SDU Digital

Referat

12. oktober 2022

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse
Dato og tidspunkt:	12. oktober 2022 klokken 10-12
Sted:	New Sapphire (V7 – 510 – 2)
Deltagere:	Bue Raun Andersen, Jacob-Steen Madsen, Jan I. Kristensen, Mads Lildholdt, Rune Nørgaard Jørgensen, Jesper Bo Nielsen, Martin Svensson, Peder Thusgaard Ruhoff, Janni Lee B. Bang Brodersen (observatør) og Simon Kamber (observatør)
Afbud fra:	Bjarne Nielsen
Referent:	Natalie Olsen

Dagsorden:

1. Godkendelse af dagsorden og referat

Ingen bemærkninger.

2. Meddelelser

Bue Raun Andersen og Jacob-Steen Madsen orienterede om, at Rigsrevisionen har fulgt op på tidligere tilsyn fra 2018 og 2019. Rigsrevisionens fokus var beskyttelsen af forskningsdata herunder blandt andet Bring Your Own Device, ukendt hardware på SDU's netværk samt hændelser. Rigsrevisionen aflægger også AU, KU, DTU og AAU besøg med samme fokusområde.

Der er afholdt to møder, og Rigsrevisionen udtrykte begejstring for SDU's måde at arbejde med operationel it-sikkerhed på. Rigsrevisionen efterspurgte udsnit af IT-sikkerhedshåndbogen, og dette har givet anledning til at fremsende enkelte reviderede afsnit, selvom den samlede håndbog ikke er endeligt revideret og godkendt. De fremsendte afsnit er revideret, så de afspejler Udvalgets tidligere beslutninger, og Udvalget vil blive forelagt IT-sikkerhedshåndbogen, når den fulde revidering er gennemført. Rigsrevisionen forventer at have en rapport klar omkring sommeren 2023.

Jacob-Steen Madsen meddelte, at Heimdal er implementeret. Heimdal muliggør, at den enkelte bruger i et kort tidsrum kan elevere sine rettigheder. Der er under implementeringen identificeret lokale behov på hhv. Det Naturvidenskabelige Fakultet og Det Tekniske Fakultet, og disse er ved at blive håndteret i samarbejde mellem SDU IT og det enkelte fakultet.

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

Jacob-Steen bemærkede, at Udvalget tidligere har godkendt en pilottest af MAM-WE med henblik på fuld udrulning på SDU. Udrulningen vil ske med afsæt i transparens for den enkelte medarbejder og med hensyn til de læringspunkter, der er identificeret i pilottesten. Udvalget vil blive forelagt en indstilling på et kommende møde.

Jacob-Steen meddelte, at praksis på SDU har været, at SDU IT med jævne mellemrum forsøge at knække ansatte og studerendes passwords, for at sikre et endnu bedre værn mod it-kriminelle. Denne praksis blev sat på hold under corona-pandemien grundet begrænsede muligheder for support. Nævnte praksis er nu genoptaget, og det er konstateret, at i alt cirka 8.000 brugere har et password, der inden for rimelig tid kan knækkes. Disse brugere vil derfor i nærmeste fremtid blive bedt skifte password. Da Udvalget senest behandlede passwordpolitik på SDU, blev det besluttet, at passwordlængden fremadrettet skulle være 14 tegn, såfremt brugeren selv aktivt skiftede password. Denne politik vil også blive implementeret i dette tilfælde, hvor der er tale om et påkrævet passwordskift. Jacob-Steen vurderer, at størstedelen af de berørte brugere er studerende, men der er også ansatte blandt de cirka 8.000.

Jacob-Steen bemærkede, at SDU anvender teknologier, som ved hjælp af machine learning identificerer unormal adfærd. Unormal adfærd kan øge brugerens risikoscore og i sidste ende lede til udelukkelse af adgang til SDU's systemer. I tilfælde af udelukkelse er det centralt, at brugerne forsat kan få adgang til SDU's systemer, og SDU IT ønsker derfor at aktivere Self Service Password Reset (SSPR). SSPR blev aktiveret for de studerende i sommer, og det ønskes nu også aktiveret for ansatte. Udvalget vil behandle indstillingen på et kommende møde.

Jacob-Steen nævnte, at der på seneste møde i Udvalget, som blev aflyst, var et punkt på dagsordenen vedrørende forvaltningsaftaler omkring driften af forskerservere. Jacob-Steen har haft en bilateral dialog herom med Det Naturvidenskabelige Fakultet og Det Tekniske Fakultet, og det har medført et behov for at tilpasse indstillingen. Den tilpassede indstilling vil blive forelagt Udvalget til godkendelse på et kommende møde.

Simon Kamber henledte Udvalgets opmærksomhed på nyhedskanalen i Teams-sitet "Databeskyttelse og informationssikkerhed på SDU". Det fremgår af de seneste nyheder fra Datatilsynet, at der i højere grad en tidligere anvendes påbud som sanktionsform. Som eksempel herpå nævnes Mariagerfjord Kommune, som fik påbud om at lukke bred anvendelse af lokaladministratorrettigheder, eller en leverandør som med kort frist fik påbud om at implementere en MFA-løsning. Lignende kan potentielt gøre sig gældende for SDU, hvis Datatilsynet observerer, at SDU's praksis ikke er i overensstemmelse med databeskyttelsesreglerne.

Peder Thusgaard Ruhoff spurgte, om Datatilsynet benytter sig af strakspåbud, som man kender det fra arbejdsmiljøsammenhænge. Simon Kamber sagde, at det ikke er noget, man direkte har set anvendt, men i sagen omkring brugen af Google Chromebooks i folkeskoler i Helsingør Kommune, føltes den korte frist nok reelt som et strakspåbud for den dataansvarlige.

Jan I. Kristensen bemærkede i forlængelse af omtalen af Google Chromebooks-sagen, at USA's præsident Joe Biden har udstedt et præsidentielt dekret om udveksling af personoplysninger mellem USA og EU. Dette kan muligvis på et tidspunkt have en betydning for SDU's muligheder for at indgå aftaler med f.eks. amerikanske leverandører. Simon Kamber oplyste, at der er flere aktører (herunder Max Schrems), der har stillet spørgsmålstegn ved om dekretet reelt løser de problemer, der gav anledning til Schrems II-dommen. Det betyder, at selv om dekretet fører til en ny aftale om overførsel, bør SDU tage hensyn til risikoen for, at også den nye aftale bliver underkendt ved EU-domstolen.

Janni Lee B. Bang Brodersen oplyste, at Uddannelses- og Forskningsministeriet har bedt SDU indmelde samfundsvigtige funktioner og kritisk infrastruktur, der understøtter disse. Det indmeldte bliver muligvis omfattet af NIS2. SDU har fulgt praksis på de øvrige universiteter og har ikke ændret på tidligere indmeldte systemer, hvorfor retsmedicins myndighedsbetjening og Tvillingeregistreret blev meldt ind igen. Denne indmelding vil blive indlejret i SDU Digital, Compliance årshjul, da det fremadrettet skal foregå en gang om året.

Janni Lee B. Bang Brodersen meddelte, at en anmeldelse af et potentielt brud på persondatasikkerheden gav anledning til en drøftelse af, om karakterer er en fortrolig oplysning. Drøftelserne tydeliggjorde, at opfattelsen og tilhørende praksis var forskellig forskellige steder på SDU. SDU Digital, Compliance og SDU Studieservice arbejder derfor i fællesskab på en tilpasning af praksis, så karakterer fra 1. februar 2023 betragtes som en fortrolig oplysning.

Natalie Olsen meddelte, at retningslinjerne for brug af IT nu er kommunikeret bredt ud i organisationen. Retningslinjerne findes i en brugerrettet version og fuld version på SDUnet, GDPR- og informationssikkerhedskoordinatorerne er orienteret, nyhed i FANe-nyhedsbrev, nyhed på SDUnet og der vil være en orientering på næstkommende område- og sekretariatschefsmøde.

3. Beslutningspunkt: Ophørs- og slette-proces på SDU

Jacob-Steen Madsen rammesatte punktet. Et udbud af SDU's Microsoftlicenser har givet anledning til en tilpasning af SDU's proces for brugernedlæggelse ved studie- og ansættelsesophør. Tilpasningen gennemføres dels for at sikre at processen er i overensstemmelse med databeskyttelsesreglerne og dels for at fritage SDU for den økonomiske byrde, det vil være at beholde licenser/brugere, som er inaktive. Det indstilles, at Udvalget godkender den beskrevne proces for nedlæggelse af studenter- og ansat-konti.

Flere af Udvalgets medlemmer bemærkede, at der kan være hensyn, der taler for ikke at nedlægge en brugerkonto ved ansættelsesophør. Det kan f.eks. være ph.d.-studerende, der afventer bedømmelse af afhandling eller forskere, der i forbindelse med publicering af forskningsartikler skal oplyse en mailadresse, de kan kontaktes på. I sidstnævnte tilfælde er det særligt centralt, at brugeren til enhver tid, uanset hvor længe efter ansættelsesophør det er, kan få adgang til mails sendt til vedkommendes SDU-mail.

Jacob anerkender disse hensyn og fremhæver, at det netop er derfor, at den endelige beslutning om nedlæggelse/forlængelse af kontoen er placeret decentralt hos det enkelte institut/afdeling – og i sidste ende dermed hos institutlederen eller område- og sekretariatschefen. Simon Kamber understregede i den forbindelse, at SDU skal sikre sig, at der fortsat er hjemmel til at opbevare oplysningerne, hvis brugeren konto forlænges, og at denne vurdering skal dokumenteres. Jacob-Steen bemærkede i forlængelse heraf, at processen ikke igangsættes førend hele processen – inkl. relevante databeskyttelsesmæssige vurderinger – er beskrevet og kommunikeret ud i organisationen. Janni Lee B. Bang Brodersen opfordrede desuden til, at journalisering af journaliseringspligtigt materiale indtænkes i processen.

Bue Raun Andersen opsummerende, at Udvalget tiltræder indstillingen, men at der skal etableres en proces, som afspejler lokale behov og som er i overensstemmelse med databeskyttelsesreglerne. Sidstnævnte kan f.eks. håndteres ved et 'begrundelsesfelt', når kontoen forlænges og ved at klæde GDPR-koordinatorerne på til at kunne bistå de lokale miljøer i at vurdere, om der fortsat er hjemmel til at behandle oplysningerne.

4. Orienteringspunkt: IT-sikkerhed – brug af IT og overvågning på SDU

Jacob-Steen Madsen introducerede punktet. Udvalget fik i juni 2022 en præsentation af SDU's SIEM-løsning, og her udtrykte Udvalget bekymring over den manglende inddragelse af Hovedsamarbejdsudvalget (HSU). Det er på baggrund af heraf beskrevet, hvordan der bedrives operationel IT-sikkerhed på SDU, og HSU er orienteret herom.

HSU tog orienteringen til efterretning og universitetsdirektøren fremhævede på HSU-mødet, at såfremt brugerne - i overensstemmelse med det tilladte i retningslinjerne for brug af IT anvender SDU's ressourcer til privat brug – og er utrygge ved disse sikkerhedsforanstaltninger, er anbefalingen at undgå brug privat brug. Det indstilles derfor, at Udvalget tager til efterretning at HSU på transparent vis er orienteret om, hvordan SDU bedriver IT-sikkerhed, og at fremtidige drøftelser og beslutninger i Udvalget for informationssikkerhed og databeskyttelse tager afsæt heri.

Mads Lildholdt anfægtede, at HSU er blevet forelagt det som et orienteringspunkt. HSU har tidligere udtrykt stærke holdninger til logning og overvågning af medarbejdere, og de skulle derfor have haft lejlighed til at drøfte om SDU's måde at bedrive IT-sikkerhed på er proportional på forkant og ikke blot som en orientering efter implementering.

Mads understregede, at rettidig inddragelse af relevante fora og organer skal sikres fremadrettet. Dette noterer Bue Raun Andersen og Jacob-Steen Madsen og går i dialog med Thomas Buchvald Vind.

Bue Raun Andersen konkluderende, at Udvalget tiltræder indstillingen og den digitale organisation noterer opmærksomhedspunktet omkring forløbet.

5. Drøftelsespunkt: URIS' retningslinjer for internationalt forsknings- og innovationssamarbejde

Bue Raun Andersen introducerede punktet. Udvalg om retningslinjer for internationalt forskning- og innovationssamarbejde har udarbejdet retningslinjer for området, og disse får også udstrakt opmærksomhed på SDU. Bue opfordrede Udvalget til at drøfte i hvilket omfang, fakulteterne er bekendt med og har arbejdet med retningslinjerne. Udvalget bedes ligeledes drøfte eventuelle input til SDU's overordnede arbejde med/implementering af retningslinjerne.

Det varierer i hvilken udstrækning, der er arbejdet med retningslinjerne lokalt. Enkelte fakulteter har arbejdet indgående med retningslinjerne, mens andre har beskæftiget sig med dem på afgrænsede områder eller i begrænset omfang.

Udvalget fremhævede vigtigheden af ikke blot at forholde sig til eksterne samarbejder, men også den fysiske sikkerhed på SDU's lokationer, hvis risikoen for at uvedkommende får adgang til forskningsdata eller lignende skal mindskes. Udvalget drøftede flere forskellige initiativer; elektronisk dørlås, fysisk omplacering af medarbejdere som beskæftiger sig med særligt udsatte forskningsområder, screening af medarbejdere, awarenessaktiviteter mv.

Jacob-Steen Madsen bakkede op om Udvalgets drøftelser, men opfordrede til at dialogen omkring den fysiske sikkerhed på SDU sker i samråd med Teknisk Service. Bue Raun Andersen bakkede ligeledes op om Udvalgets drøftelser og opfordrede til, at særligt informationssikkerhedskoordinatorerne inddrages aktivt i awarenessaktiviteter, indtil SDU's målsætninger på området er nærmere fastlagt.

Flere af Udvalgets medlemmer udtrykte i forlængelse af ovennævnte drøftelser uklarhed omkring, i hvilket omfang SDU ønsker at følge retningslinjer, og hvordan de i praksis implementeres.

Bue Raun Andersen opsummerede, at SDU's ambitionsniveau på området skal endeligt fastlægges, førend Udvalget for informationssikkerhed og databeskyttelse kan bidrage med relevante databeskyttelses- og informationssikkerhedsmæssige tiltag. I mellemtiden fokuseres der på awarenessaktiviteter med inddragelse af GDPR- og informationssikkerhedskoordinatorkredsen.

6. Beslutningspunkt: Strategi for awarenessaktiviteter på SDU 2022/2023

Janni Lee B. Bang Brodersen rammesatte punktet. Udvalget tiltrådte i slutningen af 2021, at SDU Digital Compliance skulle udarbejde en strategi for awarenessaktiviteter på SDU. Strategien består af dels nogle strategiske målsætninger og dels nogle konkrete aktiviteter. Aktiviteterne består blandt andet af kompetenceudvikling målrettet de enkelte brugergrupper (VIP, TAP og studerende), phishingkampagner, plakater, muligheden for at bestille oplæg mv.

Udvalget udtrykte generel opbakning til den skitserede strategi og underliggende aktiviteter. Peder Thusgaard Ruhoff nævnte, at det centrale er, at de forskellige brugergrupper løbende bliver præsenteret for og mindet om vigtigheden af databeskyttelse og informationssikkerhed.

Bue Raun Andersen konkluderede, at strategien betragtes som godkendt, og at den vil blive udmøntet det kommende år.

7. Eventuelt

Ingen bemærkninger.