteterne arbejde med at etablere en tværgående trusselsvurdering for universiteterne.

Allerede i forbindelse med beretningen oplyste Uddannelses- og Forskningsministeriet endvidere, at ministeriet ville kontakte universiteterne og understrege ledelsernes ansvar for området og samtidig bede universiteterne om at identificere og rette op på eventuelle it-sikkerhedsbrister.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn
- Uddannelses- og Forskningsministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne
- resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.

Sagsforløb for en større undersøgelse



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

I. Baggrund

2. Rigsrevisionen afgav i januar 2018 en beretning om universiteternes beskyttelse af forskningsdata på Uddannelses- og Forskningsministeriets område. Baggrunden for undersøgelsen var bl.a., at Center for Cybersikkerhed på baggrund af et større hackerangreb mod flere danske universiteter i perioden 2014-2016 har vurderet, at cybertruslen mod universiteterne er stor. Årsagen til det høje trusselsniveau skyldes bl.a., at universiteterne er forholdsvis åbne institutioner, hvor forskerne har store frihedsgrader med hensyn til at anvende eget it-udstyr og lokaladministratorrettigheder i forskningen. På grund af det høje trusselsniveau er det centralt, at universiteterne har en høj it-sikkerhed, der beskytter forskningsdata. Formålet med undersøgelsen var derfor at vurdere, om universiteterne beskyttede forskningsdata i tilstrækkelig grad. Først kortlagde vi de 5 største danske universiteters risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Dernæst gik vi mere i dybden på det største universitet, Københavns Universitet, for at undersøge, hvordan universitetets centrale it-afdeling og 3 udvalgte institutter arbejdede med it-sikkerheden i forhold til beskyttelse af forskningsdata.

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

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

II. Gennemgang af ministerens redegørelse

Universiteternes implementering af ISO 27001

5. Statsrevisorerne bemærkede, at der på Københavns Universitet er uklarhed om, hvorvidt ansvaret for at beskytte forskningsdata ligger centralt hos universitetets ledelse, på institutterne eller hos den enkelte forsker. Statsrevisorerne bemærkede videre, at undersøgelsen indikerer, at opgaven med at beskytte forskningsdata heller ikke løses tilfredsstillende på centralt og decentralt niveau på de øvrige universiteter.

Det fremgik også af beretningen, at Københavns Universitet havde valgt at følge ISO 27001, men ikke havde udarbejdet en trusselsvurdering eller en risikovurdering, som ISO 27001 ellers foreskriver. Derudover havde ledelsen kun fastsat utilstrækkelige overordnede rammer for anvendelse og styring af it-udstyr på universitetet. Implementeringen af ISO 27001 blev ikke undersøgt for de 4 øvrige universiteter, men undersøgelsen viste, at ingen af de 5 undersøgte universiteter fra centralt hold sikrer, at forskningsdata beskyttes tilfredsstillende, ligesom ikke alle universiteters ledelser har forholdt sig til risikoen for ukendt it-udstyr.

Uddannelses- og forskningsministeren oplyser, at Uddannelses- og Forskningsministeriet som led i det systematiske tilsyn i 2019 vil bede hvert enkelt universitet om en status på implementeringen af ISO 27001-standarden. Redegørelserne fra universiteterne vil foreligge primo september 2019.

6. Rigsrevisionen vil følge Uddannelses- og Forskningsministeriets arbejde med at sikre, at universiteterne får implementeret ISO 27001-standarden.

Etablering af en tværgående trusselsvurdering for universiteterne

7. Statsrevisorerne bemærkede, at Center for Cybersikkerhed finder truslen fra cyberspionage mod de danske offentlige forskningsinstitutioner høj. Det fremgik også af beretningen, at Københavns Universitet ikke har udarbejdet en trusselsvurdering.

Uddannelses- og forskningsministeren oplyser, at Uddannelses- og Forskningsministeriet har aftalt med universiteterne at igangsætte en dialogproces i regi af universiteternes CIO-gruppe, som består af universiteternes it-chefer, bl.a. med henblik på at etablere en opdateret tværgående trusselsvurdering for hele universitetssektoren og aftale kadence for opdatering. Dette vil bl.a. ske med inddragelse af Center for Cybersikkerhed. Ministeren oplyser videre, at det forventes, at samarbejdet mellem CIO-gruppen og ministeriet kan bidrage til at identificere tværgående sårbarheder og særligt vigtige perspektiver, som universiteterne bør have opmærksomhed på i deres respektive arbejde med ISO 27001-standarden.

8. Rigsrevisionen vil følge Uddannelses- og Forskningsministeriets arbejde med at etablere den tværgående trusselsvurdering for hele universitetssektoren.

Løsninger til at rette op på kritiske sikkerhedsbrister

9. Statsrevisorerne bemærkede, at flere universiteter giver adgang til, at forskerne medbringer eget it-udstyr, og at alle 5 universiteter tillader forskere rettigheder som lokaladministratorer. Det betyder bl.a., at de selv kan installere software, og at ikke al software opdateres fra centralt hold og derfor udgør en risiko.

Statsrevisorerne bemærkede endvidere, at der er flere eksempler på it-sikkerhedshændelser på universiteterne på grund af ukendt it-udstyr. Statsrevisorerne noterede sig, at Uddannelses- og Forskningsministeriet ville bede universiteterne om at identificere og rette op på kritiske it-sikkerhedsbrister.

Uddannelses- og forskningsministeren anerkender, at ukendt udstyr og ukendt software og applikationer udgør risikofaktorer i forhold til it-sikkerhed. Ministeren oplyser derudover, at det er et grundvilkår for universiteterne, at forskere og studerende fx kan anvende eget it-udstyr. I forskningsmiljøerne gælder endvidere, at en del af forskerne er ansat flere steder, hvilket ofte vil betyde, at it- og forskningsudstyr skal anvendes på tværs af arbejdspladser. Ministeren oplyser videre, at da meget forskningsudstyr i vid udstrækning også er it-udstyr og/eller egenudviklet/videreudviklet software forudsætter forskning ofte, at forskeren fx vil skulle have administratorrettigheder for at kunne løse sine forskningsopgaver. Ministeren oplyser, at grundvilkårene om, at forskerne i nogle tilfælde har brug for at anvende eget it-udstyr og have lokaladministratorrettigheder medfører en række sårbarheder, som universiteterne naturligvis skal håndtere og imødegå med passende tiltag, fx med udgangspunkt i ISO 27001-standarden. Det er universitetsledelsens opgave at vælge et passende sikkerhedsniveau til beskyttelse af de forskellige typer forskningsdata, der er afstemt med trusselsbillede og risikoprofil.

10. I forbindelse med beretningen oplyste Uddannelses- og Forskningsministeriet, at ministeriet ville kontakte universiteterne og understrege ledelsernes ansvar for området og samtidig bede universiteterne om at identificere og rette op på eventuelle kritiske it-sikkerhedsbrister, hvilket Statsrevisorerne noterede sig i deres bemærkning til beretningen.

11. Rigsrevisionen vil følge resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.

Lone Strøm