Evalueringsrapport for Cybersikkerhetssenter for forskning og utdanning

7. november 2023

Innhold

1 Innledning

På sitt møte 1. april 2022 ba Digitaliseringsstyret om å få en evaluering av Cybersikkerhetssenter for forskning og utdanning (eduCSC) i løpet av 2023, og at evalueringen tok opp i seg samarbeidet med andre kunnskapsmiljøer på cybersikkerhet i sektoren.

Evalueringen er nå gjennomført og oppsummert i denne rapporten. Den består av noen nøkkeltall, resultater fra en nylig gjennomført kundetilfredshetsundersøkelse og en beskrivelse av utvalgte samarbeidsaktiviteter cybersikkerhetssenteret har hatt med andre virksomheter i kunnskapssektoren.

2 Nøkkeltall

Digitaliseringsstyrets vedtak i april 2022 ga Cybersikkerhetssenter for forskning og utdanning et viktig fundament i form av vedvarende, stabil grunnfinansiering etter at satsingsmidlene fra Kunnskapsdepartementet (KD) tok slutt samme år.

Tjenestene som Digitaliseringsstyret besluttet at UH211 solidarisk skulle finansiere og konsumere er det som i dag omtales som basispakken til Cybersikkerhetssenter for forskning og utdanning (eduCSC), samt tilleggstjenesten sårbarhetsscan.

I perioden mai 2022 – oktober 2023 er det ytterligere 36 virksomheter som har besluttet å abonnere på tjenester fra eduCSC, og det er nå totalt 57 virksomheter som er tilknyttet cybersikkerhetssenteret. Det er ventet at dette antallet vil øke i tiden som kommer.

P.t. er det 67% som abonnerer på basisbakken, 26% på plusspakken og 7% på totalpakken. Det er sannsynlig at denne fordelingen vil jevne seg ut over tid, da nyutviklede tjenester i stor grad blir tilgjengeliggjort i pluss- og totalpakken.

Den økonomiske prognosen for Cybersikkerhetssenter for forskning og utdanning (eduCSC) viser et negativt resultat for 2023 på ca. 7 millioner kroner. Det er ikke planlagt å øke kostnadene for eksisterende kunder ut over normal prisjustering. De kommende årene er man derfor avhengig av økt bevilgning fra Kunnskapsdepartementet (KD) og/eller flere tilknyttede virksomheter for å sikre at dagens aktivitetsnivå er økonomisk bærekraftig. Inntektsbudsjettet inneværende år er på ca. 29 millioner kroner, der UH21 står for ca. 14 av disse.

[1] De 21 universitetene og høgskolene som er direkte underlagt Kunnskapsdepartementet

3 Kundetilfredshet

I oktober 2023 ble det gjennomført en kundetilfredshetsundersøkelse (KTU), der alle virksomheter som har et abonnement hos eduCSC ble oppfordret til å svare. Undersøkelsen var åpen i to uker, og ble sendt til postmottak ved virksomhetene, med kopi til sikkerhetsmiljøene. Totalt 44% (25 stk.) av de forespurte virksomhetene svarte på undersøkelsen. Av disse var 44% universiteter og høgskoler underlagt Kunnskapsdepartementet (UH21) og 56% øvrige virksomheter.

Respondentene hadde følgende roller i egen virksomhet:

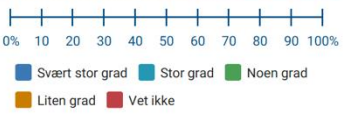
Svar	Antall	% av svar	
CISO	6	24%	24%
IT-leder	10	40%	40%
IRT-medlem	5	20%	20%
CTO	1	4%	4%
Annet	3	12%	12%

Figur 1: KTU - Roller i egen virksomhet

Tillit er et viktig fundament i arbeidet med informasjonssikkerhet, og helt avgjørende for å kunne samarbeide og samhandle på tvers av virksomheter slik vi gjør i norsk kunnskapssektor. Virksomhetene har i all hovedsak stor grad av tillit til Cybersikkerhetssenter for forskning og utdanning:

I hvor stor grad har dere tillit til eduCSC?

Svar	Svært stor grad	Stor grad	Noen grad	Liten grad	Vet ikke	Diagram
I hvor stor grad har dere tillit til eduCSC som responsmiljø ?	12	12	1			
I hvor stor grad har dere tillit til eduCSC som tjenesteleverandør?	6	15	2	2		



Figur 2: KTU - Tillit til eduCSC

Den grunnleggende tilliten vi har mellom cybersikkerhetsmiljøene i kunnskapssektoren legger til rette for utstrakt deling av informasjon. Denne informasjonsdelingen opplever de aller fleste virksomhetene at de har nytte av:

Har din virksomhet hatt nytte av at andre har delt informasjon om cybersikkerhetshendelser i et av eduCSCs forum?

Antall svar: **25**

Svar	Antall	% av svar	
Ja	23	92%	92%
Nei	1	4%	4%
Vet ikke	1	4%	4%

Figur 3: KTU – Deling av informasjon

Det er stor forskjell på virksomhetene som er tilknyttet Cybersikkerhetssenter for forskning og utdanning, både når det gjelder størrelse, kompleksitet og fagområder.

Kundetilfredshetsundersøkelsen viser også at det er et stort spenn i antall medarbeidere som jobber med informasjonssikkerhet/cybersikkerhet i den enkelte virksomhet. Rundt halvparten (48%) av virksomhetene har én eller to medarbeidere som jobber med informasjonssikkerhet/cybersikkerhet. I den andre enden av skalaen er det to (8%) virksomheter som har mellom 12 og 20 medarbeidere på samme fagområde. Dette innebærer naturligvis at virksomhetene har ulike behov for tjenester fra Cybersikkerhetssenter for forskning og utdanning. Til tross for forskjellene uttrykker de fleste virksomhetene at de er fornøyde med tjenestetilbudet som leveres fra eduCSC:

I hvilken grad er dere fornøyd med eduCSCs tjenestetilbud som helhet?

Antall svar: **25**

Svar	Antall	% av svar	
Svært stor grad	3	12%	12%
Stor grad	16	64%	64%
Noen grad	4	16%	16%
Liten grad	2	8%	8%
Vet ikke	0	0%	0%

Figur 4: KTU – Fornøyd med eduCSCs tjenestetilbud

Opplevd nytteverdi per tjeneste finnes i vedlagte rapport fra kundetilfredshetsundersøkelsen.

Oppsummert er det Sikker chat (Mattermost), varslingslister, webinar, temamøter og sertifikattjenesten som oppleves særskilt verdifulle for virksomhetene som har svart på kundetilfredshetsundersøkelsen. Rådgivning knyttet til styring og etterlevelse, samt virksomhetstilpassede øvelser er ifølge undersøkelsen de minst brukte tjenestene.

4 Roller og mandat

Cybersikkerhetssenteret har flere overlappende roller og ansvar. Forvaltningen av sikkerhetsansvaret som følger av Sikts rolle som nettleverandør er sentralt, inkludert varsling og begrenset rådgivning til nettkundene ved behov. Rollen som sektorvist responsmiljø (SRM) utgjør en formalisering av deler av dette, og utvider ansvaret til å omfatte varsling, koordinering og erfaringsutveksling både i egen sektor og nasjonalt. I tillegg leverer eduCSC en rekke sikkerhetstjenester, og har et naturlig ansvar for disse leveransene.

De ulike rollene har oppstått over tid, og dette er trolig årsaken til at om lag halvparten av respondentene i kundetilfredshetsundersøkelsen opplever rollen som noe uklar:

I hvor stor grad opplever dere rollen og mandatet til eduCSC som tydelig?

Antall svar: **25**

Svar	Antall	% av svar	
Svært stor grad	1	4%	4%
Stor grad	10	40%	40%
Noen grad	12	48%	48%
Liten grad	2	8%	8%
Vet ikke	0	0%	0%

Figur 5: KTU – Rolle og mandat

Justisdepartementet (JD) har startet en prosess der ordningen med sektorvise responsmiljø er i ferd med å bli evaluert. Det er ventet at det vil komme forslag til justeringer i kjølvannet av dette. I tillegg er Riksrevisjonen i ferd med å konkludere sine undersøker om hvordan forskningsvirksomheter under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep, og hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdannings- og forskningssektoren.

Begge disse prosessene kan påvirke den fremtidige organiseringen av arbeidet med informasjonssikkerhet i kunnskapssektoren. Cybersikkerhetssenter for forskning og utdanning (eduCSC) har jevnlig dialog med Direktoratet for høyere utdanning og kompetanse (HK-dir) knyttet til disse problemstillingene.

5 Samarbeid med andre cybersikkerhetsmiljøer i sektoren

I sitt vedtak 1. april 2022 ba Digitaliseringsstyret om at evalueringen av Cybersikkerhetssenter for forskning og utdanning (eduCSC) tar opp i seg samarbeidet med andre kunnskapsmiljøer innen cybersikkerhet i sektoren.

Cybersikkerhetssenter for forskning og utdanning (eduCSC) har i perioden siden behandlingen i Digitaliseringsstyret jobbet med å videreutvikle arenaer som legger til rette for samarbeid, erfaringsutveksling og kompetanseheving. Disse blir i varierende grad tatt i bruk av andre kunnskapsmiljøer i sektoren, og oppleves å gi noe verdi for deltakende virksomheter:

I hvilken grad gir disse tjenestene verdi for deres organisasjon?

Svar	Svært stor grad	Stor grad	Noen grad	Liten grad	Vet ikke	Diagram
Sikker chat / Mattermost	11	6	6	1	1	
Semi-ukentlig brief (IRT)	1	10	13		1	
CISO-forum	1	8	10	3	3	
CISO-kaffe		5	9	4	7	
Varslingslister (epost)	11	11	2	1		
Webinarer og digitale temamøter	6	14	5			
Cybersikkerhets senterets Sikkerhetssamling	6	8	5		6	

Figur 6: KTU – Verdi av samarbeidsfora

Respondentene er særlig fornøyd med informasjon om sårbarheter som sendes på varslingslister (epost). Cybersikkerhetssenter for forskning og utdanning (eduCSC) jobber aktivt for å identifisere sårbare instanser hos tilknyttede virksomheter for å varsle disse direkte. Dette er et arbeid som skal videreføres og forbedres, fordi det har god effekt og gir gode tilbakemeldinger fra berørte kunder.

Tilknyttede virksomheter opplever at det er enkelt å komme i kontakt med eduCSC:

I hvor stor grad synes dere det er enkelt å komme i kontakt med eduCSC?

Antall svar: **25**

Svar	Antall	% av svar	
Svært stor grad	10	40%	40%
Stor grad	13	52%	52%
Noen grad	2	8%	8%
Liten grad	0	0%	0%
Vet ikke	0	0%	0%

Figur 7: KTU – Kontakt med eduCSC

Respondentene i kundetilfredshetsundersøkelsen er også i stor grad samstemte om at Cybersikkerhetssenter for forskning og utdanning (eduCSC) i stor grad legger til rette for samarbeid knyttet til cybersikkerhet i kunnskapssektoren:

I hvor stor grad synes dere eduCSC legger til rette for samhandling og samarbeid knyttet til cybersikkerhet i sektoren?

Antall svar: **25**

Svar	Antall	% av svar	
Svært stor grad	3	12%	12%
Stor grad	17	68%	68%
Noen grad	3	12%	12%
Liten grad	1	4%	4%
Vet ikke	1	4%	4%

Figur 8: KTU - Tilrettelegging for samhandling og samarbeid knyttet til cybersikkerhet

Det er allikevel potensiale for å bli enda bedre på samhandling og deling i fremtiden. Det vil Cybersikkerhetssenter for forskning og utdanning (eduCSC) ta initiativ til.

I tillegg til nevnte felles tiltak for samhandling er det gjennomført en rekke bilaterale samarbeidsaktiviteter mellom Cybersikkerhetssenter for forskning og utdanning (eduCSC) og virksomheter i kunnskapssektoren. Noen av disse er beskrevet i det følgende.

Det er inngått rammeavtaler med både NTNU og Universitetet i Oslo (UiO)[2] som legger til rette for at Cybersikkerhetssenter for forskning og utdanning (eduCSC) kan kjøpe tjenester knyttet til cybersikkerhet fra disse. Som del av disse avtalene er det allerede inngått kontrakt om kjøp av trusselindikatorer (sperrelistedata), og det er dialog om samarbeid knyttet til deling av data fra flere kilder. Avtalene legger til rette for et avklart og velfungerende samarbeid mellom partene.

Cybersikkerhetssenter for forskning og utdanning (eduCSC) og Universitetet i Oslo har også hatt dialog knyttet til databehandleravtale for tjenester som sistnevnte konsumerer. Dette har bidratt til økt

[2] Avtalen med UiO er godkjent av begge parter, men foreløpig ikke signert

bevissthet og høyere kvalitet på avtaleverket som benyttes i forbindelse med eduCSCs tjenesteleveranser.

Det er også inngått en intensjonsavtale mellom NTNU og eduCSC om samarbeid knyttet til en doktorgrad som skulle ta for seg måling av sikkerhetskultur i kunnskapssektoren. Doktorgradsstudenten har imidlertid konkludert med at det blir for omfattende å ta for seg hele sektoren, og vil derfor starte med å ta for seg NTNU i første omgang. Sikt og eduCSC håper å kunne bidra på et senere tidspunkt i dette arbeidet, og/eller kunne være samarbeidspartner for andre PhD-studenter knyttet til fagområdet i fremtiden.

Gjennomføringen av øvelse Morris på «Norwegian Cyber Range» ved NTNU ga også god læring og nyttige erfaringer for begge parter.

Det er en rekke bilaterale samarbeid knyttet til innhold på arrangement, som for eksempel webinarer, temamøter og samlinger. De siste 18 måneder har fagmiljøene innen cybersikkerhet i følgende virksomheter vært viktige bidragsytere med å dele av sin erfaring og kunnskap i form av innlegg/foredrag på eduCSC-arrangementer:

- Direktoratet for høyere utdanning og kompetanse (HK-dir)
- Institutt for energiteknikk (IFE)
- Kunnskapsdepartementet (KD)
- NTNU
- OsloMet
- Sikt – Kunnskapssektorens tjenesteleverandør
- Sikresiden.no
- Universitetet i Oslo
- Universitetet i Stavanger
- Universitetet i Tromsø

Tilsvarende bidrar eduCSC på arrangementer i kunnskapssektoren på forespørsel, som for eksempel NTNUs stjerneprogram og NTNUs sikkerhets- og beredskapsdag.

I løpet av 2023 er det utarbeidet en produktstrategi for Cybersikkerhetssenter for forskning og utdanning (eduCSC) som gir en oversikt over hvilke aktiviteter som er planlagt gjennomført de neste årene. Denne strategien er drøftet med blant andre HK-dir, porteføljestyret for data og infrastruktur, UH-IT og CISO-forum. Det har kommet en rekke tilbakemeldinger, og disse er i hovedsak hensyntatt i den siste revisjonen av produktstrategien som er tilgjengelig for nedlasting via hjemmesidene til Sikt[3]. Respondentene på kundetilfredshetsundersøkelsen har i noen grad kjennskap til produktstrategien.

[3] https://cms.sikt.no/sites/default/files/2023-10/2023-10-20-Produktstrategi-eduCSC.pdf

I hvor stor grad har dere kjennskap til eduCSCs produktstrategi?

Antall svar: **25**

Svar	Antall	% av svar	
Svært stor grad	0	0%	0%
Stor grad	6	24%	24%
Noen grad	12	48%	48%
Liten grad	4	16%	16%
Vet ikke	3	12%	12%

Figur 9: KTU - Kjennskap til produktstrategi

6 Konklusjon

De siste atten månedene har det vært en stabil økning av virksomheter som er tilknyttet Cybersikkerhetssenter for forskning og utdanning (eduCSC), og tilknyttede virksomheter tar stadig i bruk en større andel av tjenestene som tilbys.

Dagens aktivitetsnivå er ikke økonomisk bærekraftig, men etter hvert som tjenestetilbudet utvikles og gjøres kjent vil trolig inntektene øke i takt med dette. Det jobbes også med å øke sentralfinansieringen for å dekke myndighetspålagte oppgaver.

Kundetilfredshetsundersøkelsen viser at virksomheter i norsk kunnskapssektor har tillit til Cybersikkerhetssenter for forskning og utdanning (eduCSC), og at majoriteten i stor grad er fornøyd med dagens tjenestetilbud. Den viser også at det kan være behov for tydeliggjøring av eduCSCs roller.


Sikt