

Referat

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse	15. december 2021
Dato og tidspunkt:	15. december 2021 klokken 12:30-14:30	
Sted:	Teams	
Deltagere:	Bue Raun Andersen, Jacob-Steen Madsen, Janni Lee B. Bang Brodersen, Rune Nørgaard Jørgensen, Mads Lildholdt, Martin Svensson, Peder Thusgaard Ruhoff, Jesper Bo Nielsen, Bjarne Nielsen, Jan I. Kristensen og Dorte Wulff (gæst under pkt. 3 og 4)	
Afbud fra:	Simon Kamber	
Referent:	Natalie Olsen	

Dagsorden:

- 1. Godkendelse af dagsorden og referat** Ingen bemærkninger.
- 2. Meddelelser**

Bue Raun Andersen orienterede om, at Udvalget tidligere på året blev orienteret om, at Rigsrevisionen satte fokus på universiteternes beskyttelse af forskningsdata på en række udvalgte områder. SDU har nu indleveret opdateret materiale, og på baggrund af dette vil SDU have en dialog med Rigsrevisionen i starten af det nye år.

SDU Digital arbejder i samarbejde med SDU IT og SDU RIO på at optimere processen for håndteringen af sikkerhedsbrud på SDU. Udvalget præsenteres for den optimerede proces, når denne foreligger.

Jacob-Steen Madsen orienterede om, at værktøjet til at lokalisere CPR-numre i Outlook – den såkaldte CPR-scanner som kunne hentes i Software Center – er taget ud af drift grundet udfordringer med den tekniske opbygning og pålideligheden af værktøjet. SDU IT afsøger mulighederne for at implementere en løsning, der allerede findes i SDU's MS365-miljø, som skal erstatte CPR-scanner-værktøjet. Der vil i starten af 2022 blive gennemført pilottest i samarbejde med Økonomiservice, hvorefter der foretages bredere udrulning. Jesper Bo Nielsen spurgte, hvad tidshorizonten for fuld udrulning af værktøjet er, da det er et centralt hjælpeværktøj til oprydning i Outlook. Jacob-Steen Madsens tilkendegiver, at der er en målsætning om hurtigt stille værktøjet til rådighed for alle ansatte på SDU, men at SDU IT ønsker at sikre at brugeroplevelsen er optimal før fuld udrulning.

Jacob-Steen Madsen henledte opmærksomheden på den sårbarhed der er identificeret i log4j. Log4j er et produkt benyttet til at lave logning i software, som i høj grad benyttes. AU og AAU har været nødsaget til at lukke for adgangen til centrale systemer, men qua SDU's proaktive arbejde på sikkerhedsområdet samt styr på SDU's infrastruktur, er SDU ikke synderligt berørt. Jacob-Steen understregede dog, at særligt forskningssoftware på fakulteterne udgør en særlig risiko, hvorfor fakulteterne snarest muligt vil blive bedt identificere og kvalificere servere ejet af lokale forskningsmiljøer.

Jesper Bo Nielsen opfordrede SDU IT til at 'sprede det gode budskab' om håndteringen af situationen, og Rune Nørgaard Jørgensen efterspurgte lidt tekst om sårbarheden og håndteringen. Jacob-Steen Madsen deler et kort skriv med Udvalgets medlemmer.

Bue Raun Andersen henledte opmærksomheden på, at Udvalget på seneste møde gav tilsagn til at arbejde videre med den præsenterede struktur for en årsrapport om arbejdet med databeskyttelse og informationssikkerhed på SDU. Rapportens format revideres, således at den får en mere kommunikativ vinkel. Det endelige materiale præsenteres på næstkommende møde i Udvalget.

3. Beslutningspunkt: Løbende kontrol af gæsters adgang til sites i M365

Dorte Wulff skitserede kort problemstillingen. Der er oprettet en masse Sharepoint- og/eller Teams-sites, hvor ejerne af disse på et tidspunkt har inviteret eksterne gæster ind i sitet. Udfordringen er, at der ikke løbende tages stilling til, om disse gæster fortsat har et formål med at have adgang til det enkelte site. Der indstilles til at Udvalget drøfter, hvorvidt der skal iværksættes en pilottest af det præsenterede flow, hvor ejere af Sharepoint- eller Teams-sites skal tage stilling til, om eksterne gæster fortsat skal have adgang.

Udvalget støttede overordnet, at SDU skal have styr på, at det udelukkende er brugere der har et formål med at have adgang til et site, der skal have adgang og at denne kontrol løbende skal foretages. Dorte Wulff præciserede, at det alene omhandler eksterne gæster, som ikke har en SDU-konto.

Dele af Udvalget påpeger potentielle udfordringer med den foreslåede frist på 7 dage af hensyn til f.eks. ferie. Andre dele af Udvalget fremhævede i den forbindelse, at en længere frist ikke nødvendigvis er hensigtsmæssig, da det ofte ses, at gives der en lang frist, så venter brugeren blot med at reagere – eller i sidste ende glemme at reagere.

Flere af Udvalgets medlemmer påpeger desuden, at det er u hensigtsmæssigt at inaktive gæster, som ejeren af sitet ikke har forholdt sig til inden for fristen, automatisk fjernes. Janni Lee B. Bang Brodersen supplerede i den forbindelse, at der er mulighed for en opsætning, hvor den automatiske fjernelse af gæster udelukkende berører inaktive gæster. Udvalgets medlemmer pointerede i den henseende, at det ikke adresserer de situationer, hvor inaktivitet er naturligt (f.eks. forskningsprojekter eller længerevarende projekter af anden karakter).

Bue Raun Andersen opsummerede, at brugerrettede løsninger er en forudsætning for vellykket sikkerhedsarbejde. Projektet håndterer Udvalgets opmærksomhedspunkter, og Udvalget forelægges et revideret udkast.

- 4. Drøftelsespunkt:** Dorte Wulff introducerede punktet. Projektet udspringer blandt andet af det brud Datatilsynet udtalte alvorlig kritik af SDU på baggrund af, og projektet har som målsætning at etablere et overblik over hvilke typer data, der behandles på hvilke typer sites (Teams, Sharepoint, Jammer mv.). Der findes omtrent 14.000 sites med uklassificerede data. Det foreslås, at klassificeringen fremadrettet foretages ud fra de præsenterede prædefinerede kategorier. Janni Lee B. Bang Brodersen tilføjede, at det essentielle ved denne løsning er, at brugerne alene bliver bedt forholde sig til hvilke typer data der behandles, og hvorvidt det skal deles med eksterne, og så har SDU på baggrund af dette på forhånd fastlagt et passende sikkerhedsniveau. Udvalget bedes forholde sig til de prædefinerede kategorier, samt hvordan brugerrettet implementering sikres.

Martin Svensson fremhævede, at navngivningen og de bagvedliggende sikkerhedsniveauer ikke fremstår gennemsigtige for brugeren (f.eks. hvad offentliggørelse omfatter, betydningen af webadgang og hvilken der skal benyttes til projekter med eksterne hvor der ikke deles persondata), og at det derfor potentielt af brugerne kan opleves ressourcetrævende at klassificere sit site.

Peder Thusgaard Ruhoff spurgte om denne klassificering omfatter både hoved- og sub-sites. Jacob-Steen Madsen svarede, at alle sites som udgangspunkt skal klassificeres. Der findes dog sites, hvor der anvendes en ældre opbygning af f.eks. Sharepoint, og i de tilfælde, skal kun hovedsitet klassificeres. SDU IT går i dialog med ejerne af de enkelte sites, når løsningen implementeres.

Bue Raun Andersen opsummerede, at Udvalget overordnet giver tilsagn til arbejdet med klassificering af sites. Udvalget vurderer, at udfordringen omkring uklassificerede sites i vid udstrækning kan håndteres med udgangspunkt i de forelagte prædefinerede kategorier, men at der er behov for et øget fokus på at etablere en brugerrettet løsning.

- 5. Orienteringspunkt:** Jacob-Steen Madsen skitserede kort problemstillingen, hvor SDU ønsker at opnå kontrol over data behandlet på mobile enheder. Udvalget har tidligere godkendt, at SDU IT udførte en kontrolleret udrulning af MAM-WE, førend løsningen implementeres på hele SDU. Løsningen er nu afprøvet i både SDU IT og SDU Digital, og funktionaliteten er uproblematisk. Under pilottesten blev et konkret brud på persondatasikkerheden synligt, og dette konkrete brud og fremtidige lignende brud skal håndteres før udrulningen forsætter. Når SDU IT er klar til videre udrulning, kontaktes Udvalgets medlemmer med henblik på at teste løsningen blandt forskere.

Bue Raun Andersen understregede, at opsætningen af løsningen er ligetil og i øvrigt opleves uproblematisk at anvende. Udvalget havde ingen yderligere bemærkninger.

**6. Beslutningspunkt:
Retningslinjer for
databeskyttelse i
studerendes
selvstændige
opgaver**

Bue Raun Andersen introducerede punktet. Projektgruppen har i samarbejde med ledelsesgruppen udarbejdet dels en politik og dels retningslinjer for databeskyttelse i studerendes selvstændige opgaver. Politikken foldes ud i retningslinjer med fokus på tre forskellige modeller; standard-, inddragelses- og tilknytningsmodellen. Retningslinjerne skal ikke betragtes som et kommunikativt dokument, men skal udgøre grundlaget for konkrete produkter til at understøtte studerende og vejledere. Produkterne udarbejdes af SDU Digital, SDU IT, SDU RIO og SUND.

De Studerende i Centrum har behandlet politikken, og de ønskede så meget understøttelse som muligt. Direktionen tiltrådte den endelige politik primo december 2021. Det indstilles, at Udvalget godkender retningslinjerne, således at de beskrevne produkter kan udarbejdes.

Martin Svensson vurderer, at retningslinjerne kan opfylde SDU's behov, men at de kan opleves omstændige. Jan I. Kristensen og Jesper Bo Nielsen opfordrede til, at retningslinjerne blev godkendt i deres nuværende form af imødekomme det behov SDU har for at kunne levere konkret vejledning til undervisere og studerende, men at retningslinjerne kan revideres efter behov. Jesper Bo Nielsen fremhævede desuden, at man på SUND pt. arbejder på en opdateret specialekontrakt, som tager højde for retningslinjerne, og at dette kan være én måde hvorpå studerende og vejledere kan opleve processen mere smidig.

Peder Thusgaard Ruhoff bad om at afgangsprojekter blev tilføjet eksemplerne på selvstændige opgaver, således at det er klart, at retningslinjerne også omfatter disse.

Bue Raun Andersen konkluderede, at retningslinjerne godkendes, og at SDU Digital, SDU IT, SDU RIO og SUND kan begynde at lave de i retningslinjerne beskrevne produkter. Retningslinjerne skal anses som dynamiske, således at opleves der udfordringer i implementeringen af disse, kan disse løbende behandles i Udvalget. Afgangsprojekter tilføjes retningslinjerne.

**7. Beslutningspunkt:
Retningslinjer for
brug af IT på SDU**

Janni Lee B. Bang Brodersen præsenterede punktet. Hovedsamarbejdsudvalget godkendte i december 2021 den del af de nye personalepolitiske retningslinjer, der vedrører brugen af IT. Disse afspejler SDU's overordnede politik på området, mens retningslinjerne for brug af IT på SDU, som behandles på dette punkt, i højere grad er brugerrettede og underbygget med eksempler. Udvalget har fået mandat til at vedtage løbende tilpasninger af retningslinjerne for brug af IT på SDU. Det indstilles, at retningslinjerne godkendes.

Martin Svensson tilslutter sig retningslinjerne, men understreger at de fremstår opfattende og med en del angivelser af, hvad man ikke må. På den baggrund efterspørges det, at der tilføjes en passus, hvori man forholder sig til SDU's ambition på området – dvs. at sikkerhedstiltag ikke blot skal være begrænsninger men i lige så høj grad understøtte SDU's strategi. Jesper Bo Nielsen bakkede op.

Bue Raun Andersen opsummerede, at SDU Digital tilføjer en passus i starten af retningslinjerne på baggrund af Udvalget inputs, og at retningslinjerne i derudover godkendes.

**8. Beslutningspunkt:
Automatisk
viderestilling af
mails**

Janni Lee B. Bang Brodersen præsenterede punktet. Udvalget har tidligere behandlet problematikken omkring automatisk viderestilling af mails. På baggrund af Udvalgets opmærksomhedspunkter, foreslås en pragmatisk løsning, som indebærer, at automatisk viderestilling af mails fremadrettet udelukkende kan ske til maildomæner optaget på tunnelmaillisten¹. Der indstilles, at indstillingen godkendes, og at den brugerrettede kommunikation omkring beslutningen udarbejdes og godkendes af SDU Digital og SDU IT.

Martin Svensson spurgte, om løsningen udelukkende omfatter automatisk viderestilling og ikke manuel videresendelse af mails. Janni bekræftede.

Jesper Bo Nielsen spurgte ind til omfanget af berørte mails, hvis denne løsning tiltrædes. Janni oplyser, at cirka 3.500 mails er sendt til mails som ikke er optaget på tunnelmaillisten ud af cirka. 20.000 mails. Mads Lildholdt spurgte, hvordan mails optages på denne liste, hvortil det blev gjort klart, at SDU ikke administrerer eller har indflydelse på tunnelmaillisten.

Bue Raun Andersen bemærker, at indstillingen godkendes, og den videre proces fsva. udmøntning varetages af SDU Digital og SDU IT.

9. Eventuelt

Ingen bemærkninger.

¹ Optagelse på tunnelmaillisten kræver, at man får tilkøbt virksomhedscertifikat på sit maildomæne samt laver særlige sikkerhedsindstillinger fx aktivering af TLS 1,2 kryptering. Den aktuelle tunnelmailliste bliver opdateret dagligt og kan tilgås her: <https://helpdesk.vipre.com/hc/en-us/articles/115001935647-Tunnelmaillist-Updated-20-12-2021->