SDU IT

Referat

Emne:	Møde i Udvalget for informationssikkerhed og databeskyttelse
Dato og tidspunkt:	2026-03-02 kl. 13-15
Sted:	O HUM IKV-Romeo (Ø18-307-2)
Deltagere:	Bue Raun Andersen, Janni Lee B. Bang Brodersen, Mads Niemann-Christensen, Peder Thusgaard Ruhoff, Martin Svensson, Rune Nørgaard Jørgensen, Morten Hulvej Rod, Christian Hurup Spile
Afbud fra:	Jan I. Kristensen, Simon Kamber
Referent:	Brian Truelsen

3. februar 2026

Sagsnr. UID 30
BT

truelsen@sdu.dk
T +4565503542
M +4560113542

Dagsorden:

1. Indledende punkter	1.1 **Godkendelse af dagsorden for mødet** 1.2 **Godkendelse af referat fra sidst** Bilag: referat. 1.3 **Kort nyt** 1.4 **Hændelsesrapporter** Ingen
2. Godkendelser	2.1 **Årsberetning** SDU IT laver hvert år en beretning om arbejdet med databeskyttelse og informationssikkerhed. Beretningen laves for UID med henblik på forelæggelse for direktionen. SDU IT har fået input fra SDU SAFE og SDU RIO. Bilag: Indstilling. Bilag: Årsberetning.
3. Orientering	3.1 **DPO'en årsrapport** SDU's databeskyttelsesrådgiver (DPO) forfatter årligt en rapport over de vigtigste nedslagsområder, som DPO'ens arbejde har givet anledning til i løbet af året. Bilag: Indstilling. Bilag: DPO'ens årsrapport.

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

	3.2 **Redegørelse for cyber- og informationssikkerhedsarbejdet på SDU** DCIS-UFM har anmodet universiteterne om en redegørelse for cyber- og informationssikkerhedsarbejdet i relation til universiteternes arbejde med at implementere NIS 2. SDU har ligesom AU, KU og DTU vurderet, at universitetet har aktiviteter, der gør os omfattet af NIS 2. Bilag: Indstilling. Bilag: Redegørelsen. 3.3 **Afrapportering af phishingkampagne efterår 2025** Efterårets kampagne endte med at kun 1,4%, svarende til 129 brugere, afleverede brugernavne og kodeord. Det er et meget bedre resultat end tidligere, og skyldes nok, at kampagnen var for åbenlys, fordi den falske phishing-mail blev sendt fra en Google Mail-adresse. Bilag: Indstilling. Bilag: Phishingrapport.
4. Evt.	

1. **Indledende punkter**

1.1 **Dagsorden godkendt**.

1.2 **Referat godkendt**.

1.3 **Kort nyt**.

- Velkommen til Christian Hurup Spile fra SAM.
- SAMSIK er kommet med en rapport om Cybersikkerhed i Danmark.
  Det hurtige take-away er, at truslerne udvikler sig hurtigt og komplekst.
- SDU er fremadrettet forpligtet til at rapportere om implementeringen af URIS-anbefalingerne på linje med SDU's rammekontrakt. SDU SAFE koordinerer indsatsen.
- Opdatering på punktet fra sidste møde omkring tunnelmail. SDU IT har været i dialog med SUND og Regional IT i forhold til at finde en løsning på problemerne med automatisk viderestilling. Det er ikke på nuværende tidspunkt muligt at lave en teknisk løsning i forhold til at Regionens og SDU's M365 miljø kan kobles bedre sammen. SDU IT genbesøger beslutningen i forhold til automatisk viderestilling af mails.

1.4 **Ingen nye hændelsesrapporter**.

- Der havde dog været et brud på persondatasikkerheden, som gav pressebevågenhed. Denne blev der kort orienteret omkring.

2.1 **Årsberetning**.

Vil blive forelagt direktionen evt. i tilrettet udgave primært af layoutmæssig karakter.
Udvalget udtrykte tilfredshed med formatet.
Dokumentet er fortroligt og SDU IT laver noget brugervendt ud fra indholdet.
Det er noget modenhed og risikovurderinger, som gør dokumentet fortroligt.

Det drøftes om årsberetningen med fordel også kan deles i ALT. CIO drøfter dette med direktøren.
Der blev igen spurgt til udsigterne til at bruge OpenSource på desktoppen.
CIO svarer: Vi er dybt afhængig af MS. En ændring vil være et omkostningsfuldt, langvarigt forløb. Sandsynligheden for at BigTech lukker for vores adgang vurderes fortsat til at være lav, men CIO's på tværs af universiteterne arbejder på at genbesøge problemstillingen efter den seneste udvikling. SDU kommer formentlig ikke til at lave et fuldt alternativt setup, men vi kommer til at arbejde mere med driftskontinuitet f.eks. sikre, at vi har backup af vores data, og at de kan genindlæses i et M365-uafhængigt miljø.

3.1 **DPO'ens årsrapport**.
DPO'en kunne ikke deltage på mødet, men modtager gerne konkrete henvendelser.
SUND genkender DPO'ens pointe omkring koordinering af kampagner. SUND vil gerne have DPO'en forbi institutledermødet på fakultet. Myndighedsarbejdet i Sundhedsstyrelsen har også fokus på udfordringen.
Der blev spurgt til, hvem i så fald der skal have opgaven omkring koordinering?
SUND vil gerne med i loopet, hvis der sker noget på området.
Direktionen får rapport til orientering sammen med årsberetningen.
Taget til efterretning.

3.2 **Redegørelse til ministerium**.
CISO orienterer.
SDU har fokus på at øge modenheden på informationssikkerhed generelt fordi det ikke giver mening kun at beskytte isolerede systemer, der er direkte NIS 2 omfattede. Udgangspunktet er, at hele SDU er omfattet af NIS 2. Der vil blive tale om en risikobaseret implementering.
Det er en udfordring, at vi er omfattet per aktivitet, som hører under hvert sit ressort, da vi vil blive mødt med ikke koordinerede tilsyn. Hvis ministeriet omfattede sektoren, ville de som sektoransvarlig myndighed skulle koordinere eventuelle tilsyn fra andre ministerområder.

3.3 **Phishingkampagnen**.
CISO orienterer.
Det er tydeligt at resultatet afhænger af kampagnens udformning.
Det stilles forslag til, om resultatet kan deles op imellem VIP og TAP. Kunne man forestille sig at differentiere hyppigheden i forskellige grupper?
Under phishingkampagnen havde Mac'erne ved HUM ikke nogen "Rapportér phishing"-knap. Det er en udfordring at lave vejledning til funktionalitet som Microsoft ændrer i.

Intet.

Med venlig hilsen

Brian Truelsen
GRC-konsulent