IT- og Informationssikkerhed

Orientering til Bestyrelsen

Informationssikkerhed
15. juni 2021

UNIVERSITY OF COPENHAGEN

KU's risikoprofil

Risikoprofilen viser i fem punkter det, der er vigtigst for at Københavns Universitet kan fungere og dermed også, hvad vi særligt skal have opmærksomhed på. Risikoprofilen kan bruges som udgangspunkt, når vi skal vurdere trusler, risici og værdi for Københavns Universitet.

De fem punkter er opsat i prioriteret rækkefølge.

1.Trusler mod KU's evne og muligheder for at tiltrække samarbejdspartnere, ansatte, studerende og forskningsmidler samt tab af renommé, som konsekvens af at personfølsomme og andre fortrolige oplysninger lækkes

2.Manglende evne til at kunne sikre integritet af og eftervise forskningsresultater på grund af brug af en forkert eller mangelfuld platform til datahåndtering, som ikke beskytter mod forsætlig eller uforsætlig forvanskning af data

3.Tab af renommé og validitet af eksamensbeviser grundet forvanskning af studiedata

4.Tab af renommé og evne til at udføre fremtidig forskning grundet tab eller destruktion af unikke og/eller ikke-genskabelige informationer

5.Trusler mod universitetets basale infrastruktur med deraf afledte økonomiske konsekvenser

Indledende kommentarer

- IT- og informationssikkerhed er på universiteter (verden over) en svær størrelse grundet den type af organisering, som sektoren arbejder ud fra og de relativt frie vilkår forskningen generelt fordrer
- Det ligger i forskningens natur, at der i meget høj grad samarbejdes internationalt på tværs af institutioner og forskningsgrupper. Samtidig er det en grundlæggende forudsætning, at data i videst muligt omfang deles og stilles til rådighed. Denne basale åbenhed bliver i stigende grad udnyttet af eksterne kræfter (bl.a. kriminelle og ikke ligesindede nationer), der uaftalt og/eller ulovligt forsøger at tilegne sig data og viden
- Universitetets IT- og informationssikkerhed afhænger i høj grad af brugernes viden og adfærd, systemer og udstyr, som stilles til rådighed samt den daglige ledelses forståelse for og fokus på området.
- IT- og informationssikkerhed har en stigende ekstern betydning ift. tiltrækning og image – og udgør samtidig en reel beskyttelse af universitetets værdier og daglige drift
- Ledelsen er, jævnfør Informationssikkerhedspolitikken, forpligtet til at risikovurdere og sikre informationer og systemer på passende vis. Politikken følger ISO 27001 standarden

Trafiklys - læsevejledning

- Rød betyder at niveauet er faldet eller at et væsentlig kriterie har ændret sig
- Gul betyder at der skal ekstra tiltag til eller opmærksomhed for at forblive sikker
- Grøn betyder at sikkerheden/opgaven er på rette spor

Trusselsbilledet og KU's sikringsniveau - samlet vurdering

Emne	Trafiklys 15/6	Kommentar
Trusselsbilledet og ændret risikooplevelse – siden seneste rapportering. Risiko måles ved at bedømme, hvor stor sandsynlighed der er for, at en trussel indtræffer, samt hvor store konsekvenser det kan have.		Truslen mod sektoren er steget yderligere. Truslerne vurderes af Center for Cyber Security (CFCS) som: • Cyberspionage, Cyberkriminalitet og Insidertruslen er meget høj • Cyberaktivisme er lav. Der er generelt udstedt varsler fra ligesindede landes sikkerhedstjenester om Corona-forsknings spionage fra statsmagter. Siden seneste rapportering er cyberkriminalitets-modeller udviklet og raffineret yderligere pga. Corona-situationen og de potentielle muligheder for økonomisk gevinst. Den generelt svage sikkerhedskultur internationalt blandt universiteter og andre vidensinstitutioner udnyttes til angribernes fordel og stort set hver uge bliver et nyt universitet alvorligt påvirket af et cyberangreb.
KU's sikringsniveau ift. trusselbilledet		KU's sikringsniveau har hidtil modstået angreb m.v. udefra. Men KU-IT's tekniske sikringsløsninger skal slå fuldt igennem i praksis, og der udestår fortsat, at en række tekniske forbedringer er tilgængelige for alle på KU eller anskaffet og idriftsat. Corona-hjemsendelsen har endvidere sinket tiltag, der forudsætter fysisk tilstedeværelse af brugere og/eller teknikere. En stor del af KU's forskning sker på udstyr, der er opsat i forskningsmiljøet og drevet af forskerne selv. På dette punkt hviler sikkerheden på overholdelse af den organisatoriske vejledning, der skal sikre udstyret og dets datas beskyttelse. Som en udløber af Rigsrevisionens påpegning af en manglende risikobaseret sikringskultur i forskningen blev der udarbejdet risikovurderinger for alle forskningsbærende enheder på KU. Disse risikovurderinger skal fortsat støttes til at blive vedligeholdt i alle enheder.

Overordnet sikringsniveau

Emne	Trafiklys 15/6	Kommentar
Organisatorisk og teknisk sikringsniveau	●	KU-IT's tekniske sikringsløsninger skal slå igennem teknisk og på den måde de administreres. Der udestår fortsat, at en række tekniske forbedringer er færdiggjorte og samarbejder mod et fælles sikrings- og logningsniveau for at beskytte KU's sikringsmiljø tidssvarende. Det gælder for netværk, servere samt klienter. En stor del af KU's forskning sker på udstyr, der er opsat i forskningsmiljøet og drevet af forskerne selv. På dette punkt hviler sikkerheden på overholdelse af den organisatoriske vejledning, der skal styre benyttelsen, udstyrets og dets datas beskyttelse. KU kan med fordel teknisk sikre at dette udstyr, der benyttes af forskerne, skal leve op til et minimumsniveau for at tilgå data og benytte de fælles ressourcer såsom netværksadgang.
Igangsatte initiativer	●	Som en udløber af Rigsrevisionens påpegning af en manglende risikobaseret sikringskultur i forskningen blev der igangsat en række sikringsinitiativer. Udover dette foreligger der en række besluttede initiativer til sikring. Førend at disse initiativer er færdigimplementeret foreligger der ikke en nødvendig sikring. Der skal ske installation og udskiftning af systemer og hardware, sikker administration af det samt sikres den nødvendige logning og overvågning af loggen for at opnå den påkrævede sikring af KU's netværk, udstyr og data. Færdiggørelsen konkurrer med andre udviklingstiltag om de samme ressourcer. Dette forhold bør løses ved en ledelsesbeslutning

Persondataforordningen (GDPR)

Emne	Trafiklys 15/6	Status	Kommentar
Privatlivspolitik, procedurer, vejledninger og skabeloner til persondata udarbejdet og i drift.		Løbende vedligehold	Overholdelsen af procedurerne blev evalueret af Deloitte i 2020 med positivt resultat. Evaluering af overholdelsen af GDPR i 2021 udsættes til efteråret, da det forventes, at medarbejderne vil være fysisk til stede.
Sikkerhedshændelser indberettet til Datatilsynet		12 indberetninger i første 4 måneder af 2021	Hovedsagelige menneskelige fejl. Datatilsynet har afsluttet sag om misbrug af administratoradgang uden kritik. Datatilsynet har stillet en række spørgsmål angående sag om tyveri af kamera med patientoptagelser fra studerende under praktik i lægepraksis. KU er i gang med at indkøbe en løsning til sikker lagring af studerendes optagelser i almen praksis, således at brug af analoge kameraer undgås.

Persondataforordningen (GDPR)

Emne	Trafiklys 15/6	Status	Kommentar
Opfølgning på Schrems-II-dommen angående overførsel af persondata til lande uden for EU/EØS		Der er nedsat en intern arbejdsgruppe, som skal kortlægge aftaler og kontrakter, hvor persondata overføres til lande uden for EU/EØS. Arbejdsgruppen har udarbejdet templates til registrering af databehandleraftaler mv. og arbejdet med registrering af alle aftaler forventes afsluttet inden sommerferien 2021.	EU-Domstolen har den 16. juli 2020 afsagt en dom, som betyder, at persondata ikke kan overføres til USA uden supplerende garantier. Dommen opstiller nye krav, hvis persondata skal overføres til andre lande uden for EU/EØS. Det Europæiske Databeskyttelsesråd har sendt et udkast til guideline om supplerende garantier i høring. Såfremt den nye guideline vedtages i den foreliggende form vil det blive muligt at fortsætte forskningssamarbejder med pseudonymiserede data. Der stilles krav om stærk kryptering for anvendelse af cloud-leverandører i lande, som ikke lever op til de europæiske garantier. KU-IT er ved at afsøge muligheder for at administrere krypteringsnøglen inden for EU, hvilket vil lovliggøre brug af især amerikanske leverandører af cloud-services.
GDPR on-line kursus obligatorisk		Pr 29. april 2021 har 4534 medarbejdere taget kurset ud af 12.000, som har adgang til kurset	Kurset blev i 2020 obligatorisk for alle medarbejdere, som behandler persondata Der er indledt en proces for indkøb af et on-line GDPR-kursus til studerende Ledelseskredsen vil nu blive bedt om at sikre, at medarbejderne tager kurset, hvis de behandler persondata som led i arbejdet på KU