UNIVERSITETERNES SAMARBEJDE OM CYBER- OG INFORMATIONS-SIKKERHED

AARHUS UNIVERSITET

18. SEPTEMBER 2023

PETER BRUUN NIELSEN
VICEDIREKTØR

LIDT OM MIG SELV

- Vicedirektør og it-chef på AU siden 2015
- IT-driftschef i Region Midtjylland fra 2009-2015
- Formand for universiteternes informationssikkerhedsudvalg (CISO)
- Medlem af fagrådet for informationssikkerhed i Dansk IT

BAGGRUND

- Alle universiteter i DK skal hæve niveauet for cyber- og informationssikkerhed (øget trusselsniveau, skærpede krav fra myndigheder/samarbejdspartnere, ramt af angreb)
- Behov for markante investeringer – måske trecifret millionbeløb ? Heraf stor andel som varige omkostninger.
- Efterspørgslen på cybersikkerhedskompetencer overstiger langt udbuddet (mangler15.000-20.000 i 2030)

Væsentligste fordele gennem et øget samarbejde om cybersikkerhed?

- Stordriftsfordele –> fælles indkøb/fælles drift/fælles udvikling
- Faglig specialisering – øget kvalitet + vigtig parameter for fastholdelse og rekruttering
- Mindske sårbarhed
- Øge videndeling

FORSKNINGSOMRÅDET-MANGE AKTØRER

Decentral Strategi for Cyber- og Informationssikkerhed for forskning

- DCIS i UFM – implementering af strategi, deltager i national koordinering med CFCS og andre DCIS, beredskabsøvelser, formidling og koordinering af internationale tiltag (eks. NIS og 2) i sektoren, tilsyn – lille operativ kapacitet

DKCERT – overvågning af forskningsnetværket, advarsler, ERFA-understøttelse, MISP

DEIC – Forskningsnetværket - driftes af DTU på vegne af DeiC

Universiteterne: Fuldt udbygget lokal infrastruktur, egne overvågningsenheder (SOC etableret flere steder), eget beredskab

INDSATSEN INDTIL NU

- Tæt samarbejde mellem universiteterne i forbindelse med udarbejdelse af sektorstrategien -> væsentlig indflydelse på indholdet
- Afdække potentialer for muligt samarbejde mhp prioritering
- Involvering af interessenter internt (CISO – gruppen af informationssikkerhedschefer, CIO-forum – gruppen af it-chefer, Universitetsdirektørudvalget og eksternt (DeiC, DKCERT, UFM)
- Sikre forankring i sektorstrategien

POTENTIALER OG PEJLEMÆRKER

Pejlemærke 1 - Ledelsesforankring	**Potentiale**	**Indsats**	**Ejer**
Initiativ 1.1 - Ledelsesforankring - risikoappetit og risikostyring	MELLEM	LILLE	UNI
Initiativ 1.2 - Øget modenhed	MELLEM	LILLE	UNI
Initiativ 1.3 - Øget strategisk målbarhed	MELLEM	LILLE	UNI
Pejlemærke 2 - høj sikkerhed			
Initiativ 2.1 - Universiteternes specifikke omstændigheder	MELLEM	MELLEM	UNI
Initiativ 2.2 - Detektion og påvisning	STOR	STOR	UNI
Pejlemærke 3 - risikobaserede tilgang:			
Initiativ 3.1 - Trussels- og risikoanalyser for universitetssektoren	STOR	LILLE	DCIS/UNI
Initiativ 3.2 - Løbende risikovurderinger af kritisk it-infrastruktur	STOR	LILLE	UNI
Initiativ 3.3 - Øget indsigt i trusler og konsekvenser hos forskerne	MELLEM	MELLEM	UNI
Initiativ 3.4 - universiteternes tilslutning til CFCS' sensornetværk	LILLE	LILLE	UNI
Pejlemærke 4 - Styrket samarbejde og koordinering på tværs af sektoren			
Initiativ 4.1 - Etablering af operativ DCIS	STOR	STOR	DCIS/UNI
Initiativ 4.2 - Deling af viden om aktuelle trusler med relevante fora	MELLEM	LILLE	DCIS/UNI
Initiativ 4.3 - Sikkerhedstilsyn med systemleverandører og databehandlere	STOR	STOR	UNI
Initiativ 4.4 - Intelligent overvågning	STOR	STOR	UNI
Initiativ 4.5 - Tværuniversitære awareness-fremmende tiltag	STOR	LILLE	UNI

AWARENESS – INDSATS 4,5

Indsatser, som skal øge viden og bevidsthed om cybercikkerhed blandt medarbejdere, studerende og samarbejdspartnere om

- Kampagner – eks. phishing
- E-learning
- Test i forbindelse med onboarding/rolleskift
- Uddannelse af ledere og medarbejdere målrettet deres funktion
- Målinger af effekt af indsatserne

- > Udarbejde fælles materiale/uddannelsesforløb/testværkstøjer/anskaffe fælles e-learningsplatform

MS-PRODUKTER TIL OVERVÅGNING – 4,4

Alle universiteterne anvender Microsoft sikkerhedssuite anskaffet via campusaftalen, men har meget forskellig implementeringsgrad/anvendelsesgrad.

- Øget udbytte gennem specialisering/spredning af viden
- Øget udbytte gennem ERFA
- Bedre udnyttelse af konsulenter – fælles aftaler/fælles opgaveløsning
- Dele opgaver med konfigurering/integrationer

Samarbejde om dette allerede etableret med Microsoft

OVERVÅGNING – INDSATS 4,1 OG 4,5

De store universiteter har etableret overvågningsenheder (SOC), som holder øje med alarmer fra overvågningssystemer og reagerer på advarsler fra DKCERT i dagtimerne. Universiteterne anvender i vidt omfang de samme systemer til overvågning. Omkostninger til dette er stærkt stigende.

- Etablere fælles 24-7 overvågning ?
- Etablere fælles SOC på tværs af universiteterne ?
- Mere intelligent overvågning (AI-baseret/tilslutning til CFCS-sensornetværk)

RISIKOVURDERING – INDSATS 3,2

Universiteterne anvender i stigende omfang risikovurderinger i forbindelse med systemanskaffelser/ændringer i trusselsniveau. Desuden er det i krav i ISO27001-standarden, som universiteterne har forpligtet sig på at leve op til. Opgaven er ressourcetung og varetages meget forskelligt.

- Delvist genbruge risikovurderinger for samme leverandører/programmer
- Udarbejdelse af fælles compliancepakker for produkter fra de største produktsuiter – eksempelvis Microsoft365
- Anvendelse af samme metode/skabeloner
- ERFA

ØVRIGE INDSATSER

- Penetrationstest – fælles aftale med 'gode hackere' – dele observationer – 3,1 (trusler)
- Fælles indkøb af sikkerhedssoftware – udover MS-produkter anvender universiteterne ofte de samme sikkerhedsløsninger. Måske kan der opnå besparelser gennem fælles EU-udbud i stedet for indkøb via SKI

Tema	Kort forklaring	Vurdering af ressourceforbrug	Vurdering af værdi	Prioriteret rækkefølge
Awareness-strategi	Der kan udvikles en fælles strategi, der kan understøtte og operationalisere ensartede awareness tiltag på tværs af universiteterne med konkrete services målrettet mod forskning, uddannelse, de studerende samt de tvær-administrative funktioner. Der kan muligvis opnås stordriftsfordele i sektorregi samt udvikles et ensartet serviceudbud. Dette da universiteternes brugere og deres hverdag ikke er væsentlig forskellig på tværs af institutionerne.	1	3	1
Produkter til overvågning af klienter og identiteter	Alle universiteterne anvender i større eller mindre omfang Microsoft sikkerhedsprodukter (Defender/Sentinel mm). Dette indkøbes samlet (Campus-licensen) og der er etableret et erfa-netværk, som skal sikre videndeling og anvendelse af best practice. Microsoft deltager og faciliterer netværket. Dette samarbejde kan potentielt udbygges.	2	3	2
Security Operation Center (SOC)	De større universiteter har etableret egen SOC, hvor medarbejdere sidder og overvåger/reagerer på alarmer og håndterer meldinger fra DK-CERT. Der kan opnås fordele ved at etablere en fælles SOC, med klare operationelle mål med afsæt i universiteternes modenhed.	3	3	3
Styrke tværgående operativ CERT/DCIS	Styrket og målrettet fokus på 24/7 (operativ) understøttelse af universiteternes nuværende operative sikkerhedscentre, hvor et centralt center sikrer fælles tværgående vurdering og analyse af trusler og sårbarheder mod forskningsnettet og institutionernes kritiske infrastruktur. En fælles CERT/DCIS kunne med tiden udvikles med kapacitet og beredskab til at forudsige, forebygge, opdage og indgå i håndtering af sikkerhedshændelser på universiteterne.	3	3	4
Risikovurderinger	Selvom risikovurderinger altid skal være konkrete og specifikke i forhold til data/brugsscenarier, kan man ofte genbruge de mere generelle/juridiske vurderinger. Man kan også med fordel bruge de samme skabeloner/metoder på tværs af universiteterne. Der kan desuden udvikles en risikovurdering for at afdække, hvilke leverandører sektoren er mest afhængig af og som dermed udgør den største risiko, skulle disse blive kompromitteret på nogen måde.	2	2	5
Penetrationstest/RED team øvelser	Etablere et leverandørkatalog/udbud på tværs af sektoren med et fælles aftalegrundlag for professionelle services indenfor cybersikkerhed og cyberhygiejne. Det kunne være sårbarhedsscanning, penetrationstest, RED team øvelser etc., hvor de efterspurgte services er ensartede på tværs af institutionerne.	2	2	6
Overvågning af trafikforskningsnettet	DK-CERT foretager allerede i dag overvågning af forskningsnettet i et vist omfang, men denne overvågning kan med fordel øges og gøres mere intelligent. Desuden kan universiteterne individuelt vælge at tilslutte sig Center for Cybersikkerheds sensornetværk.	1	2	7
Diverse sikkerhedssoftware	Der anvendes en række forskellige værktøjer inden for sikkerhedsområdet, som bruges af de fleste universiteter. Det kan undersøges, om der kan opnås besparelser ved at lave fælles udbud/indkøb. Indkøbscheferne har sammen med CIO-gruppen igangsat en afdækning af hvilke systemer (herunder it-sikkerhedssystemer), der bruges på tværs af universiteterne med henblik på at afdække dette.	1	2	8
Udvidet samarbejde på tværgående systemleverandører	En udarbejdelse af fællesfundament i form af compliance-pakker for de største tværgående systemleverandører og databehandlere i sektoren. Det kunne eksempelvis være en grundlæggende compliance-pakke for brug af Microsoft løsninger såsom Office365, Azure og andre Cloud services etc. for sektorens medarbejdere og de studerende.	2	2	9

UNIVERSITETSDIREKTØRUDVALGETS PRIORITERING

Sættes i gang nu

- Awareness-strategi
- Risikovurderinger
- Fælles indkøb af diverse sikkerhedssoftware med inddragelse af indkøbscheferne.

Yderligere bedes CIO-gruppe om at belyse muligheder for og fordele ved henholdsvis:

- En fælles SOC og individuelle SOC'er eventuelt med tilknytning til en fælles SAC
- Mulighederne for at styrke DKCERT
- Hvilke kompetencer og ressourcer, der er på de enkelte universiteter – dele

Ovenstående punkter skal blandt andet belyses i forhold til følgende elementer:

- Økonomi
- Organisering
- Effekten på informations- og cybersikkerheden

RISICI

- Mange aktører på området – krav til høj grad af koordination
- Stor forskel på volumen og scope mellem universiteterne
- Kan vi løse rekrutteringsudfordringen?
- Indsatserne skal styres – har vi den fornødne governance og kapacitet til at lede fælles indsatser?
- Vil krav til kontrol og ansvarsplacering være en hindring for fælles opgaveløsning?

KONKLUSION

- Potentiale for stordriftsfordele – stort volumen/samme infrastruktur/samme opgaver/samme leverandører
- Specialisering er påkrævet – det kan ikke leveres af det enkelte universitet
- Sourcing er påkrævet – universiteterne kan ikke dække alle specialer. Faglig fokusering nødvendig
- Etablering af faglige netværk styrker kompetenceudvikling -> fremme rekruttering/fastholdelse
- Fokuseret indsats og agil styring for at opnå resultater
- Universitetsdirektørenes prioriterede indsatser for samarbejdet er forankret i strategien
- Opgaven er omfattende og kompleks – stort behov for koordinering og styring af risici.

> Insert Quote text, for next level ENTER and TAB

- INSERT NAME

AARHUS
UNIVERSITET