SDU Digital

Referat

25. maj 2023

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse
Dato og tidspunkt:	2023-05-25 kl. 10:30-12:00
Sted:	O SAM Mødelokale H
Deltagere:	Bue Raun Andersen, Jacob-Steen Madsen, Jan I. Kristensen, Mads Lildholdt (ankom under pkt. 2), Rune Nørgaard Jørgensen, Peder Thusgaard Ruhoff, Martin Svensson, Jesper Bo Nielsen, Bjarne Nielsen, Simon Kamber og Janni Lee B. Bang Brodersen
Referent:	Brian Truelsen

Dagsorden:

1. **Godkendelse af dagsorden og referat**

   Ingen bemærkninger.

2. **Meddelelser**

   Bue Raun Andersen gav en orientering på Rigsrevisionens planlagte opfølgningen på deres rapport fra 2020 om tilsyn af SDU's beskyttelse af forskningsdata. Rigsrevisionen har efter planen set bort fra de punkter, der endte som grønne i den oprindelige rapport. Nu har SDU to grønne og to gule punkter. Den ene gule handler om anvendelsen af lokaladministratorer på slutbrugermaskiner. Mac-udstyr er en udfordring at komme helt i mål med. Den anden gule anmærkning handler om muligheden for at tilslutte ukendt udstyr til vores fysiske netværk. Her arbejder SDU IT stadig på udrulning af 802.1x, hvor man regner med at komme i mål indenfor 2-4 år. Der er stor udvikling på de danske universiteter som helhed. Jacob-Steen Madsen er meget tilfreds med processen og anerkender Rigsrevisionen for deres professionelle tilgang til opgaven.

   Jacob-Steen Madsen gav en orientering om udfordringen med, at Microsoft Exchange er designet således, at det er den enkelt mailklient (fx Outlook Kalender, Apple Mail, Evolution) der skal sikre, at kalender-poster, som har privat-flaget sat, ikke bliver fremvist med alle detaljer. En bruger har ved et tilfælde opdaget, at det er muligt at se, at kollegaer har skjulte aftaler ved at søge efter stikord. Brugeren kan ikke se indholdet; kun at der er en aftale. Alle informationer bliver overført fra Exchange til mail-programmet, og der skal onde hensigter

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

til, for at kunne finde de private informationer i mail-programmets cache. Der er lavet en stor afsøgning af problemstillingen, der også er blevet forelagt direktøren. Vi skal måske via en policy have indskærpet, at man ikke må gennemsøge sin cache. SDU IT kommer ikke til at godkende mail-programmer, der ikke understøtter privat-flaget. Janni kunne oplyse, at it-retningslinjerne allerede understøtter sådan en policy.

Jacob-Steen Madsen oplyste i forhold til systemforvalteraftaler på forskerservere, at lister med allerede indsamlede informationer er blevet delt i forskningsmiljøet for at få kvalificeret, at om det er de rigtige servernavne og de rigtige systemejere. Der mangler stadig en del information, men man er rigtigt langt. Det er allerede et godt udgangspunkt. Efter sommerferien begynder SDU IT at kontakte systemejerne direkte.

Jacob-Steen Madsen orienterede om, at Team Sikkerhed har besluttet, at SDU IT kommer til at spærre for opslag i DNS for de to nye toplevel-domæner (TLD), ZIP og MOV af hensyn til it-sikkerheden. Det er første gang SDU IT gør det. Udfordringen er, at Windows ikke kan skelne mellem, om .zip er slutningen på et domæne eller slutningen af en fil.

Janni Lee B. Bang Brodersen orienterede om CFCS har udgivet nye trusselsvurderinger, der er uændrede siden de i forbindelse med Ruslands invasion af Ukraine hævede truslen i relation til Cyberaktivisme til Høj. Desuden anbefales det, at kodeord har en minimumslængde på 15 tegn.

Bue Raun Andersen orienterede om, at Årsrapporten har været fremlagt til orientering i Direktionen, hvor den blev taget til efterretning. Samtidigt blev DPO'ens uafhængige beretning og rapporten over phishingkampagnen behandlet. Direktionen viste særlig interesse for sidstnævnte, og direktøren ville gerne såfremt det gav mening have en endnu højere kadence på fremtidige kampagner.

Bue Raun Andersen annoncerede, at der vil blive fundet en ny dato for næste møde.

Jacob-Steen Madsen orienterede om 2 af de fire hændelser, som var vedlagt dagsordenen.
I forbindelse med TBO har det vist sig at være endnu mere nødvendigt at teste setuppet, selvom der allerede var gjort store bestræbelser for at undgå udfordringer.

Og endelig var der en sag, hvor en menneskelig fejl gjorde, at man mistede login-adgang til alle servere. Det lykkedes ret hurtigt at genetablere de fleste adgange, men der var nogle stykker, som krævede en ekstra indsats.

3. Revidering af informationssikkerhedshåndbogen

Janni orienterede om arbejdet med revidering om informationssikkerhedshåndbogen. Bogen var sidst hos direktøren i 2021. Udvalget ejer og godkender, men bogen forelægges direktionen til orientering. Bogen har været i høring hos SDU IT, SDU RIO, eScience Centeret og i uddrag hos Teknisk Service. Informationssikkerhedshåndbogen er en del af arbejdet med ISO 27001, som universiteterne er anbefalet at følge. Håndbogen har været under en større revidering og vil først ved næste revidering følge ISO 27001:2022. Det skyldes, at standarden først sent i forløbet udkom på dansk, men at det også viste sig, at springet ville være for stort. Håndbogen skal ideelt indeholde regler eller principper for arbejdet med informationssikkerhed, der kan udmøntes i retningslinjer og procedurer. Af historiske årsager er der mange konkrete retningslinjer og procedurer i håndbogen. Det har været nødvendigt at bibeholde en del af disse, da der på flere områder ikke er andre ledelsesgodkendte retningslinjer.
Flere af udvalgets medlemmer gav udtryk for, at det er svært at forholde sig til så stort dokument indenfor den fastsatte tidsramme. Der blev efterlyst en indledende læsevejledning, så væsentlige ændringer fremgik. Udvalget drøftede håndbogens omfang og indhold og besluttede at udsætte godkendelsen, da Martin havde nogle konkrete forslag til præciseringer og ændringer. Det blev derfor besluttet at holde et opfølgende bilateralt møde med Martin, hvorefter håndbogen sendes til skriftlig godkendelse ved alle udvalgets medlemmer.
Derudover drøftede udvalget behovet for særskilte brugerrettede retningslinjer og kommunikation heraf herunder at flere afsnit på sigt kan tages ud af håndbogen, særligt ordlisten og specifikke procedurer (fx længde af password), der kan sikre en mere agil opdatering.
Ligeledes blev der opfordret til, at der i kommende sagsfremstillinger til udvalget blev henvist til relevante afsnit i Informationssikkerhedshåndbogen, så den også for udvalget får en mere praktisk anvendelse.

Bue sammenfatter, at håndbogen aldrig har været tænkt som et folkeligt værk, men institutionen skal forholde sig til den. Vi skal have lavet noget brugerrettet, og at det er et stort skridt i retning af noget, som er meget bedre. Vi laver en skriftlig rundsending og laver godkendelse per e-mail.

Janni Lee B. Bang Brodersen fremlagde punktet.
Hun fremførte behovet på baggrund af flere EU-domme og krav til

4.	**Microsoft Task Force**	dokumentation og risikovurdering af alt væsentligt, som vi anvender. Taskforcen har kortlagt, hvilke produkter vi har implementeret, og dokumentationen fylder aktuelt mere end 150 side. Normalt er det systemejeren, der godkender risikovurderinger, men fordi anvendelse af Microsoft og cloud har betydning for universitetets digitale ambitioner, lægges det op til Direktionen at fastlægge SDU's risikoappetit. Udvalget drøftede den videre proces bl.a. hvordan, der kan ske relevant inddragelse af repræsentanter for de registrerede. Udvalget var enige om, at det formentlig ikke ville give værdi at rundsende så stort et materiale. Simon gav udtryk for, at man kunne fokusere på overvågning af medarbejdere i stedet for at involvere i hele SharePoint eller de tekniske opsætninger. Mads mener, at det vil give mening med et executive summary af de enkelte kapitler, og holde diskussionen på det, som giver mening. Der var enighed om, at HSU kan høres som repræsentanter for de registrerede og repræsentanter for de studerende passende kunne være de studerende, der er valgt ind i SDU's bestyrelse.
5.	**Lukket punkt**	
6.	**TikTok**	Jacob-Steen Madsen formidlede, at han var blevet bedt af udvalget om at lave en indstilling til direktionen omkring TikTok. Rektoratet træf selv beslutningen på baggrund af indstillingen og orienterede direktionen efterfølgende.
7.	**Eventuelt**	Intet.