PROSJEKTMANDAT FOR

PROSJEKTET «ANALYSESENTER OG RESPONSMILJØ»

INNENFOR PROGRAMMET
«UH SIKKERHETSSATSING 2019-2022»

UNINETT PROSJEKTNUMMER: U1210017

Programleder Anders Lund, Uninett	Programeier Sigurd Eriksson, Unit

Prosjektleder Maria Luces, Uninett	Prosjekteier Tom Røtting, Uninett

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	10.04.19	Første versjon opprettet	AL	
0.2	14.05.19	Første utkast	AL, ML, LES	
0.8	24.05.19	Andre utkast	AL, ML, LES	
1.0	17.06.19	Siste versjon – vedtatt i programstyret	AL, ML, LES	Programstyre

1. BAKGRUNN

Prosjektet «Analysesenter og responsmiljø» er organisert som et prosjekt under det fireårige programmet «UH Sikkerhetssatsing 2019-2022», tildelt av Kunnskapsdepartement (KD) til Unit[1]. Sikkerhetssatsingen er tiltak med bakgrunn i «Digitaliseringsstrategien for UH-sektoren 2017-2021». Mandatet for programmet[2] er forankret og vedtatt i Digitaliseringsstyret. Overordnet mål for programmet er å forbedre sektorens evne til å forebygge, oppdage og håndtere trusler og iverksette tiltak som skal forbedre analyseverktøy, rådgivningstjenester og kompetanseheving innen informasjonssikkerhet og personvern.

Uninett har fått tildelt midler fra Unit for å lede arbeidet, i tett samarbeid med sektoren, for å realisere målene, og bidra til å styrke informasjonssikkerhet.

Frem til sikkerhetssatsingen ble vedtatt av KD ble det diskutert flere områder som burde inngå i et arbeid for forbedret informasjonssikkerhet i UH-sektoren. Flere av områdene er drøftet og forankret i «Fagutvalg for informasjonssikkerhet» og i «Prioriteringsrådet for nett og nettnære tjenester»:

- Helhetlig og felles deteksjons- og analysekapasitet.
- Forbedret evne til å håndtere sikkerhetstrusler i sektoren i tråd med NSMs rammeverk for hendelseshåndtering.
- Rådgivningstjenester innenfor informasjonssikkerhet til sektoren.
- Kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og andre brukere i sektoren.

Dette har ledet frem til at den nevnte Sikkerhetssatsingen organiseres som et program med tre hovedprosjekter:

1. Ny styringsmodell for informasjonssikkerhet og personvern
2. Analysesenter og responsmiljø
3. Rådgivingstjenester og kompetanseheving

Dette dokumentet beskriver mandatet for prosjektet «Analysesenter og responsmiljø».

1 Tildelingsbrev fra Kunnskapsdepartement til Unit_ref.nr. 18/4768, datert 19.12.18
2 Programmandat – Styringsdokumentasjon for UH sikkerhetssatsing 2019-2022 (styrevedtatt i Digitaliseringsstyret - 11.04.19, Oslo)

2. MÅL, HOVEDINNHOLD OG FORVENTEDE RESULTATER

Prosjektet "Analysesenter og responsmiljø" skal:

1. Forbedre deteksjons-, analyse- og responskapasiteten i UH-sektoren.

2. Etablere sektorens analysesenter for cybersikkerhet (teknisk tilrettelegging og støtteverktøy, bemanning, organisasjonsutvikling, rutiner, etc.), i tett samarbeid med sektorens etablerte sikkerhetsmiljøer.

3. Forbedre sektorens evne til å håndtere trusler.

4. Utvikle og innføre felles sikkerhetstjenester for sektoren, innen deteksjon, analyse og respons. Tjenestene må sikre bærekraftige finansieringsmodeller som gir tilstrekkelige ressurser, også etter at satsingen er over.

Arbeidet i prosjektet skal utføres i tett samarbeid med sektoren, og med konkret deltagelse fra informasjonssikkerhetsmiljøene på NTNU og UiO. Prosjektet skal ha fokus på kontinuerlige og smidige leveranser, hyppige delleveranser av nye og forbedrede sikkerhetstjenester.

Uninett, som sektorCERT og ansvarlig for forskningsnettet og andre fellestjenester i UH-sektoren, har et særskilt ansvar for å ha gode systemer og rutiner for egen beredskap rundt deteksjon og analyse av IKT-hendelser. Dette påpekes i strategier, rammeverk og retningslinjer fra blant annet regjeringen og NSM, og inngår også som beste praksis i generelt sikkerhetsarbeid.

I samarbeid med NTNU og UiO vil prosjektet i 2019 starte etableringen av en sentral plattform for håndtering av data til analyseformål. God samhandling mellom den sentrale plattformen og allerede eksisterende analysekapasitet ved UiO og NTNU vil være en viktig suksessfaktor for etableringen av et felles analysesenter for cybersikkerhet som kommer alle institusjoner i sektoren til gode.

Prosjektet skal der det er mulig og hensiktsmessig benytte eksisterende verktøy og infrastruktur i utviklingsarbeidet. Prosjektet skal vurdere anvendelse av markedet, som i en del sammenhenger kan gi hurtigere leveranser og bedre håndtere svingninger i etterspørsel.

3. ANGREPSVINKEL OG METODE FOR GJENNOMFØRING – OMFANG AV ARBEIDET

Gjennomføringen av prosjektet «Analysesenter og responsmiljø» skal skje i tråd med de føringene som er gitt gjennom tildelingsbrev fra KD, og videre i tildelingsbrevet fra Unit til Uninett. Prosjektet skal gjennomføres i tett samarbeid mellom Uninett, UiO/USIT og NTNU/Gjøvik.

Prosjektet skal i størst mulig grad benytte bestepraksis-metodikk. Prosjektet planlegger å benytte smidig metodikk og tjenestedesign («design thinking») for utvikling av nye tjenester, for å sikre brukermedvirkning og for å tilføre raskest mulig verdi for kunder og brukere.

Prosjektveiviseren, som er Difis anbefalte prosjektmodell for styring av digitaliseringsprosjekter i offentlige virksomheter, skal brukes som styringsmodell for prosjektet.

I konseptfasen skal prosjektet utarbeide et veikart som viser prioriterte tiltak og aktiviteter for prosjektperioden (2019-2022). Veikartet vil være utgangspunkt for planlegging av arbeidsomfang og ressursbehov i prosjektet.

Unit har nylig foretatt en risiko- og tilstandsvurdering for sektoren på oppdrag fra KD. Denne, og tilsvarende trusselvurderinger i sektoren, vil kunne gi relevante innspill til etablering av veikartet og prioriteringen av aktivitetene i prosjektet.

4. HOVEDAKTIVITETER OG MILEPÆLSPLAN

4.1. Hovedaktiviteter for første prosjektår (2019)

I 2019 planlegger vi i prosjektet å igangsette følgende aktiviteter:

1. DNS brannmur levert som en fellestjeneste i UH-sektoren, hvor grunnlag for sperringer også inkluderer data levert av NTNU og UiO.
2. Starte etablering av en sentral plattform for håndtering av data til analyseformål.
3. Avklaring av juridisk problemstillinger knyttet til deling av data i sektoren, som grunnlag for etablering av et helhetlig og felles deteksjons- og analysesenter.
4. Legge til rette for bedre kommunikasjon mellom de operative sikkerhetsmiljøene i sektoren, slik at dialog kan foregå fortløpende og i sann tid rundt aktuelle hendelser.
5. Distribuering av trusselvurderinger, utarbeidet av NTNU, gjennom sektorens kontaktnett av IRTer (Incident Response Team).

Hovedaktivitet	JAN	FEB	MAR	APR	MAI	JUN	JUL	AUG	SEP	OKT	NOV	DES
DNS brannmur tjeneste - Pilotfase												
DNS brannmur etablert som fellestjeneste												
Utarbeidelse av veikart for prosjektet												
Sektorens trusselvurdering												
Etablere sentral plattform for håndtering av data til analyseformål												
Nytt kommunikasjonsverktøy («Sikker chat») mellom operative sikkerhetsmiljø i sektoren												
Avklaring juridiske ramme for datahåndtering i sektoren												

4.2. Milepæler

Som beskrevet tidligere i dokumentet skal prosjektet benytte smidige metoder for systemutvikling, med vektlegging av fleksibilitet og hyppige delleveranser. Prosjektgruppen er i gang med kartlegging og prioritering av aktivitetene (veikartarbeid).

Milepælsplanen for prosjektet blir etablert etter at arbeidet med veikartet er fullført.

4.3. Konsekvenser for drift og forvaltning

De fleste av tjenestene som prosjektet skal levere krever allokering av tekniske ressurser for både utvikling, drift og vedlikehold. Tjenestene som utvikles i prosjektet overleveres som fellestjenester for sektoren, med egne betalingsmodeller og forvaltning. Denne prosessen kan være tids- og ressurskrevende og bør planlegges inn i tjenesteutviklingen.

En sentral plattform for håndtering av data til analyseformål er en levende plattform under konstant utvikling, med behov for hyppige oppgradering og gode sikrings-, drifts- og vedlikeholdsrutiner. Dette medfører behov for allokering og rekruttering av spisskompetanse for de konkrete arbeidsoppgavene. I tillegg til tekniske ressurser, er det viktig å ha tilgang til juridisk kompetanse for etablering av dekkende og entydige databehandleravtaler mellom partene.

Robuste driftsmiljøer, god rådgivning og organisasjonsutvikling vil være avgjørende for å møte stadige økende krav til sikker drift av viktige sikkerhetstjenester knyttet til myndighetenes strategier for digital sikkerhet.

5. ORGANISERING

Prosjektet er organisert i et kjerneteam bestående av sentrale ressurser fra NTNU, UiO og Uninett.

Prosjektleder rapporterer direkte til programleder for sikkerhetssatsingen.

Prosjektet skal organisere aktiviteter og delleveranser på en hensiktsmessig måte. Team og samarbeidsgrupperinger etableres ut fra behov for ressurser, kompetanse, fremdrift, samhandling.

Tabellen under viser deltakere i kjerneteamet:

Navn	Rolle i prosjektet	Periode	Spesifikke arbeids- og ansvarsområder
Maria Luces - Uninett	Prosjektleder	2019-2022	Prosjekt- og prosessledelse
Rune Sydskjør - Uninett	Fagansvarlig Uninett	2019-2022	
Stian Husemoen – NTNU Seksjonsleder digital sikkerhet	Fagansvarlig NTNU	2019-2022	
Espen Grøndahl - UiO IT Sikkerhetssjef	Fagansvarlig UiO	2019-2022	

Interessentgruppen og andre samarbeidspartnere for programmet er kartlagt gjennom en interessentanalyse.

6. BUDSJETT

6.1. Finansiering

Kunnskapsdepartementet har gitt tilsagn om 17,5 mill. kroner årlig til Unit for etablering og gjennomføring av programmet for økt sikkerhetssatsing i UH-sektoren i fire år. Av disse er det gitt tilsagn om 12,5 mill. kroner til Uninett for å rigge og lede prosjektet som skal implementere de nødvendige tiltak for å styrke informasjonssikkerhet bla etablering av sektorens analysesenter for cybersikkerhet, rådgivingstjenester og kompetanseheving inne informasjonssikkerhet og personvern. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av oppgavene og rollene i Unit.

12,5 mill. kroner tildelt Uninett fordeles mellom de to prosjektene som Uninett er ansvarlig for; «Analysesenter og responsmiljø» og «Rådgivningstjenester og kompetanseheving».

Prosjekt	**Tilskudd** (MNOK pr år)
Ny styringsmodell (Unit)	**5,0**
Analysesenter og responsmiljø (Uninett)	**12,5**
Rådgivningstjenester og kompetanseheving (Uninett)	
Totalt årlig tilskudd	**17,5**

I tabellen under vises et grovt estimat over foreslått fordeling av tilskuddet mellom prosjektene.

Budsjett	**2019**	**2020**	**2021**	**2022**
Programadministrasjon	1	0,5	0,5	1
Analysesenter og responsmiljø	**10**	**7**	**7**	**7,5**
Rådgivningstjenester og kompetanseheving	1,5	5	5	4
Totalt tilskudd (NMOK)	**12,5**	**12,5**	**12,5**	**12,5**

Et mer detaljert budsjett for prosjektet blir utarbeidet etter at veikartet for prosjektet er skissert ferdig. Prosjektet er basert på smidig metodikk og dermed er kostnadsfordelingen over år og mellom de to prosjektene som Uninett står ansvarlig for basert på et grovt estimat.

6.2. Planlagt forbruk

Prosjektet pådrar seg følgende kostnader:

- Egen ressursinnsats
- Konsulent (programstøtte) og annen innleie
- Reise- og møtekostnader
- Lisenser, hardware og andre direktekostnader

De to første prosjektårene er det estimert et timeforbruk på omtrent 5 årsverk, hvor tekniske ressurser utgjør den største andelen i arbeidet med system- og tjenesteutvikling. Arbeidsinnsatsen fra NTNU og UiO er estimert til 1 årsverk fra hver for hvert av de to første prosjektårene. Arbeidsomfanget og ressursbehovet knyttet til de ulike arbeidspakkene blir definert gjennom arbeidet med veikartet for prosjektet.

7. KRITISKE SUKSESSFAKTORER / RISIKOER

Suksessfaktor	Risikoreduserende tiltak
Konkretisering og riktig prioritering av leveransene i prosjektet i tråd med målsetninger og brukerbehov	Grundig planleggings- og veikartarbeid prioriteres, med involvering av tekniske ressurser hos Uninett og samarbeidspartnere. Veikartet forankres hos prosjektgruppen og godkjennes av Programstyret.
Tilgang på tilstrekkelige ressurser	God ressursplanlegging mht veikartet for leveransene og arbeidsomfang. Sette i gang rekruttering av kompetansen om nødvendig.
Tilfredsstillende fremdrift i prosjektet	God planlegging av delleveranser og aktivitetene som inngår i utviklingsløpet for hver tjeneste. Jevnlig statusrapportering i prosjektet.
Tydelig roller og ansvarfordeling i prosjektet	Tydelig prosjektmandat og styringsdokumentasjon. Sikre felles forståelse blant prosjektdeltakere.
Sikre forankring av prosjektet hos interessentgruppen	Involvering og jevnlig informasjon til premissgivere og andre relevante interessenter.
Tillit og godt samarbeid blant deltakere i prosjektet	Åpen og hensynsfull kommunikasjon. Klare ansvarsforhold og gode rutiner for informasjonsformidling.

8. PROSJEKTSTYRING

Prosjektet rapporterer til Programstyret i forbindelse med styremøtene som er planlagt å avholdes fire ganger per år. Minimums rapportering skal innebære en rapportering på fremdrift, kvalitet og økonomi. Rapportering utover denne minimumsrapportering kan avtales ved behandling av prosjektbeskrivelsen.

Programlederen deltar på styremøtene i tillegg til medlemmene i programstyret, med ansvar for rapportering om status på de tre prosjektene som programmet består i.

Prosjektet skal ha hyppigere rapportering og kontinuerlig dialog med programlederen, minst to ganger i måned.

Prosjektgruppen og samarbeidspartnere skal avtale hyppige status- og arbeidsmøter basert på organisering av arbeidet innen hver arbeidspakke.

Prosjektdokumentene skal lagres på programportalen opprettet på MS Sharepoint hos Uninett. Det benyttes samhandlingsverktøy (O365) der prosjektgruppen får tilgang til relevant prosjektinformasjon.