SDU Digital

Referat

14. september 2023

BT

truelsen@sdu.dk
T +4565503542
M +4560113542

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse
Dato og tidspunkt:	2023-09-14 kl. 11-13
Sted:	O HUM IKV Romeo
Deltagere:	Bue Raun Andersen, Jacob-Steen Madsen, Peder Thusgaard Ruhoff, Rune Nørgaard Jørgensen, Bjarne Nielsen, Jesper Bo Jensen, Martin Svensson. *Observatører: Janni Lee B. Bang Brodersen, Simon Kamber*
Afbud fra:	Mads Lildholdt, Jan I. Kristensen
Referent:	Brian Truelsen

Dagsorden:

1. **Godkendelse af dagsorden og referat** — Ingen bemærkninger.
2. **Meddelelser** — Informationssikkerhedspolitikken er godkendt af direktøren med informationssikkerhedshåndbogen som bilag på vegne af direktionen.

   MS taskforce. Fremlagt af Janni. Taskforcen blev etableret for at tilvejebringe den manglende dokumentation for vores anvendelse af Microsofts produkter. Der er aftalt et forløb med direktøren med henblik på høring af ansatte gennem HSU.
   Blandt de studerende forventes man at inddrage studenterrepræsentanterne i universitetsrådet.
   Der vil blive lavet en udvidet oplysningsskrivelse om hvad der bliver delt med Microsoft i arbejdsmedfør.

   Chromebooksagen. Formentlig har Data Privacy Framework (se punkt 3) udsat Datatilsynets udmelding.

   URIS. Forankret i rektorsekretariatet men bør have bevågenhed i UID. Uddannelses- og Forskningsministeriet har været på tilsyn på SDU. Der var umiddelbart tilfredshed med SDU's tilgang.

   Stillingsopslag af CSO (chief security officer) forankret i

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

rektorsekretariatet med fokus på URIS. Mads Niemann-Christensen er ansat med start 1/10-23. Fokus er udadrettet imod fakulteter og forskningslag.
Relationen til UID skal afklares?

MAM-we: Var i HSU før sommerferien. Vedtaget at det kører videre på resten af SDU. SDU IT vil være helt sikker på en ordentlig udrulning. Først ADM, så HUM, SAM, siden SUND, og til sidst TEK og NAT fordi der forventes lidt udfordringer der. Løber hen over det næste halve år.
Der blev stillet forslag om en FAQ over de f.eks. 10 mest almindelige spørgsmål.

AI: Projekt i regi af uddannelsesrådet. Mange bruger det allerede i det daglige. Bevågenhed omkring databeskyttelse. Fokus også på det administrative område. Anskaffelse af enterprise-udgave af ChatGPT, som ikke træner på input undersøges. Bruges allerede godt og konstruktivt.
I forhold til uddannelsesområdet blev der spurgt ind til håndtering af AI som hjælpemiddel. I regis af Uddannelsesrådet kommer der en udmelding for den kommende eksamensperiode, mens der er nedsat et projekt, der bl.a. vurderer det længere perspektiv.

Beredskabsøvelser:
Større koncept. IT vil blive en del af en samlet fælles beredskabsøvelse, der involverer flere områder.

Hændelser. 5 stk. Ingen alvorlige.
2a. Adgang til data i zExpense. Positivt med hændelsen, da det gav anledning til oprydning.
2b. Cloud. Udenfor vores kontrol. Sdu.dk, sdunet.dk, mitsdu.dk ligger ude hos Azure, og fejl hos MS vil bare give os problemer.
2d. Generatornedbrud. Øgning af udskiftningsfrekvens.

3. EU-U.S. Data Privacy Framework.

Janni fremlægger i Jans fravær.

Martin spørger til forskellen mellem Google og Microsoft fordi mange af hans kollegaer benytter Google.
Janni svarede at vi har aftale med Microsoft, ikke med Google. Man er strafferetlig forpligtet til at overholde de regler, som vi er underlagt (GDPR, databehandleraftaler, m.fl.).

4. DKCERT Trendrapport,

Janni fremlægger.
Trendrapporten indeholder information om, at universi-

NIS2, publikationen "Er jeres forskning i fare?"

tetssektoren og Absalon har været ramt af vellykkede hackerangreb ligesom man har været udsat for DoS-angreb (serviceafbrydelse).

SDU IT og SDU Digital tager observationerne med i strategisk planlægning og man har allerede initiativer i gang.

Publikationen "Er din forskning i fare?" er blevet opdateret bl.a. omkring droneteknologi.

Direktivet NIS2 træder i kraft fra 18. oktober 2024. Universiteterne er ikke direkte omfattet. SDU bliver indirekte omfattet, hvis man fx har HPC-anlæg. Hvis man er omfattet, er det et krav, at man anvender et anerkendt framework fx ISO 27000. Der er formaliseret bøder i direktiver som de kendes fra GDPR, men der er kortere reaktionstid til at indberette hændelser.

Jesper spørger til, om dette har konsekvenser for den enkelte bruger, hvortil Janni svarer, at man kun er berørt, hvis han laver produkter, som bliver omfattet. Fx er Retsmedicin meldt ind som en samfundsvigtig funktion, som nok gør, at de bliver omfattet. Jesper bemærker, at der ligger en oplysningsopgave her.

Bue afrunder punktet ved at bemærke, at der skal foretages en afklaring i forhold til scopet, og hvor meget der skal kommunikeres ud i organisationen.

5. Rejsevejledning.

Rejsevejledningen er forfattet af SDU IT og SDU Digital i samarbejde efter aftale med direktøren.
URIS nævner en håndfuld lande, som man skal have bevidsthed om, hvis man rejser dertil.

Janni bemærker, at dette "kun" en vejledning og spørger udvalget om en diskussion af, hvorvidt vejledningen kan eller skal ophøjes til en retningslinje?

Bue oplyser undervejs, at URIS ikke bare lægger op til retningslinjer, men også konsekvens, hvis nogen bryder retningslinjen.

Martin mener ikke, at det er nødvendigt at gøre det til en retningslinje. Den enkelte forsker ved selv, hvad denne har af fortrolige ting. Det er institutlederens opgave at kende til vejledningen og tage dialogen med sine forskere.

URIS-rapporten har fokus på rejser til meget specifikke lande. Man kender ikke til sager ved SDU, hvor der er blevet stjålet oplysninger ved rejser til disse lande, men efterretningsopgørelser tilsiger at det sker i stor stil.

Rune og Martin efterlyser mere oplysning end blot at lægge en nyhed på SDUnet. Han kender ikke til nogen lektorer, som ved, at der findes en rejsevejledning.

Rune foreslår, at man laver en flagløsning i CWT som helt naturligt ville skabe synliggørelse af eksistensen af en rejsevejledning. Bue bakker op.

Janni lægger op til, at der laves retningslinje, hvor institutlederen er forpligtet til at tage dialogen med forskeren.

Jacob bemærker, at SDU IT tilbyder Always-on VPN, som sikrer at al trafik går igennem VPN.

Peder udfordrer generelt, at det er alt for let at gå ind i forskningsmiljøer og uhindret sætte en USB-stik i en computer i ond hensigt.

Jacob oplyser, at SDU IT betragter vores interne netværk som usikkert og derfor har vi meget aktivt overvågning. Det kan vi ikke gøre lige så meget på folks rejse.

Janni lovede at Compliance vil tage snakken med Rektorsekretariatets koordinator omkring muligheden for at sætte et kritisk øje på rengøringspersonalets muligheder.

Bue sammenfatter omkring rejsevejledningen, at der er behov for øget generel awareness i et sprog der er rettet til brugerne. Anbefaling til direktion om en blød retningslinje, som forpligter ledelsen ved institutterne.

Jacob orienterede.

6. Forvaltningsaftaler.

Aftaleformularen er blevet rimeligt opdateret og overblik er etableret i forhold til tidligere behandlet materiale. Jens Svalgaard Kohrt kommer til at føre opgaven videre.

Forskerserverne skal også lægges bag WAF (Web Application Firewall).
Opgaven har svært ved at skalere fordi det er rigtigt vanskeligt at få lavet aftale med forskere. Det er tungt for alle parter.

Udvalget drøftede diverse udfordringer.

Bue sammenfattede med, at udvalget ikke ser noget problem i at vende processen om således at det er forskeren/underviserens kalender, at der styrer, hvornår omlægning kan ske, så længe at 2 uger må være det rette tidsomfang. Det er vigtigt at starte småt for at se, hvad der sker.

Kris fra SDU IT, SecOps Team fremførte sin præsentation.

7. Den aktuelle trusselsituation

Stigning mod uddannelsessektoren.
Udstilling af nødvendigheden for at SPF, DKIM, DMARC er sat rigtigt op hele vejen rundt, hvilket også er den del af de statslige minimumskrav.

Tak for nu.

8. Eventuelt