FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Januar 2019
– 8/2018

Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger

Universiteternes beskyttelse af forskningsdata

8/2018

Beretning om

universiteternes beskyttelse af forskningsdata

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 2019

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.

Uddannelses- og forskningsministeren 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 maj 2019.

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 2018, som afgives i februar 2020.

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan købes ved henvendelse til:
Rosendahls Lager og Logistik
Vandtårnsvej 83A
2860 Søborg

Tlf.: 4322 7300
distribution@rosendahls.dk
www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-595-4
ISBN pdf 978-87-7434-596-1

Statsrevisorernes bemærkning

Beretning om universiteternes beskyttelse af forskningsdata

Uddannelses- og Forskningsministeriet har det overordnede ansvar for forskningen på de 8 danske universiteter og bevilgede i 2018 knap 9 mia. kr. til forskning. Hvert af universiteterne har ansvaret for, at der på deres universitet er en høj it-sikkerhed, der kan beskytte forskningsdata.

Universiteterne har forskningsdata af stor værdi og er derfor et mål for cyberangreb eller cyberspionage. Inden for de seneste år har der været flere eksempler på cyberangreb. Center for Cybersikkerhed vurderer, at det er sandsynligt, at fremmede stater udfører cyberspionage mod danske offentlige forskningsinstitutioner. Samlet set vurderer centret, at truslen fra cyberspionage mod danske offentlige forskningsinstitutioner er høj.

Undersøgelsen omhandler Københavns Universitets, Aalborg Universitets, Aarhus Universitets, Danmarks Tekniske Universitets og Syddansk Universitets tiltag og initiativer for at beskytte forskningsdata.

Statsrevisorerne finder det utilfredsstillende, at de 5 største universiteter i Danmark ikke beskytter forskningsdata i tilstrækkelig grad, fx mod ukendt it-udstyr.

Statsrevisorerne bemærker:

- 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.
- At der er flere eksempler på it-sikkerhedshændelser på universiteterne på grund af ukendt it-udstyr.

Statsrevisorerne

18. januar 2019

Henrik Thorup
Klaus Frandsen
Henrik Sass Larsen
Villum Christensen
Frank Aaen
Britt Bager

- 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. Undersøgelsen indikerer, at opgaven med at beskytte forskningsdata heller ikke løses tilfredsstillende på centralt og decentralt niveau på de øvrige universiteter. Dette skaber også risici i forhold til efterlevelse af persondatalovgivningen.

Statsrevisorerne noterer sig, at Uddannelses- og Forskningsministeriet vil bede universiteterne om at identificere og rette op på kritiske it-sikkerhedsbrister.

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.

Rigsrevisionen har revideret regnskaberne efter § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen vedrører finanslovens § 19. Uddannelses- og Forskningsministeriet.

I undersøgelsesperioden har der været følgende ministre:

Søren Pind: november 2016 - maj 2018
Tommy Ahlers: maj 2018 -

Beretningen har i udkast været forelagt Uddannelses- og Forskningsministeriet og Københavns Universitet, hvis bemærkninger er afspejlet i beretningen. Derudover har de dele af beretningen, der omhandler Aarhus Universitet, Aalborg Universitet, Syddansk Universitet og Danmarks Tekniske Universitet, været forelagt disse universiteter, hvis bemærkninger ligeledes er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om beskyttelse af forskningsdata på Uddannelses- og Forskningsministeriets område. Uddannelses- og Forskningsministeriet har det overordnede ansvar for forskningen på de 8 danske universiteter og bevilgede i 2018 knap 9 mia. kr. til forskning. Hvert af universiteterne har ansvaret for, at der på deres universitet er en høj it-sikkerhed, der kan beskytte forskningsdata. Rigsrevisionen har selv taget initiativ til undersøgelsen i februar 2018 og bygger på it-revision, som Rigsrevisionen har udført i 2018.

2. Universiteterne har forskningsdata af stor værdi, der er et oplagt mål for cyberangreb eller cyberspionage. Inden for de senere år har der været flere eksempler på cyberangreb på de danske universiteter. Bl.a. kom det i foråret 2018 frem, at 3 danske universiteter var blevet hacket i perioden 2014-2016 som del af et større verdensomspændende cyberangreb fra en statslig aktør. Center for Cybersikkerhed har udarbejdet trusselsvurderinger i december 2016 og i marts 2018, hvor centret vurderer, at trusselsniveauet mod de danske universiteter er højt. Universiteter og offentlige forskningsmiljøer har tradition for stor åbenhed, hvilket også gør forskningsdata sårbare over for cyberangreb. Ifølge Center for Cybersikkerhed er det fx forskningsdata vedrørende økonomi, kemi, fysik, geologi, miljø og transport, der kan have hackernes interesse. Forskningen finansieres som nævnt dels af den danske stat, dels af EU og private samarbejdspartnere (knap 8 mia. kr. i 2018). Derfor kan det have økonomiske konsekvenser, hvis forskningsdata kopieres eller forsvinder. Desuden kan det føre til, at tilliden til de berørte universiteter falder, hvilket er alvorligt, da universiteterne er afhængige af at kunne tiltrække forskere og private forskningsmidler.

3. På grund af det høje trusselsniveau er det centralt, at universiteterne har en høj it-sikkerhed, der beskytter forskningsdata.

Formålet med undersøgelsen er således at vurdere, om universiteterne beskytter forskningsdata i tilstrækkelig grad.

Først har vi på de 5 største danske universiteter kortlagt universiteternes risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Dernæst har vi på det største universitet, KU, gået mere i dybden for at undersøge, hvordan universitetets centrale it-afdeling og 3 udvalgte institutter arbejder med it-sikkerheden i forhold til beskyttelse af forskningsdata.

Forkortelser
I beretningen anvendes følgende forkortelser om universiteterne:

København Universitet: KU
Aalborg Universitet: AAU
Aarhus Universitet: AU
Danmarks Tekniske Universitet: DTU
Syddansk Universitet: SDU

Center for Cybersikkerhed
Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Centret skal hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb fra fremmede stater.

Konklusion

Rigsrevisionen vurderer, at de 5 største universiteter ikke beskytter forskningsdata i tilstrækkeligt grad mod ukendt it-udstyr. Konsekvensen kan være, at fremmede aktører relativt let får uautoriseret adgang til forskningsdata på universiteterne. Dette finder Rigsrevisionen ikke tilfredsstillende.

It-udstyr
It-udstyr anvendes i undersøgelsen som samlet betegnelse for hardware, hvorpå der er installeret software.

Uddannelses- og Forskningsministeriet har oplyst, at ministeriet er enig i, at det er centralt, at universiteterne har en høj it-sikkerhed, der beskytter forskningsdata. Ministeriet deler Rigsrevisionens opfattelse af, at det er et område, hvor der trods fokus er potentiale og behov for forbedring.

Ukendt it-udstyr
Ukendt it-udstyr er udstyr, der ikke er kendt af it-afdelingen, fx hvis forskere medbringer eget it-udstyr uden at orientere it-afdelingen herom.

Undersøgelsen viser, at de 5 største universiteter alle har centralt fastsatte retningslinjer vedrørende forskernes anvendelse af software og hardware, men at universiteterne fra centralt hold ikke sikrer, at forskningsdata beskyttes tilfredsstillende. Det skyldes særligt, at der på nogle af universiteterne gives adgang til, at forskerne medbringer eget it-udstyr, og at alle universiteterne tillader forskere rettigheder som lokaladministratorer, hvilket betyder, at de selv kan installere software. Derudover har alle 5 universiteter kendskab til, at der har været ukendt hardware på deres netværk.

Da der er indikationer på, at universiteternes centrale beskyttelse af forskningsdata mod ukendt it-udstyr generelt ikke er høj, har Rigsrevisionen - med KU som eksempel - undersøgt, hvordan et universitet konkret beskytter forskningsdata, både på det centrale niveau og på 3 udvalgte institutter: Biomedicinsk Institut, Institut for Nordiske Studier og Sprogvidenskab og Niels Bohr Institutet.

ISO 27001
Den internationale informationssikkerhedsstandard, som de statslige institutioner har skullet følge fra januar 2014 og have færdigimplementeret primo 2016. Selvejende offentlige institutioner er ikke pålagt at følge ISO 27001, men de 5 største universiteter har alle valgt at følge sikkerhedsstandarden.

Undersøgelsen viser, at KU's beskyttelse af forskningsdata er utilstrækkelig. KU har valgt at følge ISO 27001, men har ikke udarbejdet en trusselsvurdering eller en risikovurdering, som ISO 27001 ellers foreskriver. Derudover har ledelsen kun fastsat utilstrækkelige overordnede rammer for anvendelse og styring af it-udstyr på universitetet. Hertil kommer, at KU's ledelse har fastsat 2 politikker, der i praksis overlader ansvaret for it-sikkerheden og beskyttelsen af forskningsdata til de enkelte forskere, der for at kunne løse opgaven skal have indsigt i en række af KU's it-sikkerhedsmæssige forhold, som ikke er beskrevet i de udmeldte overordnede rammer. Dette har i væsentlig grad begrænset muligheden for en høj it-sikkerhed.

Gennemgangen af it-sikkerheden på de 3 institutter viser, at opgaven heller ikke i alle tilfælde løses decentralt. Niels Bohr Institutet har selv etableret en bedre it-sikkerhed, der kan bruges som inspiration, om end der også her er forbedringspunkter. De 2 øvrige institutter har intet gjort og har den opfattelse, at opgaven med it-sikkerhed løses centralt.

Ledelsen på KU
Ledelsen på KU omfatter den øverste daglige ledelse på KU, herunder rektor, prorektor og universitetsdirektør.

Da KU's ledelse forventer, at forskerne selv er ansvarlige for at opbevare forskningsdata, har Rigsrevisionen undersøgt, om forskerne kender og følger de regler, der er, for at forskningsdata beskyttes bedst muligt. Undersøgelsen viser, at kun én ud af 26 adspurgte forskere kendte KU's retningslinjer for, hvordan data skal beskyttes. Undersøgelsen viser eksempler på, at forskerne opbevarer data på andre og mindre sikre løsninger end dem, der tilbydes af KU.

Rigsrevisionen konstaterer, at KU's ledelse er gjort opmærksom på flere af disse forhold, uden at det dog endnu har resulteret i konkrete handlinger for at sikre en tilstrækkelig it-sikkerhed.

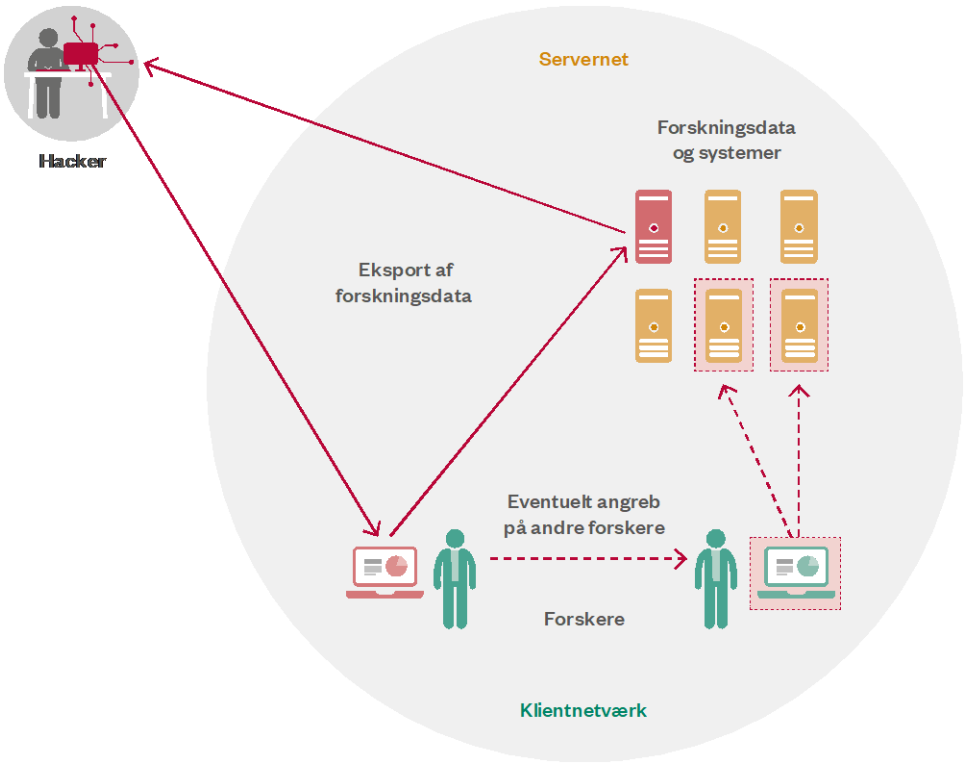
Uddannelses- og Forskningsministeriet har oplyst, at ministeriet vil bede universiteterne om bl.a. at identificere og rette op på eventuelle kritiske it-sikkerhedsbrister og derudover samarbejde med universiteterne om en plan for at etablere den nødvendige it-sikkerhedsorganisation og -kultur på universiteterne. Ministeriet vil desuden igangsætte en lignende proces på de øvrige videregående uddannelser.

1.2. Baggrund

Hackertruslen mod de danske universiteter

4. Center for Cybersikkerhed har i 2016 og 2018 udgivet trusselvurderinger, hvoraf det fremgår, at det er sandsynligt, at fremmede stater udfører cyberspionage mod danske offentlige forskningsinstitutioner. Fremmede stater har vilje, evner og resurser til at udføre særligt avancerede cyberangreb. Eksempler fra både Danmark og udlandet viser, at forskningsmiljøer er attraktive mål. Center for Cybersikkerhed vurderer, at fremmede magter relativt nemt kan skaffe sig adgang til fortrolig dansk forskning, fordi universiteter og offentlige forskningsmiljøer har tradition for stor åbenhed. Det gør miljøerne meget sårbare over for cyberangreb. Samlet set vurderer centret, at truslen fra cyberspionage mod danske offentlige forskningsinstitutioner er høj. Figur 1 viser et eksempel på, hvordan et cyberangreb kan foregå.

Figur 1
Eksempel på et hackerangreb



Kilde: Rigsrevisionen.

Eksport af forskningsdata
Kaldes også eksfiltrering af data, dvs. kopiere eller flytte data, som for hackeren er vigtige at få permanent adgang til og eventuelt eksportere til egen pc.

Det fremgår af figur 1, at et cyberangreb fx kan ske ved, at en hacker udnytter et stykke sårbart software på en medarbejders pc til at få adgang til medarbejderens rettigheder på pc'en. Hvis medarbejderen har lokaladministratorrettigheder, kan hackeren få adgang til at anvende medarbejderens rettigheder på pc'en til at kompromittere andre systemer og data på det netværk, som pc'en er tilkoblet. Derudover kan hackeren hacke sig videre til andre forskeres pc'er.

5. I 2018 kom det frem, at en udenlandsk statslig aktør havde stået bag et cyberangreb mod flere universiteter og organisationer verden over, herunder flere danske universiteter, jf. boks 1.

Boks 1

Cyberangreb mod danske universiteter i perioden 2014-2016

Center for Cybersikkerhed finder det meget sandsynligt, at flere e-mailkonti tilhørende ansatte på universiteter i Danmark har været hacket af en statslig aktør. Kompromitteringen var et resultat af et stort antal fremsendte spearfishingmails, der er blevet fremsendt i perioden 2014-2016. I Danmark har angrebet været målrettet medarbejdere på danske universiteter med specialer inden for bl.a. økonomi, fysik, geologi, miljø og transport. Center for Cybersikkerhed vurderer, at det er sandsynligt, at aktøren bag angrebet har været særligt interesseret i disse fagområder, men det kan ikke udelukkes, at aktøren har forsøgt at misbruge adgange til medarbejdere på disse områder til at indsamle informationer på andre områder end de nævnte. Ifølge udtalelser fra amerikanske myndigheder har cyberangrebene tilknytning til Iran.

Kilde: Center for Cybersikkerhed, Trusselsvurdering: Danske universiteter er mål for cyberangreb, marts 2018.

Spearfishingmails
Spearfishingsmails er e-mails rettet mod bestemte personer i en virksomhed. Målet er fx at franarre modtageren sine loginoplysninger eller få modtageren til at klikke på et link i e-mailen eller åbne en vedhæftet fil. Når modtageren klikker på linket eller åbner filen, vil personens computer blive inficeret med en malware, fx virus.

Beskyttelse af forskningsdata

6. Der er flere grunde til, at det er vigtigt, at universiteterne beskytter deres forskningsdata. Forskningsdata kan repræsentere en stor økonomisk værdi, og tabte forskningsdata kan i sidste ende også betyde tabte indtægter for den danske stat. Derudover er universiteterne bundet af gældende lovgivning og krav fra eksterne samarbejdspartnere. Universiteterne skal fx i håndteringen af følsomme persondata leve op til EU's persondataforordning. Derudover stiller eksterne samarbejdspartnere krav om sikker opbevaring af data. KU har oplyst, at det fx gælder forskningsprojekter, der finansieres gennem EU's Horizon 2020-program. Desuden stiller regionerne krav om sikker opbevaring af persondata, når der indgås aftaler om levering af sundhedsdata til forskning. KU har oplyst, at der i nogle tilfælde indgås kontrakter med ubegrænset økonomisk erstatningspligt over for samarbejdspartnere, hvis data ikke beskyttes tilstrækkeligt. Endelig har KU oplyst, at universitetet er afhængig af at kunne tiltrække samarbejdspartnere til finansiering og forskning, og at det derfor er vigtigt, at universitetet har et godt image i forhold til beskyttelse af data.

Universiteterne har oplyst, at de står over for et særligt dilemma, når det gælder it-sikkerhed. Normalt styres it-sikkerhed ved at fastsætte politikker, retningslinjer og procedurer, der understøttes af teknologiske løsninger, og ved, at der foretages opfølgning for at sikre, at det ønskede niveau af it-sikkerhed er opnået. Samtidig er det et vilkår for universiteterne at skulle sikre forskernes forskningsfrihed, hvilket umiddelbart kan være svært at forene med ønsket om en høj it-sikkerhed, som kun kan opnås ved en forholdsvis stram styring. Det er fx vigtigt for forskere at have metodefrihed i forskningen, hvilket bl.a. betyder, at forskerne skal kunne anvende det it-udstyr, de finder bedst egnet. Flere universiteter tilbyder derfor forskerne, at de selv kan anskaffe og tilslutte it-udstyr på universitetets netværk. It-udstyr, der ikke er kendt af it-afdelingerne, kan dog udgøre en sikkerhedsmæssig risiko, hvis det ikke sikkerhedsopdateres. AAU har oplyst, at universitetet har brug for at kunne tilbyde sine forskere favorable vilkår for metodefrihed til forskning, og at dette forhold i nogle tilfælde udfordrer en højere it-sikkerhed, og at det således er en balance, som universitetet skal navigere i.

Forskningsfrihed
Forskernes frihed til helt selv at vælge, hvilket udstyr og materiale og hvilke metoder de bruger i deres forskning.

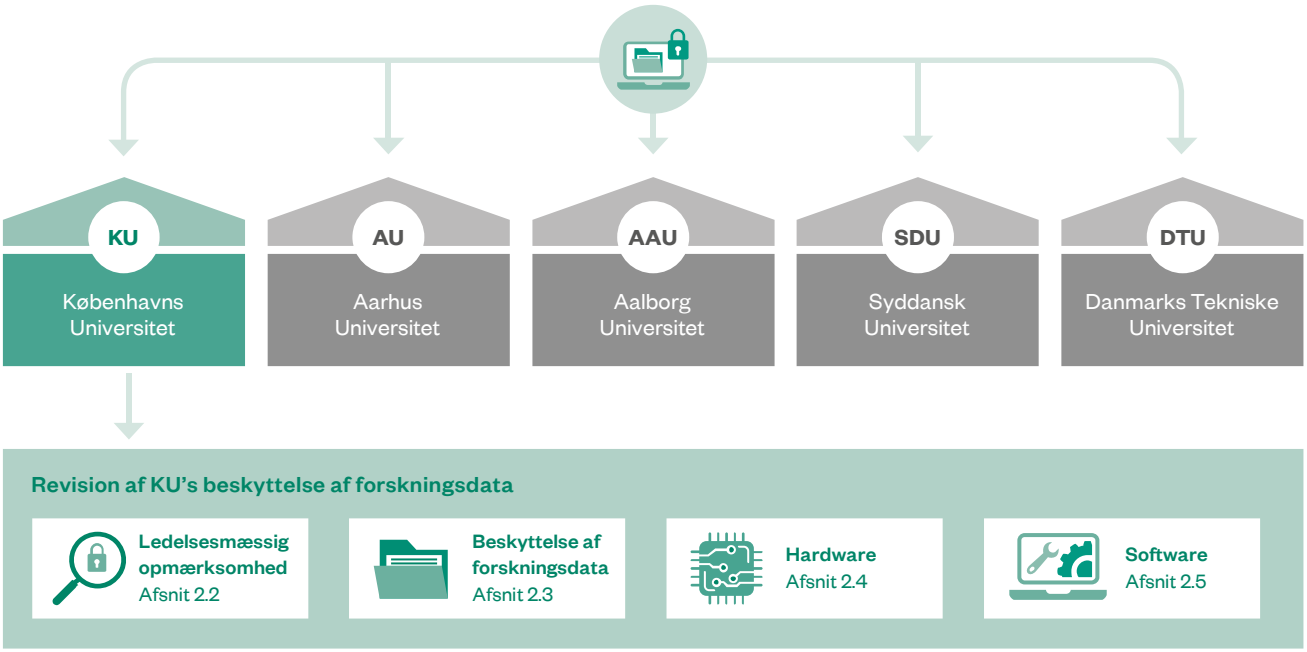
1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

KU's centrale it-afdeling
KU's fælles it-afdeling, KU-IT, der er ansvarlig for it på alle universitetets institutter på nær Niels Bohr Institutet og Kemisk Institut.

7. Undersøgelsens formål er at undersøge, om universiteterne beskytter forskningsdata i tilstrækkelig grad. Undersøgelsen er gennemført i 2 trin. Først har vi på de 5 største danske universiteter kortlagt universiteternes risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Dernæst har vi på det største universitet, KU, gået mere i dybden for at undersøge, hvordan universitetets centrale it-afdeling og 3 udvalgte institutter arbejder med it-sikkerheden i forhold til beskyttelse af forskningsdata, jf. figur 2.

Figur 2
Undersøgelsens opbygning



CIS
Det amerikanske Center for Internet Security (CIS) er en nonprofitorganisation, hvis formål er at fremme cybersikkerhed. CIS har med hjælp fra praktikere, bl.a. fra den amerikanske efterretningstjeneste NSA, udarbejdet en prioriteret liste over tiltag, der styrker cybersikkerheden – Critical Security Controls – ud fra erfaringer fra de mest almindelige angreb.

Grundlag for revisionskriterierne

8. Revisionskriterierne i undersøgelsen er baseret på ISO 27001, anbefalinger fra det amerikanske Center for Internet Security (CIS) og Center for Cybersikkerhed. Derudover er kriterierne og vurderingerne drøftet med en ekstern konsulent.

ISO 27001, som de 5 universiteter har valgt at følge, fastsætter bl.a., at ledelsen i organisationen skal sikre, at der udarbejdes ledelsesgodkendte politikker og retningslinjer for it-sikkerhed. Derudover fastsætter standarden, at ledelsen skal vurdere trusler og risici ved anvendelsen af it.

Ifølge CIS' top 20 over Critical Security Controls er styring af hardware og software nummer 1 og 2 på en prioriteret liste over 20 tiltag, som fremmer it-sikkerhed. Det betyder, at en tilstrækkelig samlet it-sikkerhed forudsætter en tilstrækkelig styring af hardware og software. Kriterierne vedrørende styring af hardware og software dækker derudover flere grundlæggende sikringstiltag, som Center for Cybersikkerhed har anbefalet danske offentlige institutioner at følge siden 2013, som bl.a. handler om at sikre, at software er opdateret, og at minimere konsekvenser af skadelig software.

Kortlægning af de 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata

9. Som grundlag for vores vurdering af universiteternes risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr har vi undersøgt, om der er 6 risikofaktorer til stede på de 5 universiteter. Vi har undersøgt, om ledelsen på universiteterne har vurderet risikoen for ukendt software eller hardware. Derudover har vi undersøgt, om universiteterne har fundet ukendt hardware på deres netværk. Dernæst har vi undersøgt, hvilke regler der gælder for anvendelse af hardware og software, herunder om forskerne kan og må medbringe og tilslutte egen hardware til universitetets netværk, og om forskerne har lokaladministratorrettigheder, dvs. selv kan installere og/eller afvikle software. Endelig har vi undersøgt, om universiteterne har været udsat for it-sikkerhedshændelser, hvor forskningsdata er blevet kompromitteret.

10. Universiteterne har anført, at kortlægningen af universiteternes risikoprofil i tabel 1 på s. 11 giver et forsimplet billede af universiteternes it-sikkerhed og beskyttelse af forskningsdata. Fx har DTU anført, at ukendt it-udstyr og utilstrækkelig opdatering af software kun udgør én mulig angrebsvinkel, og at universiteterne fx også er sårbare over for ransomewareangreb og andre typer angreb. Det udgør således ikke en tilstrækkelig beskyttelse af forskningsdata kun at sikre mod ukendt it-udstyr. Universiteterne fremhæver derudover, at de har eller planlægger at implementere tiltag ud over dem, der fremhæves i beretningen, som øger it-sikkerheden.

Rigsrevisionen er enig i, at de tiltag, der undersøges i beretningen, ikke kortlægger universiteternes samlede it-sikkerhed. Rigsrevisionen har afspejlet de eksempler på tiltag, som universiteterne har oplyst om, som de mener øger it-sikkerheden, ligesom universiteternes videre arbejde med it-sikkerhed er beskrevet.

Rigsrevisionen vurderer dog, at det ikke er muligt for universiteterne at have en tilstrækkelig it-sikkerhed, hvis ikke de har overblik over det it-udstyr, som anvendes på universiteternes netværk, opdateret software, og nedskrevne og ledelsesgodkendte vurderinger af risici ved anvendelsen af it-udstyr. Rigsrevisionen konstaterer, at bl.a. CIS og Center for Cybersikkerhed fremhæver, at styring af it-udstyr og softwareopdatering er helt centrale sikringstiltag for at have en tilstrækkelig it-sikkerhed.

It-revision af KU's beskyttelse af forskningsdata

11. Undersøgelsen viser indikationer på, at de 5 største universiteters beskyttelse af forskningsdata generelt ikke er høj. Vi har derfor gået i dybden på KU og har undersøgt, hvordan KU's centrale it-afdeling og 3 udvalgte institutter (Biomedicinsk Institut, Institut for Nordiske Studier og Sprogvidenskab og Niels Bohr Institutet) konkret beskytter forskningsdata mod ukendt it-udstyr.

Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU
12. Vi har undersøgt, om KU har haft tilstrækkelig ledelsesmæssig opmærksomhed på styring af it-udstyr. Vi har lagt til grund, at tilstrækkelig opmærksomhed indebærer, at universitetets ledelse har politikker og retningslinjer for styring af it-udstyr, og at ledelsen på KU vurderer trusler og risici ved anvendelsen af it-udstyr i forskningen.

KU's beskyttelse af forskningsdata
13. Både ISO 27001 og CIS' top 20 over Critical Security Controls fastsætter, at organisationer skal klassificere data med henblik på at kunne beskytte data i tilstrækkelig grad. Dette er særligt relevant for universiteterne, der indsamler, behandler og producerer store mængder forskningsdata. Vi har derfor undersøgt, om KU har ledelsesgodkendte politikker og retningslinjer for, hvordan data skal beskyttes. Vi har derudover undersøgt, om KU sikrer, at retningslinjer for beskyttelse af data efterleves i praksis.

KU's overblik over hardware og software
14. Vi har undersøgt, om KU har overblik over hardware, der kan tilgå universitetets netværk med forskningsdata. Vi har lagt til grund, at et overblik over hardware, der kan tilgå universitetets netværk, forudsætter, at KU har en komplet og opdateret oversigt over den hardware, som har adgang til netværk med forskningsdata, og at KU sikrer, at ukendt it-udstyr på netværket opdages. Derudover har vi undersøgt, om KU har dokumentation for, at software på forskernes pc'er og på serverne er opdateret.

Metode

15. Undersøgelsen er baseret på resultater fra Rigsrevisionens it-revision, som er udført i perioden marts-oktober 2018.

Kortlægning af de 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata
16. Vores kortlægning af, KU's, AU's, AAU's, SDU's og DTU's risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr er baseret på møder og brevveksling med universiteterne samt indhentet skriftlig dokumentation. Kortlægningen er ikke baseret på en it-revision i dybden og er således fx heller ikke baseret på møder på decentralt niveau på universiteterne.

It-revision af KU's beskyttelse af forskningsdata
17. Undersøgelsen af KU's beskyttelse af forskningsdata er baseret på møder med den centrale it-afdeling på KU og med de 3 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). Niels Bohr Institutet har som det eneste institut sin egen it-afdeling. Baggrunden for udvælgelse af institutterne fremgår af bilag 1.

På hvert revisionsbesøg har vi anvendt en spørgeguide baseret på undersøgelsens revisionskriterier. I forlængelse heraf har vi indsamlet skriftlig dokumentation for KU's centrale it-afdelings og institutternes besvarelse af spørgsmålene i spørgeguiden. Dokumentationen omfatter bl.a. skriftlige politikker og retningslinjer, dataudtræk og screendumps.

Derudover har vi gennemført en stikprøve blandt forskere på de 3 institutter. Stikprøven havde til formål at undersøge forskernes håndtering af it-udstyr og beskyttelse af forskningsdata. Vi har udvalgt tilfældigt it-udstyr (pc'er og servere) på hvert institut. Vi har i den forbindelse undersøgt, om den software, der er installeret på it-udstyret, er sikkerhedsopdateret. Derudover har vi foretaget en rundspørge af, om forskerne på de 3 institutter kender til KU's retningslinjer for beskyttelse af data.

Vurdering af opfyldelse af revisionskriterier

18. I den første del af undersøgelsen har vi i tabel 1 på s. 11 vurderet de 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata. Vi har baseret denne vurdering på, om en 6 risikofaktorer øger (rød), delvist øger (gul) eller ikke øger (grøn) risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad.

I undersøgelsens anden del har vi inden for 4 udvalgte områder vurderet, om KU opfylder (grøn), delvist opfylder eller har kompenserende tiltag (gul) eller ikke opfylder (rød) underliggende revisionskriterier. Vi har vurderet, om KU opfylder revisionskriterierne på baggrund af skiftlige revisionsbeviser. I undersøgelsen har vi lagt til grund, at KU skal opfylde alle revionskriterierne, for at beskyttelsen af forskningsdata er tilfredsstillende.

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

Afgrænsning

20. De tiltag til it-sikkerhed, som indgår i denne undersøgelse, er væsentlige og effektive, men ikke udtømmende i forhold til god it-sikkerhed. Undersøgelsen er således ikke en udtømmende gennemgang af de mange sikringstiltag, der er mulighed for, og som bl.a. fremgår af ISO 27001, herunder fx styring af brugernavne/passwords.

Vi har alene undersøgt KU's overordnede beskyttelse af forskningsdata. Vi har fx ikke undersøgt, om KU i konkrete eksempler i behandlingen af personoplysninger følger persondataloven eller den nye forordning, som trådte i kraft den 25. maj 2018.

Vi har undersøgt de netværk, hvor der indgår systemer og data, som anvendes i forskningen, og ikke netværkene for de studerende eller de administrative netværk. Undersøgelsen er derudover afgrænset til universiteternes kablede netværk, og universiteternes trådløse netværk indgår således ikke i undersøgelsen. Det har vi valgt ud fra en betragtning om, at institutioner typisk er opmærksomme på at sikre det trådløse netværk, mens det kablede netværk ofte primært beskyttes af fysisk adgang til netværket. Da universiteterne er kendetegnet ved at være åbne steder, hvor uvedkommende relativt let kan få fysisk adgang til det kablede netværk, finder vi det særligt relevant at undersøge, hvordan universiteterne sikrer det kablede netværk.

21. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. Bilag 2 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Beskyttelse af forskningsdata

2.1. De 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata

22. Vi har undersøgt de 5 største universiteters (KU, AU, AAU, SDU og DTU) risikoprofil i forhold til at sikre, at forskningsdata beskyttes i tilstrækkelig grad.

Vi har i den forbindelse foretaget en kortlægning af, om ledelsen på universiteterne har forholdt sig til risikoen for ukendt software eller hardware. Derudover har vi undersøgt, om universiteterne har fundet ukendt hardware på deres netværk, og hvilke centralt fastsatte retningslinjer der gælder for forskernes anvendelse af software og hardware, herunder om forskerne må medbringe og tilslutte egen hardware til universitetets netværk, og om forskerne selv kan installere software, fx fordi de har lokaladministratorrettigheder. Endelig har vi undersøgt, om universiteterne har været udsat for sikkerhedshændelser, hvor forskningsdata er blevet kompromitteret. Kortlægningen af universiteternes risikoprofil er baseret på oplysninger fra universiteterne. Kortlægningen af KU's risikoprofil er yderligere baseret på den gennemførte revision på KU.

Kortlægningen af universiteternes risikoprofil fremgår af tabel 1. I tabellen angives Rigsrevisionens vurdering af, om 6 risikofaktorer øger risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad, på hvert af de 5 universiteter. Vurderingen er angivet med grøn (øger ikke risikoen), gul (øger delvist risikoen) eller rød (øger risikoen).

Tabel 1
Overblik over universiteternes risikoprofil

	KU[1)]	AU[2)]	AAU[2)]	SDU[2)]	DTU[2)]
Forholder universitetets ledelse sig til risikoen ved ukendt it-udstyr?	Nej 🔴	Ja 🟢	Nej 🔴	Ja 🟢	Nej 🔴
Tillader universitetet "bring your own device"?	Ja 🔴	Ja 🔴	Delvist 🟡	Nej 🟢	Nej 🟢
Er der fundet ukendt hardware på universitetets netværk?	Ja 🔴	Ja 🔴	Ja 🔴	Ja 🔴	Ja 🔴
Blokerer universitetet sine netværk mod ukendt hardware?	Delvist 🟡	Nej 🔴	Nej 🔴	Delvist 🟡	Delvist 🟡
Tillader universitetet forskerne lokaladministrator-rettigheder?	Ja 🔴	Ja 🔴	Delvist 🟡	Delvist 🟡	Ja 🔴
Har der været hændelser på universitetet på baggrund af ukendt it-udstyr?	Ja 🔴	Nej 🟢	Nej 🟢	Ja 🔴	Nej 🟢

[1)] Kortlægningen af KU's risikoprofil er baseret på den gennemførte revision af KU.
[2)] Kortlægningen af AU's, AAU's, SDU's og DTU's risikoprofil mv. er baseret på oplysninger fra universiteterne og skriftlig dokumentation herfor.

Note: Rigsrevisionen har vurderet, om 6 risikofaktorer øger (rød), delvist øger (gul) eller ikke øger (grøn) risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad mod ukendt it-udstyr.

Kilde: Rigsrevisionen baseret på oplysninger fra universiteterne og vores revision af KU.

Det fremgår af tabel 1, at ikke alle universiteters ledelser har forholdt sig til risikoen for ukendt it-udstyr. Det fremgår også, at alle universiteterne har fundet ukendt hardware på deres netværk. Endvidere fremgår det, at flere universiteter tillader "bring your own device", og at alle universiteterne i forskelligt omfang tillader forskerne lokaladministratorrettigheder. Endelig fremgår det af tabellen, at der har været eksempler på sikkerhedshændelser på grund af ukendt it-udstyr på flere af universiteterne.

Lokaladministrator-rettigheder
Tildelingen af rettighed som lokaladministrator giver medarbejderen det højeste niveau af adgang og kontrol over den pc, som forskeren arbejder ved.

Forholder universiteternes ledelser sig til risikoen ved ukendt it-udstyr?

23. Ledelsen på KU og AAU har ikke forholdt sig til risikoen for ukendt it-udstyr på universitetets netværk. På AU og SDU har ledelsen forholdt sig til risikoen ved, at der findes ukendt it-udstyr på netværket, herunder hvad det betyder for beskyttelse af forskningsdata. På AU har ledelsen vurderet, at universitetets it-sikkerhed skal højnes, bl.a. på grund af risiko for ukendt it-udstyr. SDU har vurderet, at ukendt it-udstyr udgør en sikkerhedsmæssig risiko, og tillader på baggrund heraf ikke forskerne at medbringe eget it-udstyr. DTU har oplyst, at ukendt it-udstyr indgår på linje med andre risici i den samlede risikovurdering, og at netværket på nogle dele af universitetet er indrettet således, at ukendt it-udstyr ikke kan tilkobles. DTU har dog ikke leveret dokumentation for, at ukendt it-udstyr er behandlet eksplicit i universitetets risikovurdering. Derudover har DTU oplyst, at forskernes it-udstyr vil være kendt af den lokale ledelse på institutterne og således ikke er ukendt. DTU har dog ikke fremlagt dokumentation herfor.

Tillader universiteterne "bring your own device"?

24. KU og AU har begge en "bring your own device"-politik, dvs. at universiteterne tillader, at forskerne kan medbringe eget it-udstyr og tilslutte det på universiteternes netværk. I praksis betyder det, at hvis universiteterne ikke registrerer eller på anden måde opnår viden om forskernes it-udstyr, kan der være ukendt it-udstyr på de 2 universiteters netværk. AU har oplyst, at universitetet dog ikke tillader, at forskerne tilkobler egne servere på netværket, og at AU i sin informationssikkerhedspolitik har fastsat grænser for, hvad forskerne må anvende privat it-udstyr til. AAU har oplyst, at universitetet har en politik om, at kun autoriserede brugere og autoriseret it-udstyr må have adgang til universitetets netværk. AAU har dog oplyst, at politikken ikke bliver håndhævet i praksis, og at universitetet ikke kontrollerer for ukendt it-udstyr. DTU har oplyst, at universitetet ikke har en "bring your own device"-politik, men heller ikke har en eksplicit politik, der forbyder ukendt it-udstyr. SDU's ledelse har en eksplicit politik om, at forskerne ikke må tilkoble eget it-udstyr til universitetets netværk.

Er der fundet ukendt hardware på universiteternes netværk, og blokerer universiteterne deres netværk mod ukendt hardware?

25. Alle 5 universiteter har oplyst, at der er fundet ukendt hardware på universiteternes netværk. Ukendt hardware kan fx udgøre en risiko, hvis den software, der er installeret på hardwaren, ikke sikkerhedsopdateres.

Blokering af ukendt udstyr
Til dette formål kan universiteterne fx anvende teknologien 802.1x, som giver mulighed for, at ukendt hardware skal godkendes af it-afdelingen, inden det kan tilsluttes netværket.

En måde at sikre mod ukendt hardware er at blokere for, at man kan tilslutte ukendt hardware på netværket. AU og AAU har ikke implementeret sådanne teknologier, men har oplyst, at de vil implementere sådanne teknologier. KU og SDU har oplyst, at de har implementeret en teknologi, der kan dette på dele af universiteterne. KU har implementeret teknologien på 3 fakulteter (teologi, jura og humaniora). SDU har oplyst, at teknologien skal implementeres på hele universitetet, og at teknologien i 1. kvartal 2018 er implementeret på 30 % af universitetet. DTU anvender en anden løsning til blokering af ukendt it-udstyr og har implementeret denne på 5 institutter (vindenergi, veterinær, aqua, energi og fødevarer) og Center for Nukleare Teknologier.

Penetrationstest
En penetrationstest er en aftalt test gennemført af en it-sikkerhedskonsulent med det formål at undersøge, om det er muligt for it-sikkerhedskonsulenten at trænge ind hos en kunde.

SDU har derudover oplyst, at universitetet på baggrund af netværkstrafik reaktivt kan identificere it-udstyr på netværket, herunder at universitetet har mulighed for at blokere udstyr, som har mistænkelig adfærd. Derudover har universitetet øget sikkerheden på netværket ved bl.a. at segmentere netværket, gennemføre interne scanninger efter ukendt it-udstyr og løbende gennemføre forskellige typer penetrationstests.

DTU har oplyst, at det på hele universitetet kun er muligt at koble it-udstyr på netværket, hvis man anvender et brugerlogin, og at universitetet bl.a. på den baggrund ikke anser ukendt it-udstyr for at have betydning for beskyttelsen af forskningsdata.

Keylogger
Teknologi, der fysisk eller digitalt kan bruges til at aflure tastaturtryk, fx med henblik på at aflure loginoplysninger.

Rigsrevisionen bemærker, at alle universiteterne benytter sig af brugernavne og passwords. Det er imidlertid relativt nemt for uvedkommende at tilegne sig en medarbejders brugerloginoplysninger. Fx har ét af de andre universiteter oplyst, at der har været en sikkerhedshændelse på universitetet, hvor uvedkommende har anvendt en såkaldt keylogger til at forsøge at aflure forskeres brugeroplysninger.

Tillader universiteterne forskerne lokaladministratorrettigheder?

26. Alle 5 universiteter tillader i et vist omfang, at forskerne selv kan installere software. På KU og AU har alle forskere lokaladministratorrettigheder. På AAU, SDU og DTU kan forskerne søge om at få lokaladministratorrettigheder på udleveret it-udstyr. AAU har oplyst, at forskerne undtagelsesvist kan få tildelt lokaladministratorrettigheder på deres pc'er. SDU har oplyst, at forskerne på nogle fakulteter kan søge om at få tildelt lokaladministratorrettigheder, og at tildelingen skal ledelsesgodkendes. DTU har oplyst, at de fleste forskere på universitetet lejlighedsvist har lokaladministratorrettigheder på deres pc'er. Alle universiteterne har oplyst, at der er software, som styres fra centralt hold, fx styresystemer. Da der på alle universiteterne er forskere, der har lokaladministratorrettigheder, er det dog ikke al software, som styres fra centralt hold. Det betyder, at der på alle universiteterne findes software, som forskerne således selv skal sikkerhedsopdatere, og hvor der er risiko for efterslæb på sikkerhedsopdatering af software.

Flere universiteter har anført, at det i flere tilfælde er nødvendigt for forskerne at have rettigheder som lokaladministrator for at kunne forske, og at der dermed er et legitimt behov for lokaladministratorrettigheder. Fx har AU oplyst, at forskernes lokaladministratorrettigheder er et bevidst valg fra universitetets side om at acceptere de risici, som lokaladministratorrettigheder (og "bring your own device"-politikken) indebærer. Rigsrevisionen bemærker, at hver enkelt forsker, der har lokaladministratorrettigheder, udgør en risiko for både sin egen de øvrige forskeres it-sikkerhed på netværket. Rigsrevisionen finder derfor, at anvendelsen af lokaladministratorrettigheder bør være begrænset, og at det fx ikke er tilfredsstillende, at alle forskere på et universitet, fakultet og/eller institut automatisk tildeles rettigheder som lokaladministrator. Rigsrevisionen finder i øvrigt, at lokaladministratorrettigheder bør tildeles på baggrund af et konkret behov og begrænses til et kort tidsinterval, så forskernes daglige arbejde foregår uden lokaladministratorrettigheder. Rigsrevisionen konstaterer, at flere universiteter allerede arbejder med sådanne løsninger på dele af universiteterne. Fx har SDU på nogle fakulteter implementeret en proces, hvor forskerne ansøger om at få lokaladministratorrettigheder. Derudover har DTU oplyst, at der på universitetet netop er udviklet en mulighed for, at forskere kan få lokaladministratorrettigheder i en kort periode, fx i forbindelse med installation af et standardprogram.

AU har oplyst, at de anvender en teknologi på udleveret it-udstyr, der begrænser, hvilken software forskerne kan installere og/eller anvende. Rigsrevisionen bemærker, at forskeren stadig skal sikkerhedsopdatere software, der er installeret af forskeren selv, hvilket indebærer en risiko for et efterslæb på sikkerhedsopdateringer. Derudover er denne teknologi ikke implementeret på it-udstyr, som forskerne selv medbringer og anvender, og dette udstyr udgør således fortsat en sikkerhedsmæssig risiko.

Har der været sikkerhedshændelser på universiteterne på baggrund af ukendt it-udstyr?

27. KU og SDU har oplyst, at der har været sikkerhedshændelser, der kan henføres til brug af ukendt it-udstyr. KU har oplyst, at der har været en sikkerhedshændelse, hvor et fællesdrev med 17.000 forskningsdokumenter blev krypteret, fordi en forskers it-udstyr ikke var sikkerhedsopdateret. SDU har oplyst, at der har været et tilfælde, hvor data er gået tabt, fordi forskerne har anvendt andet it-udstyr og opbevaringsløsninger til forskningsdata end det, universitetet stiller til rådighed. AAU, AU og DTU har oplyst, at der ikke har været sikkerhedshændelser på universiteterne på baggrund af ukendt it-udstyr. Det fremgår dog af AU's eget forslag til strategi for it-sikkerhed for perioden 2018-2022, at AU er sårbar over for fx datalæk og spionage på grund af ukendt it-udstyr og ikke i alle tilfælde er i stand til at opdage sådanne sikkerhedshændelser. Rigsrevisionen vurderer, at hvis universiteterne kun i begrænset omfang kontrollerer for ukendt it-udstyr, har det som konsekvens, at det vil være vanskeligt for universiteterne at opdage eventuelle sikkerhedshændelser med baggrund i ukendt it-udstyr.

Universiteternes videre arbejde med it-sikkerhed

28. Alle universiteterne har oplyst, at de har stor opmærksomhed på it-sikkerhed, og at de arbejder på at implementere forskellige tiltag for at højne it-sikkerheden.

KU har oplyst, at universitetet har taget beretningens konklusioner til efterretning, og at universitetet allerede på tidspunktet for revisionen var i gang med at gennemføre tiltag for at forbedre it-sikkerheden. Universitetet har på baggrund af beretningen udvidet tiltagene til forbedring af it-sikkerheden med yderligere fokus, bl.a. ved at igangsætte et program, der samler tiltagene og forankrer dem i et direktionsstyret program. KU har videre oplyst, at det vil tage tid for universitetet at rette op på Rigsrevisionens kritikpunkter, da der i forskningsmiljøet er tradition for store frihedsgrader. KU anfører, at der således er tale om en organisatorisk udvikling, der skal ske i harmoni og respekt for den frie forsknings ånd.

AU har oplyst, at universitetets ledelse i lyset af den stigende trussel fra cyberkriminalitet har godkendt igangsættelse og finansiering af flere initiativer til at styrke it-sikkerheden, herunder tiltag, der har til formål at styrke universitetets evne til hurtigere at opdage og reagere på hændelser. Et konkret initiativ er implementering af teknologien 802.1x, som skal sikre mod ukendt it-udstyr. Teknologien skal implementeres i perioden 2019-2020. Derudover vil AU i 2020 implementere et projekt til at sikre efterlevelse af ISO 27001. AU har yderligere oplyst, at både "bring your own device"-politikken og forskernes lokaladministratorrettigheder har stor værdi for forretningen, og at universitetet på den baggrund ikke har aktuelle planer om at forbyde det.

AAU har oplyst, at universitetet ønsker målrettet at styrke it-sikkerheden på udvalgte områder og har derfor igangsat en masterplan for sikkerhed, der kommer med anbefalinger til de kommende 3-4 års indsatser på it- og informationssikkerhedsområdet. AAU har bl.a. oplyst, at universitetet vil implementere en teknisk løsning, der kan blokere for ukendt hardware. Derudover er AAU i gang med at opbygge en cloudløsning – Claaudia – til opbevaring af forskningsdata, der tages i brug fra primo 2019.

SDU har oplyst, at universitetet har stort fokus på it-sikkerhed og har implementeret en handlingsplan for it-sikkerhed. SDU har desuden oplyst, at universitetet bl.a. på baggrund af en sikkerhedshændelse med ukendt it-udstyr har iværksat en it-sikkerhedsplan, som omfatter 9 anbefalinger. Som led heri har universitetet bl.a. indført passwordaudit og sortlistet ca. 4 mia. "dårlige" passwords. Derudover har den fælles it-afdeling på universitetet fået beføjelser til at håndhæve it-sikkerhedspolitikken for alt it-udstyr.

Resultater

Undersøgelsen viser, at de 5 største universiteter (KU, AU, AAU, SDU og DTU) alle har centralt fastsatte retningslinjer vedrørende forskernes anvendelse af software og hardware i form af retningslinjer for "bring your own device" og tildeling af lokaladministratorrettigheder til forskere. Undersøgelsen viser dog, at universiteterne fra centralt hold ikke sikrer, at forskningsdata beskyttes i tilstrækkelig grad. Det skyldes særligt, at der på flere af universiteterne gives adgang til, at forskerne medbringer eget it-udstyr, og at alle universiteterne tillader forskere rettigheder som lokaladministratorer, hvilket betyder, at de selv kan installere software. Alle universiteterne har kendskab til, at der har været ukendt it-udstyr på deres netværk.

Universiteterne har oplyst om flere sikkerhedshændelser, der kan henføres til brug af ukendt it-udstyr, fx fordi forskerne ikke har sikkerhedsopdateret deres it-udstyr eller har anvendt andet it-udstyr og dataopbevaringsløsninger end dem, som universiteterne stiller til rådighed.

2.2. Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU

29. Da den centrale beskyttelse af forskningsdata på de 5 største universiteter generelt ikke er tilstrækkelig, har Rigsrevisionen med KU som eksempel undersøgt, hvordan et universitet konkret beskytter forskningsdata, både på det centrale niveau og på 3 udvalgte institutter.

30. Vi har undersøgt, om ledelsen på KU har haft tilstrækkelig ledelsesmæssig opmærksomhed på styring af it-udstyr. Vi har i den forbindelse undersøgt, om universitetets ledelse har fastsat politikker og retningslinjer for styring af it-udstyr, og om ledelsen på KU har vurderet trusler og risici mod universitetets anvendelse af it-udstyr.

31. Tabel 2 viser undersøgelsens resultater vedrørende KU's ledelsesmæssige opmærksomhed på styring af it-udstyr.

Tabel 2
Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU

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

Kilde: Rigsrevisionen.

Det fremgår af tabel 2, at KU ikke opfylder nogen af de 3 tiltag i forhold til den ledelsesmæssige opmærksomhed på styring af it-udstyr.

Ledelsesgodkendte politikker og retningslinjer for styring af it-udstyr

32. Det er KU's ledelse, der har ansvaret for it-sikkerheden på universitetet. KU har valgt at følge ISO 27001, der også understreger, at ansvaret for it-sikkerheden ligger hos ledelsen, hvilket bl.a. indebærer, at ledelsen skal sørge for, at der bliver udarbejdet en vurdering af trusler og risici ved anvendelsen af it. I den forbindelse skal ledelsen tage stilling til, om de risici, der er til stede ved it-anvendelsen på KU, skal accepteres, eller om der skal implementeres yderligere sikringsforanstaltninger.

33. KU's *politik for forskningsdata* og KU's *retningslinjer for overvågning og adgang til elektronisk post og internet* udgør rammerne for anvendelse og styring af it-udstyr på universitetet.

KU's *politik for forskningsdata* gælder for al forskning på universitetet og fastlægger rammer og minimumskrav for håndtering af forskningsdata, som forskerne er helt eller delvist ansvarlige for. Politikken skal bl.a. sikre, at forskningsdata bevares til senere brug, jf. boks 2.

Boks 2

KU's politik for forskningsdata

"Indsamling, opbevaring og arkivering
Den enkelte forsker bærer inden for lovgivningens rammer ansvaret for valget af passende og tilstrækkelig metode til indsamling af forskningsdata samt opbevaring og arkivering heraf. KU sikrer i rimeligt omfang – og så vidt det er muligt – at de nødvendige infrastrukturer til opbevaring og arkivering kan etableres. Forskningsresultater mv. skal som udgangspunkt kunne genskabes. Det påhviler den enkelte forsker at opbevare forskningsdata, som danner grundlag for den pågældendes forskning. Det er den enkelte forskers ansvar at være tilstrækkeligt uddannet og at have kvalifikationer til behandling af data inden for det enkelte forskningsområde."

Kilde: KU's politik for forskningsdata, 1. juli 2014.

Som det fremgår af boks 2, fastsætter politikken, at forskerne har ansvaret for at vælge metode til indsamling af forskningsdata, herunder fx hvilket it-udstyr, forskerne skal anvende. Derudover er forskerne selv ansvarlige for opbevaring af forskningsdata. I forlængelse af denne politik har KU valgt at have en "bring your own device"-politik, der giver forskerne mulighed for at tilslutte eget it-udstyr til universitetets netværk. Rigsrevisionen konstaterer, at KU's politik for forskningsdata giver forskerne meget store frihedsgrader.

Ud over politikken for forskningsdata har KU retningslinjer for overvågning af og adgang til elektronisk post og internet, der har til formål at sikre datas fortrolighed. Af boks 3 fremgår et uddrag af retningslinjerne.

Boks 3

KU's retningslinjer for overvågning af og adgang til elektronisk post og internet

Det fremgår af retningslinjerne, at de skal sikre integritet, fortrolighed og tilgængelighed og skal sikre mod uvedkommendes adgang. Retningslinjerne må ikke forhindre it-afdelingernes arbejde. Retningslinjerne fastsætter bl.a.:

- KU må ikke overvåge den enkelte medarbejders søgninger eller øvrige brug af internettet.
- Løbende overvågning af indholdet i kommunikation og registrering af, hvem den enkelte medarbejder korresponderer med, må ikke finde sted.
- En systemadministrator må aldrig gennemgå en medarbejders elektroniske post alene. Hvis det af tekniske grunde er nødvendigt for en systemadministrator at gennemgå en medarbejders elektroniske post, skal gennemgangen – når det er muligt – foretages sammen med den berørte medarbejder og dennes faglige tillidsrepræsentant.
- Beslutningen om at skaffe sig adgang til medarbejderens elektroniske post kan kun træffes af rektor, prorektor, dekan eller universitetsdirektør. Medarbejderen og dennes tillidsrepræsentant skal straks underrettes skriftligt om beslutningen.

Kilde: KU's retningslinjer for overvågning og adgang til elektronisk post og internet, 1. januar 2009.

Det er Rigsrevisionens vurdering, at retningslinjerne i praksis vanskeliggør den overvågning, it-afdelingerne bør foretage, og som er nødvendig af hensyn til it-sikkerheden. KU's centrale it-afdeling har i den forbindelse oplyst, at it-afdelingen ikke foretager scanninger af netværkstrafik. Dermed er der risiko for, at politikken har den modsatte effekt i forhold til, hvad den egentlig er tiltænkt. Politikken kan svække it-sikkerheden betragteligt og dermed også svække beskyttelsen af forskningsdata. Undersøgelsen viser, at ledelsen på KU har modtaget rapporteringer fra den centrale it-afdeling, hvor der gøres opmærksom på, at it-afdelingen har begrænsede beføjelser til at føre kontrol med it-sikkerheden.

34. Rigsrevisionen vurderer, at KU med de 2 politikker (KU's politik for forskningsdata og KU's retningslinjer for overvågning af og adgang til elektronisk post og internet) ikke har fastsat tilstrækkelige rammer til styring af it-udstyr, og at politikkerne ikke bidrager til at sikre, at forskningsdata beskyttes i tilstrækkelig grad.

De manglende rammer for styring af it-udstyr betyder, at KU's samlede it-sikkerhed på væsentlige punkter overlades til de enkelte forskere. Det er således op til hver enkelt forsker at have kendskab til bl.a. KU's firewalls, opbygning af netværk, routere, servere og de andre forskeres sikkerhedsforanstaltninger. Derudover skal forskeren have kendskab til universitetets trusselsbillede og samlede risikovurdering. Hertil kommer, at forskeren selv har mulighed for at downloade og installere software fra internettet. En tilstrækkelig it-sikkerhed forudsætter således, at forskeren ikke downloader inficeret software og sikrer, at al software til hver en tid er opdateret. Derudover vurderer Rigsrevisionen, at de 2 politikker medfører en uklar rolle for den centrale it-afdeling, og at KU dermed ikke har tilstrækkelig mulighed for at styre it-sikkerheden. På den baggrund er det Rigsrevisionens vurdering, at KU's ledelse ikke lever op til sit ansvar, både i forhold til bevillingsgiver og i forhold til den eksisterende lovgivning på området.

Rigsrevisionen konstaterer i øvrigt, at ingen af de 3 underliggende institutter har suppleret universitetets nedskrevne og ledelsesgodkendte politikker og retningslinjer for styring af it-udstyr på deres institutter.

KU's vurdering af trusler mod KU's it-sikkerhed

35. En trussel kan fx være, at en fremmed stat eller andre uvedkommende vil stjæle information i form af forskningsdata. Et samlet overblik over trusler kan anvendes til at vurdere, hvor mange resurser ledelsen skal prioritere at bruge på it-sikkerhed. Ledelsen på KU har fastsat retningslinjer for udarbejdelse af et register over trusler mod universitetet. Retningslinjerne fastsætter, at der skal udarbejdes et samlet trusselsregister for universitetet, og at registret skal opdateres minimum én gang årligt. KU har dog oplyst, at et egentligt trusselsregister endnu ikke er udarbejdet, og at universitetet heller ikke har fulgt op på, om der udarbejdes trusselsvurderinger lokalt.

Rigsrevisionen konstaterer, at det ikke er muligt for ledelsen på KU at foretage en langsigtet, samlet prioritering i forhold til, hvilke resurser der skal afsættes til it-sikkerhed, når der ikke er foretaget en samlet trusselsvurdering.

KU's vurdering af risici ved at anvende it i forskningen

36. Det fremgår af ISO 27001, at ledelsen skal sikre, at der udarbejdes en vurdering af risici ved it-anvendelsen. En risikovurdering er en vurdering af risici i forbindelse med en aktivitet. Risikoen kan fx måles ved at bedømme, hvor stor sandsynligheden er for, at en fremmed stat eller andre uvedkommende vil udnytte en sårbarhed, og hvilke konsekvenser det vil have.

37. KU har ikke udarbejdet en samlet vurdering af risici ved at anvende it i forskningen. KU har dog udarbejdet flere delkomponenter, som kan danne grundlag for en risikovurdering. Fx udarbejder KU's informationssikkerhedsgruppe årligt en risikovurdering af anvendte systemer og samlinger af forskningsdata med henblik på at udarbejde beredskabsplaner. Risikovurderingen handler om de enkelte systemer og samlinger og udarbejdes i samarbejde med it-afdelingerne på KU. Derudover har informationssikkerhedsgruppen udarbejdet en risikoprofil for KU med input fra fakulteterne. Risikoprofilen indeholder 4 risici, som KU er udsat for i forhold til forskning og uddannelse. Risikoprofilen forholder sig til trusler mod universitetet, men det fremgår ikke klart, hvor sårbart universitetet er i forhold til hvert af punkterne.

Undersøgelsen viser, at KU ikke har dokumentation for, at ledelsen systematisk bruger risikovurderingerne af de udvalgte systemer og samlinger og risikoprofilen til at træffe beslutninger om it-sikkerhed eller til at iværksætte konkrete sikkerhedsforanstaltninger på institutterne.

Derudover er ledelsen på KU flere gange blevet orienteret af KU's informationssikkerhedsgruppe om forskellige risici i it-anvendelsen. Ledelsen blev fx i januar 2017 orienteret om status for KU's it-sikkerhed, herunder at KU har en lav it-sikkerhed. Orienteringen indeholdt en række initiativer til at hæve niveauet for it-sikkerhed, bl.a. at KU skal opdatere politikker og retningslinjer, og at de lokale ledelser skal involveres mere i it-sikkerheden. Derudover fremgår det, at KU skal øge indsatsen i forhold til beskyttelse af forskningsdata og efterlevelse af EU's persondataforordning. KU's ledelse har efterfølgende iværksat flere initiativer med henblik på at højne it-sikkerheden, herunder sammenlægningen af it-afdelingerne på de enkelte fakulteter til én it-afdeling.

38. Niels Bohr Institutet har ikke en ledelsesforankret og nedskrevet risikovurdering, der er godkendt af KU's ledelse. Rigsrevisionen har interviewet systemadministratorer mv., der oplyste, at it-afdelingen på Niels Bohr Institutet tager udgangspunkt i en vurdering af trusler og sårbarheder i tilgangen til it-sikkerhed. Dette bekræftes af, at undersøgelsen viser, at Niels Bohr Institutet har valgt en opbygning af netværket, som Rigsrevisionen vurderer kan beskytte forskningsdata bedre end på de øvrige institutter. Rigsrevisionen konstaterer dog, at da risikovurderingerne ikke er dokumenterede, er beskyttelsen af forskningsdata i høj grad afhængig af enkelte nøglepersoner.

Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab har ikke udarbejdet risikovurderinger. Institutterne har oplyst, at det er deres opfattelse, at KU's centrale it-afdeling håndterer anvendelsen af it på vegne af institutterne.

Fremadrettet har KU's ledelse fastsat, at de enkelte fakultets- og institutledelser skal efterspørge risikovurderinger for it-anvendelse fra forskerne.

Resultater

Undersøgelsen viser, at KU's ledelse ikke har tilstrækkelig opmærksomhed på it-sikkerhed og beskyttelse af forskningsdata. For det første har KU's ledelse fastsat 2 politikker, der i praksis overlader it-sikkerheden og beskyttelsen af forskningsdata til de enkelte forskere, der forventes at have indsigt i en række af KU's it-sikkerhedsmæssige forhold, for at de kan løse opgaven. For det andet har KU fastsat, at der skal udarbejdes et trusselsregister, men universitetet har endnu ikke udarbejdet registret. For det tredje er KU's risikovurderinger mangelfulde, og risikovurderingerne anvendes kun i begrænset omfang til at fastsætte it-sikkerheden på universitetet.

Niels Bohr Institutet har suppleret KU's retningslinjer med mundtlige risikovurderinger og retningslinjer og en heraf følgende praksis. Det betyder, at Niels Bohr Institutet på flere punkter har en højere it-sikkerhed end KU generelt. Mundtligheden betyder dog, at retningslinjerne for it-sikkerhed er meget afhængige af personer, der har viden om risici og beslutninger om sikringstiltag. Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab har ikke suppleret KU's retningslinjer og risikovurderinger. Institutterne har oplyst, at det er deres opfattelse, at it-sikkerheden håndteres centralt på KU. Fremadrettet har KU's ledelse fastsat, at de enkelte fakultets- og institutledelser skal efterspørge risikovurderinger for it-anvendelse fra forskerne.

2.3. KU's beskyttelse af forskningsdata

39. Vi har undersøgt, om KU har en politik for beskyttelse af forskningsdata, og om universitetet sikrer, at data beskyttes i overensstemmelse hermed.

40. Tabel 3 viser undersøgelsens resultater vedrørende KU's beskyttelse af forskningsdata.

Tabel 3
KU's beskyttelse af forskningsdata

Universitetet har ledelsesgodkendte politikker og retningslinjer for klassificering og beskyttelse af data	●
Universitetet sikrer, at klassificerede forskningsdata beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer herfor	●

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

Kilde: Rigsrevisionen.

Det fremgår af tabel 3, at KU har ledelsesgodkendte politikker og retningslinjer for klassificering og beskyttelse af data, herunder en dataklassifikationsmodel. KU sikrer imidlertid ikke, at klassificerede forskningsdata i praksis beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer.

KU har fastsat retningslinjer for klassificering og beskyttelse af data i form af en dataklassifikationsmodel, der fastsætter, hvordan forskellige typer forskningsdata skal beskyttes. Ifølge retningslinjerne skal it-afdelingerne stille løsninger til rådighed, hvor forskerne kan opbevare data i overensstemmelse med dataklassifikationsmodellen. Hvis forskerne vil anvende en anden løsning end den, der stilles til rådighed af KU, skal forskerne risikovurdere opbevaringen af data og orientere institutledelsen herom. Institutledelserne på de 3 institutter har ikke modtaget indberetninger om brug af andre løsninger om opbevaring af forskningsdata end de løsninger, som KU stiller til rådighed, og har ikke efterspurgt disse. Hverken KU's centrale it-afdeling eller nogen af de 3 institutter har periodisk eller stikprøvevist undersøgt, om reglerne efterleves. KU har dermed ikke vished for, at forskerne efterlever politikkerne for dataklassifikation og beskyttelse af forskningsdata.

Rigsrevisionen har gennemført en rundspørge blandt tilfældigt udvalgte forskere på de 3 institutter. Rundspørgen viser, at kun én ud af 26 adspurgte forskere på de 3 institutter kendte indholdet af KU's dataklassifikationsmodel. Vores gennemgang viser derudover eksempler på, at klassificerede data ikke blev opbevaret på KU's løsninger til dataopbevaring. Forskerne anvendte fx online-fildelingstjenester og private servere. Rigsrevisionen vurderer, at KU ikke i tilstrækkelig grad sikrer, at forskerne beskytter data i overensstemmelse med KU's politik.

Resultater

Undersøgelsen viser, at KU ikke i tilstrækkelig grad sikrer, at forskerne opbevarer data i overensstemmelse med KU's politik.

KU har ledelsesgodkendte politikker og retningslinjer for klassificering og beskyttelse af data, herunder en dataklassifikationsmodel. Undersøgelsen viser dog også, at forskerne ikke kender KU's dataklassifikationsmodel. Rigsrevisionen har fundet eksempler på, at forskerne beskytter deres forskningsdata på andre løsninger end dem, som KU stiller til rådighed, uden at de klassificerer data og orienterer institutterne om eventuelle risici ved opbevaringen af forskningsdata. Undersøgelsen viser derudover, at ingen af de 3 institutter har modtaget nogen risikovurderinger fra forskerne om opbevaring af data, og at institutterne heller ikke har efterspurgt disse fra forskerne.

2.4. KU's overblik over anvendt hardware

41. Ukendt hardware på netværket kan udgøre en risiko, hvis der på hardware fx anvendes software, der ikke er opdateret. Derudover kan det udgøre en risiko, hvis uautoriserede personer kobler hardware med installeret software på netværket og dermed har en computer internt i netværket, hvor et angreb på forskningsdata kan startes fra. Vi har undersøgt, om KU har en komplet og opdateret fortegnelse over hardware, som forskerne på universitetet anvender. Derudover har vi undersøgt, om KU identificerer eventuelt ukendt hardware på netværket.

42. Tabel 4 viser undersøgelsens resultater af, om KU har overblik over anvendt hardware.

Tabel 4
KU's overblik over anvendt hardware

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

Kilde: Rigsrevisionen.

Det fremgår af tabel 4, at KU ikke har tilstrækkeligt overblik over anvendt hardware.

Fortegnelse over hardware

43. Det er vigtigt, at KU har et overblik over den hardware, der anvendes på universitetets netværk, så det fx er muligt for it-afdelingerne at følge op på, om den installerede software er sikkerhedsopdateret.

44. Forskerne på KU har mulighed for at anskaffe it-udstyr gennem den centrale it-afdeling på KU. Derudover har KU som tidligere nævnt en "bring your own device"-politik, der fastsætter, at forskere kan anskaffe og medbringe eget it-udstyr. Vores stikprøve viser, at der var it-udstyr, som forskerne selv styrer på alle 3 institutter.

Den centrale it-afdeling på KU har fortegnelser over den hardware, som it-afdelingerne stiller til rådighed for forskerne. Rigsrevisionen har gennem stikprøver kontrolleret disse fortegnelser, og der kun var mindre fejl i disse. KU har dog ikke fuldstændige fortegnelser over den hardware, som forskerne selv medbringer på de 2 institutter.

45. Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab har ikke suppleret den centrale it-afdelings fortegnelse over den hardware, som anvendes på institutterne. Niels Bohr Institutets it-afdeling tilbyder at stille hardware til rådighed for forskerne, og instituttet har fortegnelser over den hardware, som it-afdelingen stiller til rådighed og administrerer. Vi har gennemgået én af disse fortegnelser, og gennemgangen viser, at fortegnelsen var korrekt og opdateret. Niels Bohr Institutet har imidlertid ikke fortegnelser over hardware, der ikke er indkøbt gennem instituttets it-afdeling.

46. KU's ledelse har siden 2017 været vidende om, at universitetet har hardware, som ikke styres af universitetets centrale it-afdeling eller af andre it-afdelinger på KU. Ledelsen har ikke iværksat initiativer til at imødegå dette konkrete problem.

Opdagelse af ukendt hardware på netværk med forskningsdata

47. Da forskerne på KU har tilladelse til at anskaffe og tilslutte it-udstyr til netværk med forskningsdata, er det særligt vigtigt, at universitetets it-afdelinger bruger de tekniske metoder, der findes, til at opdage ukendt it-udstyr, herunder fx scanninger for ukendt it-udstyr. Derved kan it-udstyret undersøges nærmere, ligesom det kan afdækkes, om installeret software er registreret og opdateret.

48. KU har oplyst, at den centrale it-afdeling ikke scanner interne netværk med forskningsdata på Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab, hverken i forhold til ukendt it-udstyr eller i forhold til sårbarheder. Rigsrevisionen konstaterer, at da it-afdelingen ikke scanner efter sårbarheder og trusler, bliver it-sikkerheden på KU helt afhængig af, at hver enkelt forsker agerer sikkerhedsmæssigt forsvarligt. Hvis en forsker tilslutter "usikkert" it-udstyr på netværket, er der stor risiko for, at sikkerheden i det samlede netværk svækkes. Det betyder, at beskyttelsen af de andre forskeres data også svækkes. KU har dog oplyst, at den centrale it-afdeling foretager netværksscanninger på Det Natur- og Biovidenskabelige Fakultet. KU har derudover oplyst, at netværket på Det Natur- og Biovidenskabelige Fakultet er segmenteret i sikkerhedszoner. Formålet er at placere kendt it-udstyr, som ikke kan sikkerhedsopdateres, i disse zoner, så udstyret ikke udgør en sikkerhedsmæssig risiko for forskningsdata. Rigsrevisionen skal hertil bemærke, at effekten af denne løsning dog forudsætter, at KU's centrale it-afdeling har kendskab til det it-udstyr, der skal placeres i sikkerhedszonerne, fx hvis forskeren har oplyst om anskaffelse af udstyret. Rigsrevisionen konstaterer, at løsningen ikke sikrer, at ukendt it-udstyr ikke kan få adgang til netværk med forskningsdata.

49. Der anvendes forskellige løsninger på de 3 institutter til at undgå, at ukendt udstyr får adgang til netværk med forskningsdata.

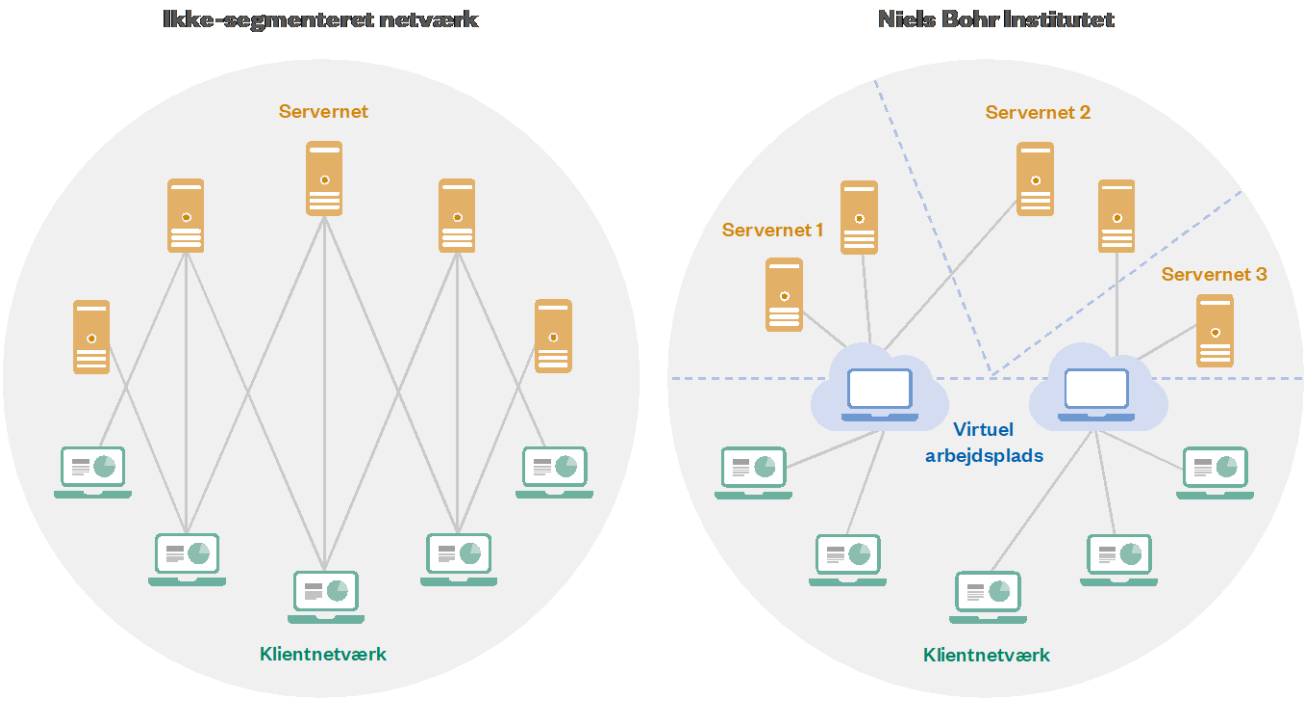
Den centrale it-afdeling anvender på Biomedicinsk Institut en løsning, hvor forskernes adgang til systemer, der indeholder forskningsdata, er stærkt begrænset. Begrænsningen består i, at netværket, som forskerne kan tilgå, er delvist adskilt fra det netværk, hvor forskningsdata er placeret. Hvis hackere eller andre uautoriserede aktører får adgang til netværket med forskningsdata, vil det dog i praksis være muligt at få adgang til andre systemer og forskningsdata på netværket.

På Det Humanistiske Fakultet, som Institut for Nordiske Studier og Sprogvidenskab hører under, anvender KU's centrale it-afdeling teknologien 802.1x, som kan bruges til at sikre, at ukendt it-udstyr ikke kan tilgå netværk, som indeholder forskningsdata. Denne funktion af teknologien anvendes dog ikke, og KU udnytter dermed ikke teknologiens sikkerhedsmæssige potentiale.

802.1x
Teknologi, som kan bruges til at styre, hvilke netværk it-udstyr får adgang til.

Niels Bohr Institutets it-afdeling har vurderet, at it-afdelingen ikke kan beskytte netværk og data, hvor forskerne kan tilslutte hardware, i tilstrækkelig grad. I stedet har hver forsker en "virtuel arbejdsplads", som afvikles på en server separat fra forskerens pc, hvor Niels Bohr Institutet tilbyder, at forskerne kan opbevare deres forskningsdata. Forskerne har så adgang til forskningsdata via denne virtuelle arbejdsplads. Figur 3 viser opbygningen af Niels Bohr Institutets netværk sammenlignet med et ikke-segmenteret netværk.

Figur 3
Opbygning af netværk på Niels Bohr Institutet



Kilde: Rigsrevisionen.

Figur 3 viser, hvordan it-afdelingen på Niels Bohr Institutet har valgt at opdele servernettet på instituttet i forskellige afsnit, så når forskere eller andre får adgang til system og data ét sted, får de ikke automatisk adgang til alle systemer og data på hele servernettet. Det betyder, at en hacker skal hacke hver enkelt forsker for at få adgang til al forskningsdata.

Niels Bohr Institutets opbygning af sine netværk betyder, at det i forhold til beskyttelse af forskningsdata ikke er nødvendigt at styre forskernes pc'er i samme grad som på resten af KU, herunder scanne dem, da forskningsdata opbevares separat. Niels Bohr Institutet scanner jævnligt efter sårbarheder og efter ukendt it-udstyr på det netværk, hvor forskningsdata opbevares.

Niels Bohr Institutets tilgang giver mulighed for, at sikkerheden kan opretholdes på de netværk, der indeholder forskningsdata, idet instituttet kan tilbyde forskerne en løsning, hvor deres forskningsdata er beskyttede, samtidig med at forskeren kan tilslutte sit eget it-udstyr. Rigsrevisionen konstaterer, at dette ikke i samme grad gør sig gældende på de øvrige undersøgte institutter. Det er Rigsrevisionens vurdering, at Niels Bohr Institutets opbygning af netværk kan bruges som inspiration for de øvrige institutter på KU.

Resultater

Undersøgelsen viser, at KU ikke i tilstrækkelig grad har fortegnelser over det it-udstyr, som anvendes af forskerne. KU's centrale it-afdeling og it-afdelingen på Niels Bohr Institutet har fortegnelser over det it-udstyr, som de stiller til rådighed for forskerne, men ingen af it-afdelingerne har dog fortegnelser over det it-udstyr, som forskerne selv anskaffer og tilslutter netværket.

KU's centrale it-afdeling har oplyst, at it-afdelingen ikke scanner netværk med forskningsdata, hverken i forhold til ukendt it-udstyr eller sårbarheder på Biomedicinsk Institut eller Institut for Nordiske Studier og Sprogvidenskab. Sårbarheder og trusler, som kunne afsløres ved scanninger, bliver således ikke identificeret af KU's it-afdelinger.

Niels Bohr Institutet har et design og en tilgang til it-sikkerhed, der åbner mulighed for at beskytte forskningsdata for de forskere, der ønsker dette, selv om der er ukendt it-udstyr på nogle af instituttets netværk. Det er Rigsrevisionens vurdering, at Niels Bohr Institutets opbygning af netværk kan bruges som inspiration for de øvrige institutter på KU.

2.5. KU's overblik over software og softwareopdatering

50. Software, der ikke er opdateret, kan udgøre en risiko for, at hackere kan få uautoriseret adgang til netværket ved at udnytte kendte sårbarheder i softwaren. Vi har undersøgt, om KU har dokumentation for, at softwaren på den anvendte hardware (pc'er og servere) er opdateret. Vi har i den forbindelse udtaget en stikprøve på både pc'er og servere på de 3 institutter.

51. Tabel 5 viser undersøgelsens resultater af, om KU har et tilstrækkeligt overblik over software på henholdsvis pc'er og servere, som har betydning for sikkerheden for forskningsdata, og om softwaren er opdateret.

Tabel 5
KU's overblik over software og softwareopdatering

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

Kilde: Rigsrevisionen.

Det fremgår af tabel 5, at KU ikke har tilstrækkeligt overblik over, hvilken software der anvendes på universitetet, hverken på pc'er eller servere, og om softwaren er opdateret.

Overblik over software på pc'er, og om softwaren er opdateret

52. Den centrale it-afdeling på KU har overblik over og dokumentation for den software, som it-afdelingen selv har installeret på forskernes pc'er. It-afdelingen bruger dog ikke denne dokumentation til at sikre, at softwaren bliver opdateret. Vores stikprøver viser eksempler på pc'er, der styres af KU's centrale it-afdeling, som havde software, der var forældet og i nogle tilfælde sårbar over for angreb.

Dertil kommer, at forskerne har lokaladministratorrettigheder på deres pc'er. Det betyder, at forskerne selv kan downloade og installere software på deres pc'er. It-afdelingerne på KU har ikke ansvar for at sikre software, som it-afdelingen ikke selv har installeret, dvs. at det alene er op til forskeren selv at vurdere risikoen ved at installere den pågældende software og at sikre, at softwaren sikkerhedsopdateres. Rigsrevisionen vurderer, at forskernes lokaladministratorrettigheder udgør en sikkerhedsmæssig risiko for at kunne beskytte forskningsdata, da den samlede sikkerhed afhænger af hver enkelt forskers adfærd.

Det it-udstyr, som forskerne selv anskaffer og tilslutter netværket, udgør ligeledes en risiko. Da it-afdelingen ikke har kendskab til al hardware, som forskerne anvender, er det ikke muligt at vide, hvilken software, der er installeret på hardwaren, og om softwaren er opdateret, når it-afdelingerne ikke gennemfører scanninger på it-udstyret.

Undersøgelsen viser, at hverken Biomedicinsk Institut eller Institut for Nordiske Studier og Sprogvidenskab har overblik over den software, som anvendes på forskernes pc'er. Begge institutter har oplyst, at de ikke har opfattet det som deres opgave at forholde sig til installeret software.

53. Niels Bohr Institutet har fortegnelser over software, der anvendes på det netværk, hvor instituttet placerer forskningsdata. Instituttet har dog ikke fortegnelser over software, som forskerne selv har installeret på it-udstyr, der er tilsluttet det netværk, som forskerne kan tilgå.

54. Undersøgelsen viser, at ledelsen på KU i januar 2017 er blevet orienteret af KU's informationssikkerhedsgruppe om, at universitetet har software, som ikke styres af én af universitetets it-afdelinger, og at det udgør en it-sikkerhedsmæssig risiko. KU's ledelse har på den baggrund besluttet, at de lokale fakultets- og institutledelser skal involveres mere i arbejdet med it-sikkerhed. KU har endnu ikke iværksat konkrete initiativer til at sikre overblik over software og opdatering heraf, hvorfor it-sikkerheden fortsat ikke er tilfredsstillende.

Overblik over software på servere, og om softwaren er opdateret

55. Undersøgelsen viser, at KU's centrale it-afdeling ikke har fuldt overblik over software, der er installeret på servere, hvor der opbevares forskningsdata. It-afdelingen har overblik over den software, som it-afdelingen selv har installeret og styrer, men scanner ikke serverne for ukendt software eller sårbarheder. Derudover har it-afdelingen mulighed for at trække en oversigt over software på de fleste servere, men it-afdelingen bruger dog ikke denne mulighed i forhold til it-sikkerhed.

Endvidere viser undersøgelsen, at Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab heller ikke har overblik over software, der er installeret på serverne. Vores stikprøve viser eksempler på servere på både Biomedicinsk Institut og Institut for Nordiske Studier og Sprogvidenskab med sårbar software, herunder en server, som ikke var blevet sikkerhedsopdateret siden 2015. Det udgør en risiko for beskyttelsen af forskningsdata, da serverne var tilsluttet samme netværk som de øvrige servere. Dermed kan hackere eventuelt udnytte svagheder i software, der ikke er opdateret, til at få adgang til forskningsdata på både den pågældende server og de øvrige servere på netværket.

Derudover viser vores stikprøve, at der på begge institutter er tilsluttet servere, hvor dele af softwaren ikke styres af KU's centrale it-afdeling, dvs. at forskerne selv skal sørge for sikkerhedsopdateringer mv. Disse servere påvirker den samlede beskyttelse af forskningsdata, da de befinder sig på samme netværk som de øvrige servere.

56. Niels Bohr Institutets it-afdeling har dokumentation for, hvilken software der er installeret på de servere, som it-afdelingen selv styrer. It-afdelingen scanner det netværk, som serverne er tilsluttet, for sårbarheder. Vores stikprøver viser, at softwaren på disse servere var sikkerhedsopdateret.

Resultater

Undersøgelsen viser, at den centrale it-afdeling på KU har overblik over den software, som it-afdelingen selv installerer på serverne og på forskernes pc'er, men bruger ikke dette overblik til at sikre, at softwaren opdateres. Vores stikprøve viser eksempler på software på både pc'er og servere, der ikke er sikkerhedsopdateret.

Forskerne har derudover lokaladministratorrettigheder, og det betyder, at der er software, som forskerne selv har downloadet og installeret og selv skal sørge for at sikkerhedsopdatere. Den centrale it-afdeling har heller ikke overblik over software, der er installeret på hardware, som forskerne selv har anskaffet og tilsluttet universitetets netværk. Det betyder, at den samlede it-sikkerhed og beskyttelse af forskningsdata er afhængig af hver enkelt forskers adfærd.

It-afdelingen på Niels Bohr Institutet har overblik over software på de servere, som it-afdelingen selv styrer, og stikprøverne viser, at softwaren var opdateret. Hverken Biomedicinsk Institut eller Institut for Nordiske Studier og Sprogvidenskab har overblik over den software, som anvendes på forskernes pc'er. Institutterne har oplyst, at det er deres opfattelse at it-sikkerheden håndteres centralt på KU.

Ledelsen på KU har i hvert fald siden 2017 været vidende om, at der anvendes ukendt software på universitetet, og at det udgør en sikkerhedsmæssig risiko, hvis denne software ikke opdateres. KU's ledelse har ikke på den baggrund iværksat sikringstiltag, hvorfor it-sikkerheden fortsat ikke er tilfredsstillende.

2.6. Uddannelses- og Forskningsministeriets bemærkninger til undersøgelsen

57. Uddannelses- og Forskningsministeriet har oplyst, at ministeriet på baggrund af de oplysninger, der fremgår af beretningen, tilslutter sig Rigsrevisionens opfattelse af, at beskyttelse af forskningsdata ikke håndteres tilfredsstillende på universiteterne. Ministeriet konstaterer, at det er universiteternes ledelser, der har ansvar for, at der er en høj it-sikkerhed på den pågældende institution, herunder ansvar for, at forskningsdata beskyttes i tilstrækkelig grad. Uddannelses- og Forskningsministeriet har oplyst, at ministeriet i forbindelse med det skriftlige tilsyn i perioden 2015-2017 med de videregående uddannelsesinstitutioner har vejledt institutionerne om vigtigheden af ledelsesmæssigt fokus på informationssikkerhed. Ministeriet er således enig i, at det er centralt, at universiteterne har en høj it-sikkerhed, der beskytter forskningsdata, og ministeriet deler Rigsrevisionens opfattelse af, at det er et område, hvor der trods fokus er potentiale og behov for forbedring.

Uddannelses- og Forskningsministeriet vil kontakte universiteterne og understrege ledelsernes ansvar for området og samtidig bede universiteterne om at identificere og rette op på eventuelle kritiske it-sikkerhedsbrister. Ministeriet vil samtidig i samarbejde med universiteterne udarbejde en plan for, hvordan universiteterne kan rette op på forholdene og få etableret den nødvendige it-sikkerhedsorganisation og -kultur. Målet er, at der udvikles en systematisk og god it-sikkerhedskultur på alle niveauer i organisationen. Ministeriet vil desuden igangsætte en lignende proces på de øvrige videregående uddannelsesinstitutioner.

Resultater

Uddannelses- og Forskningsministeriet deler Rigsrevisionens vurdering af, at der er behov for bedre beskyttelse af forskningsdata, og vil bede universiteterne om at identificere og rette op på eventuelle kritiske it-sikkerhedsbrister. Ministeriet vil igangsætte en lignende proces på de øvrige videregående uddannelsesinstitutioner.

Rigsrevisionen, den 11. januar 2019

Lone Strøm

/Peder Juhl Madsen

Bilag 1. Metodisk tilgang

Formålet med undersøgelsen er at vurdere, om universiteterne beskytter forskningsdata i tilstrækkelig grad.

Først har vi på de 5 største danske universiteter (KU, AU, AAU, SDU og DTU) kortlagt universiteternes risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Dernæst har vi på det største universitet, KU, gået mere i dybden for at undersøge, hvordan universitetets centrale it-afdeling og 3 udvalgte institutter arbejder med it-sikkerheden i forhold til beskyttelse af forskningsdata.

I undersøgelsen indgår Uddannelses- og Forskningsministeriet og de 5 største universiteter målt på antal forskere.

Kortlægningen af universiteternes risikoprofil i forhold til beskyttelse af forskningsdata er baseret på møder med universiteterne og gennemgang af skriftligt materiale.

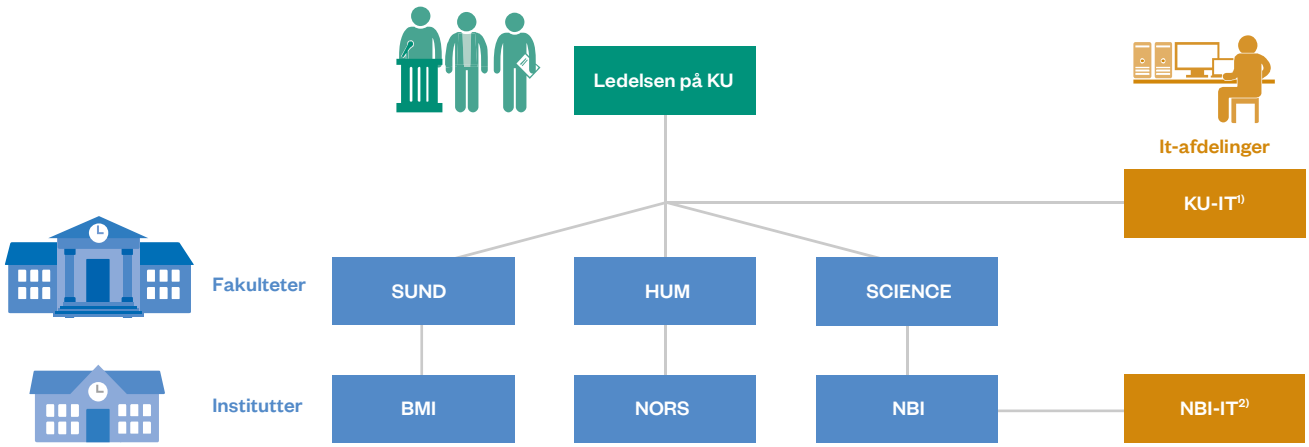
Undersøgelsen på KU er baseret på resultater fra Rigsrevisionens it-revision på KU, som er udført i perioden marts-oktober 2018. Revisionen er baseret på revisionsbesøg på KU, skriftlig dokumentation, en stikprøve med tilfældigt udvalgte pc'er og servere og en rundspørge blandt forskere på KU. Den gennemførte it-revision er afrapporteret i en revisionsrapport, hvori den gennemførte revision og resultaterne heraf er beskrevet.

Udvælgelse af institutter på KU

I undersøgelsen af KU's beskyttelse af forskningsdata indgår KU's ledelse og den centrale it-afdeling på KU. Derudover har vi udvalgt 3 institutter, hvor vi har undersøgt beskyttelsen af forskningsdata.

Vi har valgt Biomedicinsk Institut (BMI) på Det Sundhedsvidenskabelige Fakultet (SUND), Institut for Nordiske Studier og Sprogvidenskab (NORS) på Det Humanistiske Fakultet (HUM) og Niels Bohr Institutet (NBI) på Det Natur- og Biovidenskabelige Fakultet (SCIENCE). Niels Bohr Institutet har som det eneste af de undersøgte institutter sin egen it-afdeling, der ligeledes indgår i undersøgelsen, jf. figuren nedenfor.

Institutter og it-afdelinger, der indgår i undersøgelsen



1) KU-IT er navnet på den centrale it-afdeling på KU. It-afdelingen leverer service til hovedparten af KU, herunder til SUND, HUM, SCIENCE, BMI og NORS.

2) NBI-IT er NBI's egen it-afdeling. NBI hører således ikke under KU-IT.

Kilde: Rigsrevisionen.

De 3 institutter er valgt for at dække så stor en del af KU's virksomhed som muligt. Institutterne er valgt ud fra spredning på forskellige parametre, jf. tabellen nedenfor.

Parametre for udvælgelse af institutter

	"Våde" fag	"Tørre" fag	802.1x	Egen it-organisation	Særlige personoplysninger	Data med høj økonomisk værdi	Data underlagt kontraktuelle krav
SCIENCE: Niels Bohr Instituttet	X			X		X	
SUND: Biomedicinsk Institut	X				X	X	X
HUM: Institut for Nordiske Studier og Sprogvidenskab (audiologopædi)		X	X		X		

Kilde: Rigsrevisionen på baggrund af oplysninger fra KU.

"Tørre" fag og "våde" fag

"Tørre" fag: humanistiske og samfundsvidenskabelige fag.

"Våde" fag: naturvidenskabelige fag.

Med de 3 institutter dækker vi Det Natur- og Biovidenskabelige Fakultet og Det Sundhedsvidenskabelige Fakultet, der er de 2 største fakulteter på KU målt på antal forskere. Begge fakulteter har primært "våde" fag. De øvrige 4 fakulteter på KU er "tørre" fag. Blandt disse har vi valgt Det Humanistiske Fakultet, som har implementeret 802.1x, og som samtidig er det største fakultet blandt de restende 4 fakulteter målt på antal forskere.

Institutterne er valgt for at dække forskellige typer data, der er særligt væsentlige at beskytte: Særlige personoplysninger, data med høj økonomisk værdi og data underlagt kontraktuelle krab.
Endelig er Niels Bohr Institutet også udvalgt, da instituttet har sin egen it-organisation i modsætning til de andre, der hører under KU's centrale it-organisation KU-IT.

På Det Humanistiske Fakultet er der i mindre grad data, som har umiddelbar økonomisk værdi eller er underlagt kontraktuelle krav til beskyttelse, end på de 2 øvrige udvalgte fakulteter. Vi har valgt Institut for Nordiske Studier og Sprogvidenskab, hvor studiet Audiologopædi (tale-høre-pædagog) er tilknyttet. På dette studie findes særlige personoplysninger om både børn og voksne, fx personer med læbe-gane-spalte og hjerneskade. Beskyttelsen af disse data kan være afhængig af den generelle it-sikkerhed på instituttet, herunder om de øvrige forskere sikrer, at deres it-udstyr er opdateret i tilstrækkelig grad. Derudover gennemføres der på instituttet også klassisk humanistisk forskning, hvor det også er relevant at beskytte forskningsdata, der kan være svære eller umulige at genskabe.

Audiologopædi
Audiologopædi handler om talesprogsvanskeligheder. Det udgør ifølge KU's hjemmeside et stort forskningsfelt, som dækker både grundforskning og anvendt forskning. Forskerne på KU deltager p.t. bl.a. i 2 internationale forskningsprojekter om børn, som er født med læbe-ganespalte. De forsker også i virkninger af hjerneskade, bl.a. i forhold til tilbagevenden på arbejdsmarkedet.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

Fra AU, AAU, SDU og DTU

- Korrespondance med AU, AAU, SDU og DTU vedrørende 6 risikofaktorer:
  - Forholder universiteterne sig til risikoen for ukendt it-udstyr?
  - Tillader universiteterne "bring your own device"?
  - Er der fundet ukendt hardware på universiteternes netværk?
  - Beskytter universiteterne deres netværk mod ukendt hardware?
  - Tillader universiteterne forskerne lokaladministratorrettigheder?
  - Har der været sikkerhedshændelser på universiteterne på baggrund af ukendt it-udstyr?
- Skriftlig dokumentation fra universiteterne vedrørende ovenstående risikofaktorer.

Formålet med gennemgangen af dokumenterne er at vurdere de 5 største universiteters risikoprofil i forhold til beskyttelse af forskningsdata.

Fra KU

- KU's informationssikkerhedspolitik med underliggende politikker, fx for hardwareindkøb
- KU's politik for forskningsdata
- KU's retningslinjer for overvågning af og adgang til elektronisk post og internet på KU
- KU's risikovurderinger
- KU's politik for opbevaring af forskningsdata
- KU's årsrapporter vedrørende informationssikkerhed
- KU's scanningsrapporter vedrørende sårbarheder
- KU's Service Level Agreements (SLA-aftaler) –primært mellem KU-IT og de enkelte fakulteter
- KU's rapporter/udtræk vedrørende hardware og software asset management
- mødereferater fra KU's informationssikkerhedsudvalg
- opslag på KU's intranet vedrørende awareness
- sagsnotater om opståede sikkerhedshændelser

- eksempler på varslingsmails til KU, fx fra DKCERT
- screendumps og udtræk fra forskeres pc'er af software og status på, om softwaren er opdateret.

Formålet med gennemgangen af materialet er at vurdere, om KU beskytter forskningsdata i tilstrækkelig grad.

Møder og stikprøve

I forbindelse med kortlægningen af universiteternes risikoprofil har vi holdt møder med KU, AU, AAU, SDU og DTU.

Formålet med møderne var at kortlægge universiteternes risikoprofil i forhold til beskyttelse af forskningsdata.

Derudover har vi i forbindelse med undersøgelsen af KU's beskyttelse af forskningsdata holdt møder med:

- den centrale it-afdeling på KU
- Biomedicinsk Institut
- Institut for Nordiske Studier og Sprogvidenskab
- Niels Bohr Institutet, herunder instituttets it-afdeling.

På møderne har vi bl.a. drøftet KU's politikker og retningslinjer for it-sikkerhed og implementeringen af disse.

Derudover har vi udtaget stikprøver på de 3 institutter. Stikprøven er foretaget ved, at forskerne på forhånd blev informeret om vores besøg og undersøgelsens formål. Vi mødte op på de 3 institutter og udvalgte tilfældigt servere og 26 forskere til at indgå i stikprøven. Vi har dokumenteret stikprøven med screendumps og udtræk som dokumentation for de installerede programmer og opdateringer på serverne og på forskernes pc'er.

Stikprøven havde til formål at undersøge, om softwaren på pc'er og servere var opdateret. Derudover har vi foretaget en rundspørge blandt de forskere, som indgik i stikprøven for at afdække:

- forskernes kendskab til KU's retningslinjer for klassificering af data
- forskernes kendskab til KU's retningslinjer for beskyttelse af data
- hvilken type data forskerne arbejder med
- hvordan forskerne behandler og opbevarer deres data.

Høringsprocedure

Beretningen har i udkast været forelagt Uddannelses- og Forskningsministeriet og KU. Derudover har AU, AAU, SDU og DTU fået forelagt de dele af beretningen, der omhandler disse universiteter. Uddannelses- og Forskningsministeriets og de 5 universiteters bemærkninger er afspejlet i beretningen.

KU har derudover afgivet høringssvar i forbindelse med it-revisionen. I den forbindelse har KU haft mulighed for at rette faktuelle fejl, stille spørgsmål og komme med supplerende oplysninger. I forbindelse med høringerne har vi bl.a. drøftet med KU, hvilke sårbarheder undersøgelsen eksponerer, med henblik på at undersøgelsens resultater blev formuleret i generelle vendinger, så sårbarheder ikke eksponeres unødigt.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision. 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).

Bilag 2. Ordliste

802. 1x	Teknologi, som kan bruges til at styre, hvilke netværk it-udstyr får adgang til. Dermed kan teknologien bruges til at forhindre ukendt it-udstyr i at få adgang til netværk med klassificerede systemer og data.
Bring your own device	Betyder, at ansatte på universitetet har mulighed for at købe it-udstyr uden om it-afdelingen og at tilslutte udstyret til universitetets netværk.
Cyberangreb	Systematisk aktion, hvor nogen forsøger at trænge ind i ét eller flere it-systemer, typisk via internettet.
Cyberspionage	Målrettet og systematisk aktion, hvor nogen forsøger at trænge ind i ét eller flere it-systemer via internettet for at få fat i fortrolige kommercielle oplysninger, fx oplysninger om fremstillingsprocesser eller ingredienser.
Cybertrussel	Trussel fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester.
Forskningsdata	Det materiale og de data, som indgår i forskning.
Forskningsfrihed	Forskernes frihed til helt selv at vælge, hvilket udstyr, metoder og materiale og hvilke metoder de bruger i deres forskning.
Hardware	Den fysiske side af et it-system, dvs. computere eller enheder tilkoblet en computer, fx en printer.
ISO 27001	International informationssikkerhedsstandard, som de statslige institutioner har skullet følge fra januar 2014 og have færdigimplementeret primo 2016. Selvejende offentlige institutioner er ikke pålagt at følge ISO 27001, men Københavns Universitet har valgt at følge sikkerhedsstandarden.
It-sikkerhed	Samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet af informationer og arkiver.
It-sikkerhedshændelse	En fysisk eller logisk hændelse, der har eller kunne have påvirket datas it-sikkerhed.
It-udstyr	It-udstyr anvendes i undersøgelsen som samlet betegnelse for hardware, hvorpå der er installeret software.
Lokaladministrator	Tildelingen af rettighed som lokaladministrator giver medarbejderen det højeste niveau af adgang og kontrol over den computer, som medarbejderen arbejder ved.
Persondataforordning	EU-forordning, som har til formål at styrke beskyttelsen af EU-borgeres personligoplysninger.
Software	Samling af programmer, som gør computeren i stand til at løse opgaver.
Ukendt it-udstyr	It-udstyr, der ikke er kendt af it-afdelingen, fx hvis forskere medbringer eget it-udstyr uden at orientere it-afdelingen om det.