

Referat

Emne: Møde i Udvalg for informationssikkerhed og databeskyttelse
Dato og tidspunkt: 2023-12-19 kl. 12:30 – 14:30
Sted: OD Sapphire
Deltagere: Bue Raun Andersen, Janni Lee B. Bang Brodersen, Mads Lildholdt, Martin Svensson, Jan I. Kristensen, Jesper Bo Nielsen, Mads Niemann-Christensen, Simon Kamber, Bjarne Nielsen, Jacob-Steen Madsen, Rune Nørgaard Jørgensen.
Afbud fra: Peder Thusgaard Ruhoff
Referent: Brian Truelsen
Dagsorden sendt til orientering til: UID

19. december 2023

Sagsnr. UID 20
BTtruelsen@sdu.dk
T +4565503542
M +4560113542

Dagsorden:

- 1. Godkendelse af dagsorden og referat**

Bue Raun Andersen konstaterede at dagsorden og referat er godkendt.
- 2. Meddelelser**

Janni Lee B. Bang Brodersen orienterede omkring status på taskforce omkring SDU's anvendelse af Microsoft-produkter. Den ligger i høring i en underarbejdsgruppe i HSU og bliver til en direktionssag senere.

Jacob-Steen Madsen orienterede om, at SDU IT arbejder på at bringe compliance af SDU's Mac'er op på samme niveau som Windows-computere inklusive passwordless login. Man er ikke begyndt at kigge på Linux endnu. Der er 9 faktorer, som skal være opfyldt for at udstyr er compliant.

Jacob orienterede om, at SDU IT styrker device-teamet, så man bedre kan følge med Microsofts forandringstakt.

Jacob kunne oplyse, at den finansielle it-revision forløb uden anmærkninger.

Jacob kunne oplyse, at man næsten er kommet op på 1000 websites, som er kommet bag F5.

Janni orienterede om sektorberedskabsøvelsen.

Bjarne Nielsen træder ud af udvalget i forbindelse med pensionering. Bue takkede Bjarne for deltagelse og bidrag i udvalget.

- 3. Orienteringspunkt:** Mads Niemann-Christensen orienterede om sin organisatoriske indlejring og funktion. Mads er i sin funktion af CSO for SDU, observatør i udvalget.

Velkommen til Mads Niemann-Christensen Mads har statusmøder med Janni, CISO, hver 14. dag. Der er nedsat en URIS-gruppe, som blandt andet skal definere, hvad kritikalitet betyder for SDU, samt sikre et tættere samarbejde mellem de enheder, som naturligt beskæftiger sig med sikkerhed ved SDU. URIS-arbejdet understøttes af en *ad hoc*-gruppe under Danske Universiteter. Mads sidder også med i FIKS, Forum for International Koordinering og Samarbejde. Noget af det første Mads har lavet er retningslinjer for, hvem der skal sikkerhedsgodkendes ved SDU. Ledelsesniveau 1 skal sikkerhedsgodkendes, og andre kan sikkerhedsgodkendes efter en konkret vurdering af behovet.
- 4. Orienteringspunkt:** Jacob gennemgik omstændighederne omkring strømnedbruddet den 15. november. En væsentlig læring er, at Telenors mobilnet ikke kan holde til, at alle aktiverer deres hotspots på mobiltelefoner for at få netværksforbindelse. Nogle bestemte medarbejdere har efterfølgende fået prioriterede mobilnumre (som sikres forbindelse selvom mobilnettet er overbelastet). Alt cloudbaseret virkede, hvis man ellers havde forbindelse, og det er vurderingen at mindst 90% kunne arbejde videre, særligt hvis de arbejdede hjemmefra. Der var også en læring om, at den operationelle krisestab (som ikke er it-beredskabet) måske skulle træde hurtigere sammen i sådan en situation. Alt nødstrøm bliver serviceret og testet som planlagt, og situationen kunne have været opstået ved næste, planlagte test. Den beredskabsansvarlige ved Teknisk Service, Claus Lund, skal undersøge, hvilke personer, der skal underrettes fakultært, og hvordan man ellers kommer kommunikativt ud i organisationen. Overordnet læring: Det er så ekstremt vigtigt, at afholde beredskabsøvelser.

Orientering omkring beredskabsøvelse og hændelsen den 15. november 2023
- 5. Drøftelse/beslutning** Jacob oplyste, at lokaladministrator-muligheden ikke bliver brugt ret meget, og der ikke er nogen grund til, at den er der.

Standardiseret PC til TAP uden administrative rettigheder Mads NC mener, at det er relevant at drøfte VIP'ers adgang til administrative rettigheder. Rune Nørgaard Jørgensen mener som udgangspunkt ikke,

at vi skal sondre mellem TAP og VIP, hvortil Jacob oplyser, at TAP'er har adgang til administrative informationer, og at det er en vurdering af, hvad man kan komme igennem med at ændringer på nuværende tidspunkt.

Jacob oplyser at hensigten er, at der laves et flow i CRM, hvor en leder kan godkende en anmodning selv uden at skulle involvere SDU IT. Godkendelsen fjernes efter 90 dage, hvis rettigheden ikke har været benyttet i mellemtiden. Bjarne påpeger, at delegationen fra leder til sekretær i forskningsmiljøerne ofte er stiltiende, så lederen ikke bliver inddraget i stillingtagen om, hvorvidt den enkelte forsker rent faktisk har behov for adgangen; dette vil Jacob undersøge.

Bue opsummerer med, at udvalget har udtrykt et ønske om at det skal være udgangspunktet, at man ikke har administrative rettigheder uanset stillingskategori. Udvalget godkendte indstilling, men implementering forudsætter et brugerrettet godkendelsesflow for at elevere rettigheder. Jacob skal kigge ind i godkendelsesprocesserne for at der i februar kan foreligge et valideret godkendelses-flow. På et senere møde vil udvalget behandle en indstilling vedrørende VIP'ers adgang til administrative rettigheder.

**6. Godkendelses-
punkt: Afrapporte-
ring af det samlede
risikobillede**

Janni orienterede.

Risikobilledet er før mitigerende foranstaltninger.

Bjarne, som selv afgav informationer til risikovurderingerne, oplyste, at de fremførte trusler ikke var konsistente med hensyn til gruppering af medarbejdere, brugere, ansatte, studerende, m.v.

Udvalget drøftede problemstillingen omkring adresse- og navnebeskyttelse. 3 studerende var lige ved ikke at starte på deres studium fordi SDU ikke kunne sikre beskyttelsen.

Nogle Microsoft-produkter er ikke direkte med i risikovurderingen fordi disse er omfattet af risikovurderingen, som er lavet i Microsoft-taskforcen.

Bue opsummerer med, at systemejere er begyndt at agere efter resultaterne af risikovurderingerne, og at udvalget bakker op om de foreslåede mitigerende tiltag, hvorfor det indstilles til direktøren at det nuværende risikobillede tages til orientering, og at de foreslåede mitigerende foranstaltninger iværksættes mhp. at nedbringe risikoappetitten på et acceptabelt niveau.

7. Fortroligt punkt

8. **Orienteringspunkt:** Bue orienterede om de områder/udvalg, hvor SDU arbejder med retningslinjer i forhold til AI.
Mini-taskforce vedrørende Copilot Simon Kamber fremlagt taskforcens anbefalinger.
SDU Digital er ved at bygge et alternativ til ChatGPT op, men omkostninger i form af afgifter til Microsoft er ukendte.
Martin Svensson opfordrer til, at man inddrager eScience Centret.

Bue opsummerede med, at Jacob og han tager en dialog med Claudio Pica ved eScience Centret.
9. **Orienteringspunkt:** Jacob orienterede om, at det er svært at få projektlederkræfter på. Udfordringen er nu, at DLP-projektet er blevet en udfordring også for SDU's AI-understøttelse, hvilket gør, at det har fået højere prioritet.
DLP-projektet. Simon Kamber fra SDU Digital bliver projektleder fremadrettet.
10. **Orienteringspunkt:** SDU er i undersøgelse gået fra, at hver femte bliver kompromitteret til det nu er hver tyvende. De to seneste undersøgelser er dog ikke helt sammenlignelige.
Phishingkampagne Martin har skabt kontakt til Peter Mayer ved IMADA, der forsker i blandt andet phishing, og som gerne vil give input på fremtidige kampagner, hvilket den digitale organisation naturligvis har takket ja til.
Desværre faldt en phishing-kampagne rettet imod de studerende oveni strømudfaldet den 15. november, så denne måtte trækkes tilbage.
11. **Eventuelt** Mads Lildholdt ønsker en drøftelse, der kan belyse, om der er evt. udfordringer i forhold til den praksis, at SDU lægger alle æg i samme kurv hos Microsoft. Herunder om vi binder os til en ugenomsigtig prismodel.