SDU Digital

Referat

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse	16. september 2021
Dato og tidspunkt:	16. september 2021 klokken 10-12	
Sted:	Teams	
Deltagere:	Bue Raun Andersen, Simon Kamber, Brian Truelsen, Jacob-Steen Madsen, Jesper Bo Nielsen, Peder Thusgaard Ruhoff, Martin Svensson, Rune Nørgaard Jørgensen og Mads Lildholdt	
Afbud fra:	Bjarne Nielsen og Jan I. Kristensen	
Referent:	Natalie Olsen	

Dagsorden:

1. Godkendelse af dagsorden og referat

Ingen bemærkninger.

2. Meddelelser

SDU's DPO, Simon Kamber, går på fædreorlov fra uge 42 frem til marts 2022. DeiC's DPO-tjeneste varetager DPO-opgaven i perioden.

SDU Digital, Compliance har påbegyndt arbejdet med udarbejdelse af en fortegnelse over SDU's behandlingsaktiviteter jf. databeskyttelsesforordningens artikel 30. Der arbejdes ud fra et udenlandsk rammeværk, som også indgår i SDU Digital, Transformations procesarbejde. Rammeværket er ved at blive oversat til en dansk universitetskontekst. Forventningen er, at arbejdet i første omgang resulterer i tredive overskrifter, som løbende skal udbygges og eller/uddybes i samarbejde med områder og fakulteter.

Simon Kamber gav en kort status på arbejdet med studerende og specialer. Der er udarbejdet et udkast til en politik, som skal konkretiseres i nogle retningslinjer. Projektet er ved at drøfte, hvordan SDU forholder sig i de situationer, hvor SDU enten overtager eller sammen med den studerende er dataansvarlig. Politikken bliver i nærmeste fremtid forelagt De Studerende i Centrum, hvorefter politikken forelægges Direktionen.

Udvalget er tidligere gjort opmærksom på potentielle konsekvenser af Brexit. EU-Kommissionen har afgjort, at Storbritannien kan betragtes som et sikkert tredjeland.

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

Bue Raun Andersen orienterede om, at der er en rekrutteringsproces i gang i SDU Digital, Compliance ift. CISO-funktionen og en afdelingsleder. Den nye informationssikkerhedschef tiltræder i november, og er dermed næste skridt i arbejdet mod at indfri de målsætninger der er besluttet i handleplanen.

Jacob-Steen Madsen orienterede om en konkret sag på Det Sundhedsvidenskabelige Fakultet, hvor en ph.d.-studerende har afinstalleret den software SDU IT benytter til håndtering af maskiner. Sagen er efter god dialog med den konkrete person og ledelsen på det konkrete institut håndteret.

Jacob-Steen Madsen orienterede om, at der er en SIEM-løsning på vej. Løsningen skal vha. algoritmer identificere adfærd som afviger fra normalen. Det giver en synlighed omkring hvilke trusler SDU står overfor, i hvilket omfang og derfor også mulighed for at imødegå dem. Simon Kamber understregede vigtigheden af, at de databeskyttelsesmæssige krav til løsningen bliver identificeret, dokumenteret og håndteret inden løsningen sættes i drift. Peder Thusgaard Ruhoff fremhævede i den forbindelse, at transparens omkring hvad systemet gør er central, for at brugerne ikke oplever det som overvågning. Jacob-Steen Madsen tager disse opmærksomhedspunkter til efterretning. SDU IT vil præsentere SIEM-løsningen på et kommende møde i Udvalget.

Jacob-Steen Madsen orienterede om MFA enforcement ved udlandsrejser. Trusselsbilledet nødvendiggjorde, at brugere ved udlandsrejser blev påkrævet at benytte MFA hvis man f.eks. skulle tilgå sin mail. SDU IT oplevede en smule support på baggrund heraf. Jesper Bo Nielsen fremhævede at COVID-19 situationen har begrænset rejseaktiviteten, men at sådanne ændringer fremadrettet må forventes at påvirke et større antal brugere.

Jacob-Steen Madsen orienterede om patch management, som har til hensigt at sikre at brugerne benytter de versioner af software de skal. SDU IT benytter patch management anledningsbaseret, hvilket betyder at brugerne udelukkende oplever, at de skal opdatere, når brugeren ønsker at benytte en forældet version af den givne software. Hvis brugeren blot har software installeret men ikke benytter det, vil brugeren ikke blive påvirket. Såfremt Udvalgets medlemmer bliver opmærksom på at brugerne oplevelser uhensigtsmæssigheder relateret til dette bedes de kontakte servicedesk.

Jacob-Steen Madsen orienterede om, at SDU's licens med AMP (virusbeskyttelse til Mac) udløber 1/11. SDU benytter i stedet ATP som virusbeskyttelse. Ændringen vil blive udrullet via Software Center eller ved direkte henvendelse til den enkelte bruger.

Bue Raun Andersen orienterede om, at en opdateret version af e-læringskurset er ved at blive flyttet til ItsLearning og at der i den forbindelse ligeledes er ved at blive sikret adgang til de studerende, der måtte have behov for det. Kurset vil i første omgang kun være tilgængeligt på dansk, men den engelske version forventes at følge snarest herefter. Der vil blive udsendt mere information herom.

Natalie Olsen gav en status på arbejdet med de nye sider om databeskyttelse og informationssikkerhed. Siderne er tilgængelige på sdunet.dk og mitsdu.dk, men organisationen modtager mere information herom i starten af næste uge.

Bue Raun Andersen henledte opmærksomheden til DPO, Simon Kambers notat omkring databeskyttelse i forbindelse med uniTEST. I forbindelse med uniTEST 2022 er man opmærksom på tidligt at få gjort sig de rette databeskyttelsesmæssige overvejelser.

Bue Raun Andersen orienterede om at GDPR- og informationssikkerhedskoordinatorrollen er ved at blive evalueret som led i årsrapporten om arbejdet med databeskyttelse og informationssikkerhed på SDU. SDU Digital, Compliance har udsendt et spørgeskema, og der vil efterfølgende være en dialog omkring hvilke erfaringer man har gjort sig.

Bue Raun Andersen orienterede om at næste møde i Udvalget afholdes fysisk på campus. Mødeindkaldelsen vil blive opdateret.

Jacob-Steen Madsen gav en kort status på lokaladministratorrettigheder, som Udvalget besluttede skulle være ens på hele SDU. Der mangler fortsat 70 maskiner på TEK, og en del maskiner på SAMF. Arbejder skrider frem, og der opleves ingen udfordringer.

Jacob-Steen Madsen orienterede om, at der fortsat afvikles test af en MAM-WE løsning. SDU Digital vil i den kommende uge teste den nye løsning, og test udbredes efterfølgende til VIP-personale.

Jacob-Steen Madsen orienterede om, at SDU IT og SDU RIO i fællesskab kigger på processen omkring indgåelse af databehandleraftaler ved indkøb af nyt software. Konkret betyder det, at de personer som er tæt på denne proces mødes én gang om ugen for at sikre at brugerne oplever en hurtig og smidig proces.

3. Orienteringspunkt: IT-beredskab

Jacob-Steen Madsen rammesatte punktet, og fremhævede at den digitale organisation har vurderet, at der er behov for at kigge på IT-beredskabet. Det har resulteret i, at der er etableret en mere systematisk fremgangsmåde end hidtil; beskrivelse af hvad der skete, hvordan det blev løst og hvordan det kan forhindres at lignende sker fremadrettet. Denne fremgangsmåde benyttes i alle beredskabssituationer – som f.eks. netværksnedbrud eller tabet af den engelske version af SDU's hjemmesider. Brian Truelsen indfører denne dokumentation i SDU's ISMS.

Jesper Bo Nielsen efterspurgte mere synlighed og transparens omkring hvilke beredskabstiltag SDU IT tager. Rune Nørgaard Jørgensen foreslog, at det kunne være noget materiale lig den månedsopdatering Det Humanistiske Fakultet har modtaget. Udvalget var enige i Jesper og Runes betragtninger, men understregede at det i den forbindelse er vigtigt, at der er knyttet lidt flere ord til kommunikationen omkring beredskabshændelserne, og at denne information udsendes via. linjeledelsen.

Den digitale organisation tager Udvalgets betragtninger til efterretning og indarbejder den i det videre arbejde med IT-beredskabet.

4. **Drøftelsespunkt: Handling på baggrund af trusselsvurderinger fra FE og PET**

Bue Raun Andersen introducerede punktet, ved at henlede Udvalgets opmærksomhed på, at Udvalget tidligere har behandlet PET-rapporten "Er jeres forskning i fare?", men at der siden da er kommet en ny trusselsvurdering fra Forsvarets Efterretningstjeneste. Bue fremhævede enkelte centrale konklusioner i de to rapporter.

Bue fremhævede, at nogle trusler kan håndteres teknisk, mens andre skal adresseres på anden vis. Universitetsdirektør, Thomas Buchvald Vind, har bedt Udvalget drøfte konkrete ting SDU kan iværksætte for at imødegå de trusler som blandt andet PET og FE har identificeret.

Rune Nørgaard Jørgensen foreslog et pixi-oplæg med information om sikkerhed; hvad er udfordringerne, og hvad kan jeg selv gøre, som enhver med grundlæggende indsigt i sikkerhed kan præsentere for sit lokalmiljø. Udvalget bakkede op om forslaget, og påpegede i den forbindelse, at SDU bør trække på interne kompetencer som besidder en særlig viden eller teknisk kunnen på området (eksempelvis kontrolleret hacking af SDU's systemer).

Mads Lildholdt og Martin Svensson gjorde desuden opmærksom på, at det i den forbindelse er vigtigt, at brugerne ved henvendelse til servicedesk om konkrete brud/sårbarheder, oplever at henvendelsen bliver taget alvorligt.

Bue Raun Andersen opsummerede, at Udvalget har taget indholdet i de to rapporter til efterretning. SDU Digital, Compliance (inkl. ny CISO) går i dialog med SDU IT omkring konkrete handlinger for at imødegå det skitserede trusselsbillede. Den digitale organisation tager Udvalget forslag/betragtninger omkring et pixi-præsentation, brugen af interne kompetencer på SDU og at brugerne skal opleve at blive taget alvorligt, når de henvender sig om sårbarheder/brud med i det videre arbejde.

5. **Beslutningspunkt: Fjernelse af private enheder fra SDU's Azure AD miljø**

Jacob-Steen Madsen introducerede punktet inkl. at IT-service i 2019 konstaterede at privat udstyr aktivt kunne indmeldes på SDU's AD. Dette er ikke længere en mulighed, men der er fortsat cirka 50 maskiner som er indrullet på SDU's AD, og det udgør en sikkerhedsmæssig udfordring.

Udvalget udtrykte bekymring for om det er hensigtsmæssigt at følge den kommunikationsplan der er foreslået i indstillingen - opgaven bør i stedet afleveres – og til dels løses – via. medlemmerne af Udvalget. Simon Kamber opfordrede i den forbindelse Udvalget til at indtænkte informationssikkerhedskoordinatorerne i opgaveløsningen jf. rollebeskrivelserne i SDU's arbejde med informationssikkerhed og databeskyttelse.

Bue Raun Andersen opsummerende at begge perspektiver bør afspejles, og at opgaven i den konkrete sag sendes til medlemmerne af Udvalget, som inddrager den lokale koordinator i opgaveløsningen. På sigt er det hensigten at Udvalget ikke agerer operationelt, men at denne opgave i stedet varetages af informationssikkerhedskoordinatorerne.

6. Beslutningspunkt: Password længde på SDU

Jacob-Steen Madsen introducerede indstillingen. MFA benyttes mange steder, men nogle steder i SDU's infrastruktur er det på nuværende tidspunkt ikke muligt at benytte MFA, og brugerne er derfor nødsaget til at bruge password. Svage passwords udgør en angrebsvektor, og SDU IT indstiller derfor til, at længden på password på SDU øges fra 12 til 14 tegn for at mindske risikoen for vellykkede eksterne angreb. Brugerne vil udelukkende mærke denne ændring, når og hvis de af forskellige årsager selv skifter password. Brugere som ikke af sig selv skifter password vil ikke blive berørt. SDU IT vurderer derfor at påvirkningsgraden for den enkelte bruger er meget lille, samtidig med at SDU høster rimelige sikkerhedsmæssige gevinster.

Udvalget tilslutter sig indstillingen, men opfordrer samtidig SDU IT til at være opmærksomme på at password længden ikke blot øges gradvist over tid. Jacob-Steen Madsen påpegede i den forbindelse, at dette er en nødvendighed så længe alle systemer ikke er underlagt MFA eller application firewall. Bue Raun Andersen spurgte i den forbindelse om password managers kunne være en måde at imødegå denne problemstilling på. SDU IT tager Udvalgets bemærkninger til efterretning.

Bue Raun Andersen opsummerede, at Udvalget tiltræder indstillingen, men at der bør være en generel opmærksomhed på ikke blot at øge password længden gradvist over tid, da brugerne i så fald finder andre måder, hvorpå sikkerhedsforanstaltningerne kan omgås.

7. Drøftelsespunkt: Rapport om arbejdet med databeskyttelse og informationssikkerhed på SDU

Bue Raun Andersen indledte punktet med at takke Udvalget for input til årsrapport om arbejdet med informationssikkerhed og databeskyttelse på SDU drøftet på seneste møde. SDU Digital, Compliance har udarbejdet et udkast til en struktur, som Udvalget bedes forholde sig til. Udvalget havde ingen bemærkninger. Udvalget vil blive præsenteret for første udkast af rapporten på næstkommende møde.

8. Eventuelt

Martin Svensson oplever frustration over meddelelse øverst i mails som fremhæver, at man sjældent modtager mails fra den pågældende afsender. Brugere oplever at meddelelsen forhindrer dem i at læse første del af mailen fra deres telefon. Jacob-Steen Madsen understregede, at hensigten med meddelelsen er at hjælpe brugeren med at identificere eventuelle phishing-mails – mails som SDU i skrivende stund modtager mange af.

Andre medlemmer af Udvalget har ikke oplevet disse udfordringer. Jacob-Steen Madsen tager med tilbage, at der er behov for at få afklaret om enkeltpersoner kan slå denne funktion fra, at få blotlagt algoritmen bag løsningen og at SDU IT skal blive bedre til at kommunikere formålet de sikkerhedstiltag, der sættes i værk.