ØF-notat nr. 04/2004

Bluelight: nettverk for informasjonssikkerhet

- historien og kritiske suksessfaktorer

av

Svein Bergum og Lene Nyhus

Østlandsforskning

er et forskningsinstitutt som ble etablert i 1984 med Oppland, Hedmark og Buskerud fylkeskommuner samt Kommunaldepartementet som stiftere, og har i dag 29 ansatte.

Østlandsforskning er lokalisert i høgskole-miljøet på Lillehammer. Instituttet driver anvendt, tverrfaglig og problemorientert forskning og utvikling.

Østlandsforskning er orientert mot en bred og sammensatt gruppe brukere. Den faglige virksomheten er konsentrert om to områder:

Regional- og næringsforskning
Offentlig forvaltning og tjenesteyting

Østlandsforsknings viktigste oppdragsgivere er departement, fylkeskommuner, kommuner, statlige etater, råd og utvalg, Norges forskningsråd, næringslivet og bransjeorganisasjoner.

Østlandsforskning har samarbeidsavtaler med Høgskolen i Lillehammer, Høgskolen i Hedmark og Norsk institutt for naturforskning. Denne kunnskaps-ressursen utnyttes til beste for alle parter

ØF-notat nr. 04/2004

Bluelight: nettverk for informasjonssikkerhet

- historien og kritiske suksessfaktorer

av

Svein Bergum og Lene Nyhus

Tittel:	Bluelight: nettverk for informasjonssikkerhet - historien og kritiske suksessfaktorer
Forfattere:	Svein Bergum og Lene Nyhus
ØF-notat nr.:	04/2004
ISSN nr.:	0808-4653
Prosjektnummer:	K20708
Prosjektnavn:	VS 2010 Innlandet
Oppdragsgiver:	Norges Forskningsråd, Morgenlandet
Delprosjektleder:	Svein Bergum
Referat:	Innlandet har i lengre tid hatt en god del aktører med spisskompetanse innen informasjonssikkerhet. Fra 2001 er det skjedd en rekke aktiviteter for å få til økt formelt samarbeid mellom de 40 aktørene i Innlandet. Det største resultatet så langt av dette er opprettelsen av Masterstudium i informasjonssikkerhet ved Høgskolen i Gjøvik høsten 2002. Nettverket har nå betegnelsen Bluelight, og ble fra høsten 2002 en del av Innovasjon Norge sitt Arena Program. Her beskrives status og mål for samarbeidet i Bluelight. Vi gir en oversikt over sentrale aktører, og historien bak nettverket presenteres. Til slutt gjør vi en analyse av nettverket, der spesielt kritiske suksessfaktorer trekkes fram.
Sammendrag:	Nei
Emneord:	IKT, informasjonssikkerhet, bedriftsnettverk
Dato:	Juni 2004
Antall sider:	32
Pris:	Kr 60,-
Utgiver:	Østlandsforskning Serviceboks 2626 Lillehammer Telefon 61 26 57 00 Telefax 61 25 41 65 e-mail: post@ostforsk.no http://www.ostforsk.no

Forord

Dette notatet er laget som del av forskningsprogrammet "Verdiskaping 2010" (forkortet VS-2010). Det overordnede målet er at VS 2010 skal bidra til å videreutvikle og utløse potensialet for bedriftsintern og nettverksbasert nyskaping. Dette skal skje gjennom partsbasert medvirkning og utviklingskoalisjoner særlig på regionalt nivå. Samtidig skal det vitenskapelige kunnskapsgrunnlaget på feltet styrkes.

VS-2010 har moduler i ulike deler av Norge, og en av disse har fokus på innlandet. Denne modulen er et samarbeidsprosjekt mellom Norsk Institutt for By og Regionforskning (NIBR), Østlandsforskning og Høgskolen i Hedmark. Tom Johnstad fra NIBR er modulansvarlig. Modulen har ulike aktiviteter knyttet til ulike nettverk, slik som lettmetallklynga på Raufoss, treklynga i Glåmdalen, reiseliv i Valdres, matproduksjon, samt IKT/media.

Dette notatet er utdrag fra ett av kapitlene i statusrapporten for innlandsmodulen for VS-2010, som planlegges å komme ut rett før sommerferien 2004. Notatet omhandler delprosjektet om IKT/media med fokus på informasjonssikkerhet. Det gir en oversikt over bakgrunn, historie, status og kritiske suksessfaktorer for det nettverk innen informasjonssikkerhet som er utviklet i innlandet de siste tre årene. Nettverket har fått betegnelsen "Bluelight".

Notatet har blitt utarbeidet av Svein Bergum, som delprosjektleder, sammen med Lene Nyhus.

Vi takker alle intervjuobjektene i Bluelight for velvillighet både i intervjuer og møter. En spesiell takk til Svein Pettersen/Gjøvik Kunnskapspark og Eivind Petershagen/Innovasjon Norge, som har gitt verdifulle kommentarer på tidligere utkast og gitt god tilgang på informasjon fra arbeidet i nettverket..

Lillehammer, juni 2004

Svein Bergum
Prosjektleder VS 2010 - IKT/media

Lene Nyhus
Forskningsleder

Innholdsfortegnelse

Sammendrag

Arbeidet med IKT/media har i 2003 konsentrert seg om feltet *informasjonssikkerhet*. Innlandet har i lengre tid hatt en god del aktører som har hatt spisskompetanse på dette området. Av disse aktørene er majoriteten brukermiljøer, og et fåtall er leverandører av produkter/tjenester. Dette er derfor ikke noen bransje eller næring, men et funksjonsområde i en organisasjon.

Fra 2001 har det skjedd en rekke aktiviteter for å få til økt formelt samarbeid mellom de 40 aktørene i Innlandet. Det største resultatet så langt av dette er opprettelsen av Masterstudium i informasjonssikkerhet ved Høgskolen i Gjøvik høsten 2002. Nettverket har nå betegnelsen Bluelight, og ble fra høsten 2002 en del av Innovasjon Norge sitt Arena Program. Vi har i hele perioden fra desember 2002 til nå vært observatører i styringskomité og drivernode i dette nettverket.

Her beskrives status og mål for samarbeidet i Bluelight. Vi gir en oversikt over sentrale aktører, og historien bak nettverket presenteres. Til slutt gjør vi en analyse av nettverket, der spesielt kritiske suksessfaktorer trekkes fram.

Alle vi har vært i kontakt med er enig om at Bluelight har nådd sine mål så langt, og således er en suksess. Etablering av Masterstudiet og etter hvert også FOU-enheten "NIS-lab" ved Høgskolen i Gjøvik er to eksempler på resultater. I tillegg er det etablert flere møteplasser for kompetanseutvikling eksempel innen kommunal sektor. Bluelight oppfattes som nyttig av aktørene, og er i ferd med å skape seg aksept i markedet. Det er også etablert mye kontakt mot sentrale myndigheter.

I forhold til VS 2010 sin målsetning om "bred medvirkning", har Bluelight klart å skape bred medvirkning blant relevante interessenter både hos leverandører, brukere og offentlige aktører (departement, NFR, kommuner, Innovasjon Norge mv). Det kan for eksempel nevnes at Foreningen for kommunal informasjonssikkerhet (KINS) allerede etter ett år har 66 medlemmer, og har arrangert to seminarer på ett halvt år med til sammen 300 deltakere.

Blant de faktorer som kan forklare at Bluelight har vært vellykket så langt er at målsettingene for nettverket har vært *konkrete*. At det første samarbeidsområde var kompetanseutvikling, anses nyttig og ukontroversielt. Det er også forhold ved deltakerne i nettverket som forklarer det gode resultatet: Det var kompetanse til stede i Innlandet i utgangspunktet, blant annet på Jørstadmoen og i Telenor. Videre er det god blanding av ulike aktører hvorav mange kjenner hverandre fra tidligere. Tillitt og kommunikasjon har derfor vært god i Bluelight. Både regionale og nasjonale aktører er representert. Enkeltpersoner har vært drivkrefter, og de jobber i bedrifter som har flere målsettinger enn kun "bunnlinje", eksempelvis regional utvikling. Prosjektledelsen fra Gjøvik kunnskapspark betraktes som god, blant annet ved at de har legitimitet hos aktører både i næringsliv (leverandører og brukere), FOU og offentlige aktører. Og til sist: det er skapt et godt samarbeidsmiljø mellom offentlige og private aktører, der offentlige aktører som Høgskolen i Gjøvik og Innovasjon Norge har vist markedsorientert handling.

Selv om Bluelight har vært en suksess så langt, er det et stykke før alle målsettinger innfris. Det er antagelig større utfordringer med å få til produktutvikling og FOU-prosjekter enn å realisere et studium. De planlagte tiltakene til Bluelight framover tar imidlertid tak i en god del av disse utfordringene.

1 Innledning

I Innlandet har det de senere årene utviklet seg et interessant samarbeid og nettverk innen informasjonssikkerhet. Dette er knyttet til sentrale aktører i regionen, og der også nasjonale og internasjonale aktører er aktivt med. Det er store potensialer for utdanning, forskning, innovasjon og næringsutvikling knyttet til dette. I dette kapitlet beskrives historien om nettverket for informasjonssikkerhet Bluelight, og en analyse av suksessfaktorene for dette.

I avsnitt to tar vi en kort presentasjon av status innen IKT/medier i innlandet, men hovedfokus vil være på forklaring av sentrale begreper og utviklingstrekk innen informasjonssikkerhet. I avsnitt tre vil vi gå nærmere inn på status og målsettinger for informasjonssikkerhet i Innlandet. Vi vil blant annet se nærmere på organisering og aktører. Innovasjonsnettverket Bluelight vil bli presentert med status og planer.

I avsnitt fire vil vi gå litt tilbake i tid og se hvordan samarbeidet om informasjonssikkerhet i Innlandet startet og har utviklet seg. Vi vil legge vekt på det som har skjedd formelt de siste tre årene.

Etter disse beskrivelsene vil vi i avsnitt fem analysere en del sentrale forhold ved samarbeidet, for å identifisere mulige kritiske suksessfaktorer.

Siste avsnitt inneholder avslutning og foreløpige konklusjoner.

2. IKT/media-sektoren med fokus på informasjonssikkerhet

2.1 Generelt

IKT/Mediesektoren er viet en god del oppmerksomhet i forbindelse med utviklingen i Innlandet. Selv om sektoren ikke utgjør store tall når det gjelder antall sysselsatte, har den en vekst og et framtidig vektspotensial. Samtidig har IKT/media en betydning utover sysselsettingstallene for sektoren selv, i og med at det er mange med slike funksjoner i andre næringer, eksempelvis IKT-ansatte i bank eller offentlig sektor. Antall IKT-ansatte vil derfor påvirkes av hvordan disse tjenestene organiseres, for eksempel om de er internt i en bedrift eller kjøpes eksternt av en tjenesteleverandør. IKT/Mediesektoren er derfor en sammensatt sektor som er vanskelig å lese direkte ut av statistikken. Det er mange sysselsatte innen IKT i nesten alle typer næringer og bransjer og som dermed er registrert under andre næringer enn "IKT" eller "Media". Den tekniske utviklingen går også mot en sammensmeltning av ulike medier og det blir vanskeligere å kategorisere etter form. Konvergensen fører blant annet til at forskjellig innhold som tekster, lyd og bilder kan distribueres på mange måter gjennom ulike media. Eksempelvis kan en PC i dag benyttes både til tekstbehandling, bildebehandling og til å høre radioprogrammer og musikk.

Ser en på IKT- og mediesektoren samlet var det i 4. kvartal 2000 registrert 3.200 arbeidsplasser i Hedmark og Oppland. De to fylkene hadde på den tid om lag 152.000 arbeidsplasser totalt med 50.000 lokalisert til de fire byene Kongsvinger, Hamar, Lillehammer og Gjøvik. Sektoren utgjorde 2,3% av totalt antall arbeidsplasser i Hedmark og 2,0% i Oppland mot 3,8% på landsbasis. Tallene er basert på en noe utvidet definisjon av mediesektoren og framkommer i en næringsanalyse av IKT/mediesektoren (medieproduksjoner og kulturbaserte næringer[1]) (Ericsson, 2002 m.fl.). Ca. 30% av de registrerte arbeidsplassene er knyttet til virksomheter som enten er eller nylig har vært statlige monopolbedrifter. Mange av disse arbeidsplassene er derfor politisk lokalisert og trolig basert på andre vurderinger enn de private virksomhetene. I begge fylkene domineres sektoren av avisforlegging, telekommunikasjoner, datakonsulenter samt lotteri og totalisatorspill. Disse bransjene utgjør samlet to tredjedeler av arbeidsplassene i sektoren.

Et hovedinntrykk av IKT/mediabransjen i Innlandet er at den består av flere mindre, men også noen større (f.eks. Norsk Tipping), aktører som i stor grad opererer uavhengig av hverandre og med sine viktigste relasjoner ut av regionen[2]. På enkelte områder er det satt i gang slikt regionalt samarbeid, og nettverket vi skal omtale videre, innen *informasjonssikkerhet*, er eksempel på et slik samarbeid. Informasjonssikkerhet er valgt som område å studere innen IKT/media fordi det er et område i vekst og strategisk viktig. Det utgjør ikke verken sysselsettingsmessig eller kostnadsmessig mer enn 5-10% av IKT totalt sett, men har større betydning enn dette. Det er foreløpig ingen statistikk for informasjonssikkerhet verken nasjonalt eller regionalt, men i følge Nærings- og Handelsdepartementet (NHD) jobber de med saken sammen med SSB.

[1] Her er også OECD-standard lagt til grunn. De næringsgrupper som inngår er forlagsvirksomhet, grafisk produksjon (med unntak av trykking), annonse- og reklame - og fotografivirksomhet, samt deler av fritidsvirksomhet og kulturell tjenesteyting (film, video, radio, TV, selvstendig kunstnerisk virksomhet, underholdning, opplevelsesparker, lotteri og totalisatorspill mm.). Næringsanalysen for mediesektoren i Hedmark og Oppland ble utarbeidet på oppdrag fra INNOVASJON NORGEi forbindelse med forprosjektet Regionale Innovasjonspiloter, Innovasjon Innlandet.

[2] Dette er basert på intervjuer med ledere fra et utvalg IKT/medie -bedrifter i regionen (Ericsson m.fl. 2002).

2.2 Informasjonssikkerhet

Prioriteringen av informasjonssikkerhet skyldes foruten at dette er et område i vekst, også at dette området er prioritert innen SND's Arena-program. Sistnevntes prioritering skyldtes at de hadde konkret fokus, og at aktører både fra offentlig, privat og FOU-sida deltar aktivt. Ikke minst anses det viktig at næringslivet er aktiv initiativtaker og drivkraft.

Hva er informasjonssikkerhet?

Informasjon er et aktivum som kan ha stor verdi for en virksomhet eller for et individ. Informasjon, informasjonssystemer (dvs systemer der informasjonen produseres, lagres og behandles) og nett der informasjonen utveksles kan utsettes for trusler og anslag, og må derfor beskyttes forsvarlig. Beskyttelse av informasjon innebærer sikring av informasjonens:

- tilgjengelighet (for rett person, til rett tid og i rett form)
- integritet (at informasjonen er korrekt og ikke forfalsket/ødelagt)
- konfidensialitet (at informasjonen sikes mot uvedkommende innsyn)

> "Informasjonssikkerhet kan derfor defineres som tiltak for å beskytte informasjonen som behandles av et informasjonssystem mot brudd på konfidensialitet, integritet og tilgjengelighet, for å beskytte systemet i seg selv og for å beskytte nett der informasjonen utveksles (FD, NHD, JPD, 2003)".

Informasjonssikkerhet brukes ofte i samme betydning som IT-sikkerhet eller IKT-sikkerhet, da informasjon i stor grad lagres, behandles og kommuniseres i stor grad ved hjelp av IT-systemer. Med økt bruk av IT/IKT, vil også behovet for informasjonssikkerhet øke. Informasjonssikkerhet er derfor et område med økt fokus og med rask vekst. Med den store økningen i bruk av Internett, epost, elektronisk forretningsdrift og elektroniske tjenester, gjør at stadig flere organisasjoner åpner sine datasystemer for eksterne brukere. En slik økt tilgjengelighet øker også muligheten for kriminelle aktiviteter eller annen type anslag (FD, NHD, JPD, 2003). Informasjonsteknologien har derfor gjort samfunnet sårbart på nye områder, blant annet gjennom bevisste angrep på informasjonssystemer. Informasjonssamfunnets særskilte utfordringer innen informasjonssikkerhet er blant annet:

- identifisering av kritisk IT-infrastruktur
- sikring av kritisk IT-infrastruktur
- sikker overføring av informasjon (bl.a gjennom krypering)
- utvikling av regelverket
- virksomhetens fokus på sikkerhet, bl.a gjennom formelle planer og bevisstgjøring og kompetanseutvikling av ledelse og ansatte (FD, NHD, JPD, 2003)

Et sentralt begrep innen sikkerhet er begrepet *risiko*, som dreier seg om sannsynligheten for at en sikkerhetshendelse vil inntreffe og om den forventede skadevirkningen hendelsen kan medføre.

God sikkerhet krever en involvert ledelse, kompetanse, gode rutiner, metodikk, nødvendige fysiske og systemtekniske tiltak og ydmyke leverandører. God informasjonssikkerhet er nødvendig for å kunne konkurrere i et stadig mer internasjonalisert og utsatt marked og for å tilfredsstille lovpålagte krav. Til hjelp i dette arbeidet ble den internasjonale sikkerhetsstandarden ISO 17799 vedtatt som norsk standard i mai 2001 (Daler m.fl, 2002).

2.3 Noen utviklingstrekk innen informasjonssikkerhet

Det er relativt lite skrevet om utviklingstrekk innen markedet for informasjonssikkerhet i Norge. Vi får et klart inntrykk av at dette er et område i vekst, men vi har foreløpig ikke kommet over tall som viser omfang og framtidsutsikter. Alt som skrives peker imidlertid på informasjonssikkerhet som et vekstområde. I utenlandske publikasjoner finner vi undersøkelser som viser noe om størrelse og utvikling: I konsulentselskapet PWC sin rapport fra i fjor (PWC 2003) sier de at verdensmarkedet for sikkerhetsteknologi nådde en størrelse på 20 billioner dollar i 2002, som betydde en økning på 20% fra året før. Selv om IT-markedet generelt sank i 2002, ble IT-sikkerhet en topp-prioritet for mange selskaper. PWC deler markedet inn i tre kategorier:

- software
- hardware
- tjenester (konsulentarbeid, implementering, ledelse, opplæring mv)

I 2002 sto tjenester for 48% av inntektene, software for 34% og hardware for 18%. PWC viser til prognoser fra IDC som sier at hardware og software vil vokse med 20% årlig til 2006, mens software vil vokse med 12 prosent årlig. Prognosene er ytterligere spesifisert innenfor markedsområdene, men det tar vi ikke med her. Det er mange faktorer som påvirker denne etterspørselsøkningen: En generell forklaring som gis hos PWC (2003) er at informasjonssikkerhet vil gjennomgå en fundamental transformasjon. Dette fordi IKT vil inngå i alle de viktige forretningsaktivitetene. Informasjonssikkerhet er derfor ikke lenger bare en administrativ "parantes" på overhead-budsjettet eller en teknisk detalj.

Informasjonssikkerhet har derfor steget i strategisk betydning for en organisasjon. Det påvirker organisasjoners formål og ytelse, slik at ledere i langt høyere grad må engasjere seg i dette. Det blir viktig å forstå hvordan informasjonssikkerhet bidrar til verdier i en organisasjon, dvs sammenhengen mellom investeringer i informasjonssikkerhet og organisasjonens mål.

2.4 Informasjonssikkerhet i Innlandet: status og mål

I Innlandet finnes det over 40 aktører som har stor fokus på informasjonssikkerhet. Aktørene omfatter næringsliv, offentlige aktører (brukere/sikkerhetsindustri og utdanningsinstitusjoner), samt store nasjonale/internasjonale aktører hvor sikkerhet er virksomhetskritisk, eller utgjør selve forretningsideen. Aktørene kan deles inn i:

- **leverandører** som leverer produkter og tjenester i markedet, slik som Ibas og Krogh& Hansen i Kongsvinger
- **store brukermiljøer** internt i bedrifter der primærområdet for bedriften er noe annet enn informasjonssikkerhet (eksempelvis informasjonssikkerhet i Norsk Tipping)
- **offentlig virksomhet,** eksempelvis IT-avdelingen i kommuner, der informasjonssikkerhet er et av arbeidsområdene
- **andre:** for eksempel små og mellomstore bedrifter

De mange aktørene i Innlandet betyr at denne regionen kan bli et nasjonalt tyngdepunkt innen informasjonssikkerhet. Det siste året har det blitt etablert et mer formalisert samarbeid for å lage nettverk mellom aktørene. Siktemålet er å utvikle et nettverk eller en næringsklynge for informasjonssikkerhet i Innlandet. Nettverket skal ha flere målsettinger, for å profilere, styrke og videreutvikle etablert miljø, lage arenaer og møteplasser, konkret og faglig målrettet samarbeid, kople og videreutvikle samspillet mellom høgskole/FOU og næringsliv, stimulere til

knoppskyting og nyetableringer, samt å hente ut og skape verdiskapingspotensial. Av disse grunner er det etablert et organisert samarbeid mellom aktørene, som kalles Bluelight, som vi beskriver nærmere nedenfor.

2.5 Metodisk tilnærming

Vi har i over ett år vært observatør i møtene både til den såkalte drivernoden samt styringskomité for nettverket om informasjonssikkerhet i Innlandet - Bluelight. Deltakelsen i over 10 møter har gitt rik førstehåndsinformasjon om de problemstillinger nettverket står ovenfor. Deltakelsen har også gitt tilgang til all skriftlig dokumentasjon som er produsert. Det er denne dokumentasjonen som i stor grad ligger til grunn for avsnittene tre og fire.

I tillegg har vi hatt personlige intervjuer med 11 sentrale personer i nettverket. Data fra disse er også brukt i avsnitt tre, men spesielt i avsnitt fire. Intervjuene ble gjort i april til juni 2003, de fleste personlig, men enkelte pr telefon på grunn av avstand.

Når det gjelder det analytiske avsnittet i avsnitt fem, er dette en blanding av ulike metoder. Delvis er analysene gjort med utgangspunkt i empiriske funn, der vi trekker fram sentrale variabler som kan forklare hvor vellykket nettverket har vært. I tillegg er også noen av analysene relatert til relevante nettverksteorier.

2.6 Hva er Bluelight?

Bluelight er betegnelsen på et innovasjonsnettverk av sentrale aktører innen området informasjonssikkerhet, med utgangspunkt i kompetansemiljøer i Innlandet. Bluelight er et prosjekt i det såkalte ”Arena-programmet – innovasjon i nettverk” i regi av Innovasjon Norge (tidligere SND), Norges Forskningsråd og Siva. Nettverket består av sentrale nasjonale og internasjonale aktører både fra næringslivet (sikkerhetsindustri, brukere, og konsulenter), offentlige aktører og utdanning/FOU-aktører. Gjøvik Kunnskapspark er prosjektleder og operatør. Blant aktørene finner vi:

- Telenor
- IBAS
- Thales
- Norsk Tipping
- PricewaterhouseCoopers
- Sambandsregimentet Jørstadmoen
- Gjensidige NOR
- Sparebanken Hedmark
- ErgoGroup
- Helse Øst RHF
- Institutt for Datasikkerhet
- Secure-Group
- Gjøvik Kunnskapspark
- Høgskolen i Gjøvik

Bluelight sin visjon er å være anerkjent som ett av de ledende kompetansenettverk innen fagområdet informasjonssikkerhet i Europa.

Bluelight fikk i mai 2004 egen hjemmeside: www.bluelight.no

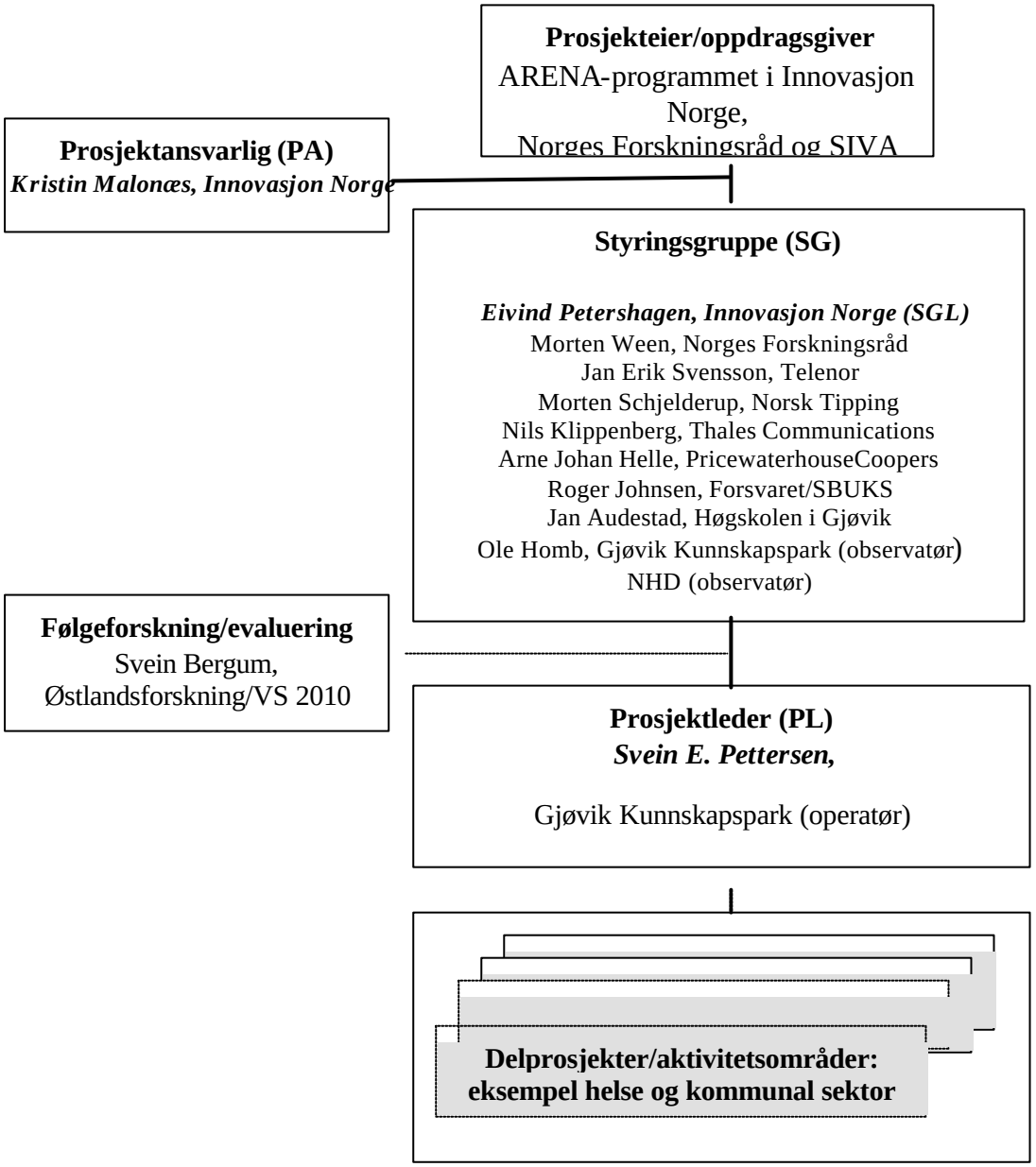
Målsettinger

Formålet med Bluelight er, i følge planer fra mars 2004, å generere kompetanseutvikling, bevissthet, verdiskaping og nyskaping relatert til informasjonssikkerhet i et internasjonalt perspektiv. Bluelight skal styrke deltakerne og sørge for etablering av nye aktører i markedet. Bluelight skal bistå utviklingen av Norwegian Information Security Laboratory (NISlab) ved Høgskolen i Gjøvik (HiG), og befeste NISlab som det faglige tyngdepunktet i nettverket. NISlab er FOU-enheten innen informasjonssikkerhet ved HiG.

Bluelight skal være pådriver for videreføring og videreutvikling av Masterstudiet i informasjonssikkerhet, og utvikling av andre studietilbud innen fagområdet. Bluelight skal også via NISlab innen 2005 også ha initiert/deltatt i minst ett nordisk og ett internasjonalt innovasjonsprosjekt. Innen samme tidsrom skal Bluelight også bidra til minst tre produkt/tjenestelanseringer og opprettelse av tre levedyktige virksomheter. Av andre målsettinger kan nevnes bidrag til to nasjonale og en regional faglige arena for informasjonssikkerhet. Bluelight skal innen utgangen av 2004 ha lagt grunnlaget for sin videreføring som et nasjonalt ekspertsenter (Center of Expertise-CoE).

Organisering av Bluelight

Fram til mars 2004 besto Bluelight av en styringskomité for strategiske saker, en drivernode som skulle være det operative organet, samt ulike delprosjekter. På styringskomitemøtet i mars 2004 ble det vedtatt å legge ned drivernoden. Det operative arbeid skulle heller gjøres i ulike delprosjekter, slik som for eksempel kommunal sektor og helsevesen. Organisasjons- og ansvarsforhold i juni 2004 er vist i vedlagte skisse, der også navn/organisasjon på deltakere finnes:



I gjennomgangen av målsettinger for Bluelight, ble det nevnt enkelte navn/begreper, som trenger nærmere forklaringer: *Nis Lab, Master studium, og Security partner*

NISLAB

NISlab står for Norwegian Information Security laboratory. NISlab er fellesbetegnelsen på det akademiske miljøet innen informasjonssikkerhet ved Høgskolen I Gjøvik. NISlab ble grunnlagt i januar 2003, og aktivitetene er forskning og utdanning. Masterstudiet i informasjonssikkerhet tilbys via NISlab. Ved NISlab er det nå etablert et fagmiljø med to fulltids professorer, flere vitenskapelige ansatte med førstestillingskompetanse, samt 5 doktorgradsstipendiater. Det er også igangsatt omfattende forskningsaktivitet med finansiering fra Norges Forskningsråd. De prioriterte områdene er: ”Security Metrics”, samt problemstillinger mot helsesektoren og

kommunal sektor. NISlab sto sentralt i to internasjonale forskningskonferanser på Gjøvik høsten 2003, hvor til sammen ca 150 forskere deltok. Nislab har eget hjemmeside: www.nislab.no.

Masterstudium i informasjonssikkerhet ved Høgskolen i Gjøvik (HiG)

Masterutdanningen i informasjonssikkerhet tilbys av HiG i samarbeid med de akademiske partnerne KTH (Kungliga Tekniska Högskolan-Stockholm) og AFIN (Avdeling for forvaltningsinformatikk – Universitetet i Oslo). I tillegg er disse bedriftene støttespillere både økonomisk og kompetansemessig: Telenor, Thales, PricewaterhouseCoopers, Norsk Tipping, Gjensidige Nor og Sparebanken Hedmark. Medvirkende er også Innovasjon Norge, Norges Forskningsråd og omstillingsprogrammet "Morgenlandet".

Målet for studiet er å gi studentene holdninger, kunnskaper og ferdigheter som gjør dem i stand til, på en profesjonell måte, å planlegge, gjennomføre og lede arbeid innen informasjonssikkerhet i både offentlig og privat sektor. Studentene skal tilegne seg et grunnlag for videreutvikling av faget og av egen kompetanse. Etter å ha fullført studiet skal studentene ha holdninger, kunnskaper og ferdigheter om de relevante teknologiske, samfunnsmessige og rettslige aspekter ved informasjonssikkerhet. Dette innebærer inngående kjennskap til temaene konfidensialitet, integritet og tilgjengelighet til informasjon. Studentene skal gjennom en prosjektoppgave og hovedoppgave fordype seg i minst ett faglig tema rettet mot anvendt eller teoretisk informasjonssikkerhetsproblematikk.

De fag som inngår i studiet er: informasjonssikkerhet og samfunnets sårbarhet, systemutvikling og sikkerhetsarkitektur, kryptologi, sikkerhetsledelse, rettslige aspekter, sikkerhet i distribuerte systemer, to fordypningsemner og masteroppgaven. Det unike med dette er at informasjonssikkerhet sees i et helhetlig perspektiv, med fokus på både teknikk, jus, ledelse og samfunnsaspekter. Opptakskrav til studiet er minimum 3-årig høgskole- eller universitetsutdanning, samt kompetanse i matematikk (15 studiepoeng) og informatikk (60 studiepoeng). Studiet fører fram til internasjonal mastergrad ved KTH. Studielengden er 2 år på heltid (120 studiepoeng). Det er 30 studieplasser, og til disse har det vært stor søkning så langt med over 100 søkere hvert år. Masterstudiet har for tiden 50 heltids- og 15 deltidsstudenter.

Security Partner

SecurityPartner er et selskap som er under etablering våren 2004, som en direkte "spin-off" fra Bluelight. Selskapets formål er å forvalte og videreutvikle metoder og verktøy innen informasjonssikkerhet basert på bidrag fra aktører i Bluelight. Selskapet blir etablert i henhold til et franchisekonsept. Aktører som blant annet Telenor, Norsk Tipping, ErgoGroup og PricewaterhouseCoopers deltar aktivt i arbeidet med etableringen av selskapet. Produkter fra disse firmaene er basis for porteføljen i SecurityPartner. Det er foreløpig tre produkter i porteføljen til SecurityPartner, fra mer overordnet temperaturmåling av informasjonssikkerhet i bedriften til mer omfattende analyser av status og behov. E-læring innen informasjonssikkerhet vurderes også. Produktene fra Security Partner ventes på markedet de nærmeste månedene, og er de første produkter/tjenester i kjølvannet av Bluelight. SecurityPartner holder til i Gjøvik Kunnskapspark, som også leder arbeidet.

2.7 Nærmere om enkelte sentrale aktører innen informasjonssikkerhet i innlandet

En av grunnene til at det satses på informasjonssikkerhet i Innlandet er som nevnt at det finnes 40 aktører i regionen, både leverandører, store brukere, FOU-institusjoner samt offentlige aktører

som Innovasjon Norge. Nedenfor presenteres et utvalg av aktørene, med vekt på også å få med noen leverandører og ikke bare brukere.

Sambandsregimentet Jørstadmoen (SBUKS)

I Bluelight er Forsvaret først og fremst representert ved sikkerhetsseksjonen som er lokalisert på Jørstadmoen nord for Lillehammer. Seksjonen ledes av major Roger Johnsen og har ca. 15 ansatte. Johnsen rapporterer til øverste leder på Jørstadmoen, brigader Arve Senderud og deltar i ledergruppa og i strategiarbeidet som pågår. Jørstadmoen er både hovedsete for Sambandsinspektøren og UKS Hærens Samband (Utdannings- og kompetansesenter). Utdanningstilbudene er befalsskole, ingeniørskole og rekruttskole. Det er ca. 230 ansatte totalt. SBUKS utvikler og prøver ut informasjons- og sambandssystemer for Hæren og er kompetansesenter for kontor, arkiv og meldingstjenesten i Forsvaret. Sikkerhetsmiljøet på Jørstadmoen skal etter hvert ha et nasjonalt ansvar for sikkerhet og være Forsvarets kompetansesenter for informasjonssikkerhet. Sikkerhet er en av tre strategiske bærebjelker ved SBUKS, og de to andre områdene er "kommunikasjonssystemer" og "informasjonssystemer" De som arbeider i sikkerhetsseksjonen driver både med utvikling og undervisning. Det har lenge vært et nært samarbeid mellom SBUKS og Høgskolen på Gjøvik (HiG), ved blant annet utveksling av forelesere.

Jørstadmoen har en lang historie innen samband og sikkerhet. Jørstadmoen militærleir ble opprettet i allerede i 1787. Fra 1787 hadde "Det Nordre Dragoncompagnie" sin ekserserplass på Onsummoen ca 600 meter nordvest for Jørstadmoens nåværende indre leirområde. Etter at kavaleriet brukte leiren de første årene, overtok infanteriet i 1830, og de disponerte leiren til 1940. Under 2. verdenskrig brukte den tyske okkupasjonsmakten leiren som transittleir for sovjetrussiske krigsfanger. Etter at de 4-5000 tyske krigsfangene var hjemsendt, ble leiren klargjort for Hærens samband (HSB) som inntok Jørstadmoen som første avdeling. Hærens Samband ble opprettet som eget våpen sommeren 1945 og etablerte seg på Jørstadmoen samme høst .

Telenor, spesielt om sikkerhetstaben i Lillehammer

Telenor er den største tele- og kommunikasjonsaktøren i Norge, men har også internasjonale operasjoner for eksempel innen mobilkommunikasjon. De har årlige driftsinntekter på ca 50 milliarder og har ca 14.000 ansatte i Norge, hvorav hele 1000 i Mjøs-regionen. Dette er den største konsentrasjonen av Telenor-sysselsetting utenom Oslo. Innenfor dette store selskapet er det sikkerhetsstaben som representerer Telenor i Bluelight-arbeidet. Denne har hovedbase i Lillehammer, og ledes av sikkerhetsdirektør Jan Erik Svensson. Han er stabsdirektør, men har også et faglig ansvar overfor forretningsområdene (eksempelvis: Networks, Business Communication, Mobil, Telefoni & Internett, Broadcast). Fra nyttår 2002/2003 ble sikkerhetsarbeidet i Telenor organisert på en ny måte, og i den nye sikkerhetsfunksjonen sitter representanter fra alle enhetene. Alle sikkerhetsansvarlige samles i en konsernfelles funksjon, med sikkerhetsdirektør Jan Erik Svensson som faglig ansvarlig. Han leder et faglig miljø på mellom 50-60 personer, som er spredt på flere steder, selv om ledelsen og 6 andre personer i sikkerhetsstaben er plassert i Lillehammer (andre steder: 2 i Bergen, 2 i Trondheim, 1 i Bodø, resten i Oslo). Sikkerhetsledelsen er det øverste faglige beslutningsråd og består av sikkerhetsdirektør, sikkerhetssjefene i forretningsområdene (8 personer), samt fagansvarlige for henholdsvis informasjonssikkerhet, kriminalitet og holdninger. Oppgaver skal samordnes og ivaretas på tvers i hele organisasjonen. Sikkerhetsfunksjonen hadde fire hovedfokus i 2003: holdninger, datasikring, bedre rapportering og forenkling av regelverk.

Norsk Tipping, spesielt om sikkerhetsavdelingen

Norsk Tipping AS ble etablert i 1946, og flyttet til Hamar i 1975, etter beslutning i Stortinget. Hovedproduktet var lenge fotballtipping, men de siste årene har en rekke nye produkter blitt lansert, slik som Lotto, Oddsen, Joker, Extra og Flax. Muligheter for spill gjennom nye kanaler som Internett tilbys. Antall ansatte i Norsk tipping er ca 290. Omsetningen i 2002 var 9,73 milliarder kr, en fordobling på ti år.

Norsk Tipping har en egen sikkerhetsstab som ledes av sikkerhetsdirektør Morten Schjelderup. Staben har 6 medarbeidere. Disse medarbeiderne har litt forskjellig bakgrunn hvorav bl.a to har økonomisk utdannelse. De er rekruttert blant annet fra Forsvaret og regionale høgskoler. Sikkerhetsstaben har fire hovedoppgaver:

a) administrasjon (brann, adgangskontroll mv)
b) datasikkerhet: metodeutvikling, prosessdriver ifm prosjekter
c) risikostyring
d) spillsikkerhet (hvordan foregår trekningene)

Sikkerhetsstaben skal hjelpe andre avdelinger med hensyn til sikkerhetskrav, for eksempel mot teknologiavdelingen.

Ibas

Ibas er et selskap som startet i 1978 med vedlikehold av utstyr for Televerket (Telenor). Gradvis gikk de over til å reparere datamaskinutstyr tidlig på 1980-tallet. I 1982 startet de med datarekonstruksjon. Siden den gang har de bygget opp kompetanse, utviklet eget verktøy og utstyr. Deres erfaring og kompetanse innen datarekonstruksjon førte Ibas over til dataslettingstjenester i løpet av 1990-årene. I dag er Ibas et av verdens ledende selskaper innen datarekonstruksjon og datasletting og satser også på dataetterforskningstjenester. Ibas er representert i hele 18 land. De har datterselskaper i Benelux, Sveits, Italia, Spania, Tyrkia og Singapore. I tillegg har selskapet distributører i Nederland, Belgia, Luxembourg, Sveits, Spania, Italia, Tyrkia, Hong Kong, Canada og USA. Hovedkontoret ligger i Kongsvinger.

Mens Ibas opprinnelig var et norsk selskap på det norske markedet, hentes nå 80 prosent av inntektene utenfor Norge. Ibas er en del av Norman Gruppen. Ibas startet tidlig med rekonstruksjon av data i det europeiske markedet. En utfordring har vært å holde tritt med utviklingen innen lagringsteknologi. De har investert mye innen FOU, og har flere årsverk til dette. Svært varierte oppdrag har skaffet Ibas en betydningsfull erfaringsdatabase, kompetanse og renomé. De bestreber seg på 100% produktnøytralitet og å ha en uavhengig posisjon i markedet.

Ibas har i dag 66 ansatte i konsernet, hvorav 43 er Norge. De fleste av disse er lokalisert i Kongsvinger.

Krogh & Hansen AS

Krogh & Hansen AS er et konsulentselskap innenfor IKT, som har tre ansatte. De er lokalisert i Kongsvinger. Kjernevirksomheten deres er innenfor IKT-rådgivning, e-handel, IKT-sikkerhet, bredbåndsteknologier og prosjektledelse. Markedet er regionalt og mot Oslo-markedet.

Innenfor IKT-sikkerhet tilbyr de tjenester innen sikkerhetspolicy, sikkerhetsorganisering, katastrofeberedskapsplaner, og fastsetting av sikkerhetsmål.

Senter for it-samhandling AS (SitS)

Dette er et selskap som primært arbeider med IKT-anvendelse i kommunesektoren og øvrig offentlig sektor på nasjonal basis. SitS er lokalisert i Fakkelgården på Lillehammer og har i tillegg et avdelingskontor i Vågå Næringshage i Vågå. Selskapet ledes av adm.dir. Narvin Tangen. SitS har utviklet seg fra 1 til 4 ansatte siden opprettelsen i 1997 og har en omsetning på ca. 3,5-4 mill. SitS er et aksjeselskap som eies av en gruppe offentlige aktører: Kommunenes Sentralforbund, Oppland fylkeskommune og syv kommuner i Oppland. Selskapets tjenester er rådgivning, prosjektutvikling, prosjektledelse, ivaretakelse av sekretariatsfunksjoner og kurs- og kompetanseutvikling, og arbeidet spenner over ulike tema som bredbåndsanvendelser, e-handel, e-forvaltning, geografiske informasjonssystemer, strategi og ledelse, informasjonssikkerhet og omstilling og samhandling. En av selskapets hovedoppgaver er å være sekretariat for foreningen GEOLOK (geodata i lokalforvaltningen) og å arrangere deres årlige konferanse. SitS har også fått en viktig rolle for den kommunale foreningen for informasjonssikkerhet (www.kins.no.) hvor SitS er sekretariat.

-KINS:

Foreningen "Kommunal informasjonssikkerhet" (KINS) ble startet etter initiativ fra Bluelight våren 2003. KINS har som mål å bli den nasjonale arenaen for spørsmål rundt informasjonssikkerhet i kommunal sektor. En viktig aktivitet så langt har vært å arrangere to konferanser, den siste med hele 170 deltakere i mars 2004. Sits har vært arrangør av konferansene. Kins har i april 2004 hele 64 kommuner, fylkeskommuner og private bedrifter som medlemmer, etter under ett års drift. Hele 21 av kommunene/fylkeskommunene kommer fra Hedmark/Oppland. I tillegg er det et økende antall medlemmer fra næringslivet. Formålet med foreningen er å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner. Dette skal skje gjennom samhandling med aktuelle fagmiljøer, etablering av arenaer for kompetanseheving og utvikling av standarder. Foreningen søker å få til samarbeidsarenaer, lager kurs og konferanser og har etablert egen Internett-side. I tillegg skal en komme med veiledere til praktisk arbeid. Foreningen vil bidra til utvikling av standarder på sikt.

Andre aktører/miljøer

I presentasjonen foran valgte vi å konsentrere oss om noen regionale aktører, og vi ville også presentere leverandører som for eksempel Ibas og Krogh & Hansen. Vi har også i liten grad presentert Innovasjon Norge, som utvilsomt har spilt en viktig rolle både i oppstarten og i hovedprosjektet.

Bluelight er imidlertid i stor grad avhengig av sentrale nasjonale aktører. Blant disse må spesielt nevnes Thales og Price WaterhouseCoopers (PWC). Begge disse sitter i styringsgruppen for Bluelight. Thales er en stor nasjonal og internasjonal leverandør som innehar stor kompetanse innen informasjonssikkerhet. De har etablert et par arbeidsplasser i Lillehammer som følge av sitt Bluelight-arbeid. PWC har engasjert seg meget i Master-studiet på Gjøvik, og støtter dette både økonomisk og kompetansemessig.

Firmaet Ergogroup er også en viktig aktør, spesielt knyttet til deres kompetanse om smart kort. En gruppe på ca 10 personer er lokalisert i Gjøvik, og har deltatt i flere interessante utviklingsprosjekter i regionene blant annet mot Norsk Tipping og helsevesenet.

Av aktører som har kommet inn "utenfor regionen" i den senere tid, kan også nevnes firmaet Secure-Group, som har hovedbase i Oslo, og foreløpig dekker innlandet derfra.

Oppsummering

Det er fagmiljøer innen informasjonssikkerhet på de fleste større stedene i Innlandet, både Lillehammer, Gjøvik, Hamar og Kongsvinger. Hver av disse stedene har sine sterke aktører og sin spesielle profil. Lillehammer har Telenor, Forsvaret, Thales og kommunen som sentrale aktører. Gjøvik har kunnskapsparken og Høgskolen, foruten næringsaktører som Ergo Group. Hamar har Norsk Tipping med samarbeidspartnere, mens i Kongsvinger er Ibas den store.

Antall sysselsatte i Innlandet innen informasjonssikkerhet er foreløpig litt vanskelig å måle, avhengig av definisjon og avgrensning av f.eks brukermiljøene. Antagelig er det et antall på mellom 200-300 totalt sysselsatte, hvorav Ibas er den største med mellom 30-40 ansatte på Kongsvinger. Det er mange relativt små miljøer fra 2-5 personer, og mange av aktørene er brukermiljøer. Det er relativt lite antall leverandører så langt. Verdt å merke er at alle de miljøene som er nevnt i oppsummeringene satser på FOU, der forholdstallet mellom forskning og utvikling nok varierer mellom de forskjellige aktørene.

En stor aktørgruppe i Innlandet er også de offentlige virksomhetene med høgskoler og kommuner. Men sysselsetting innen informasjonssikkerhet her begrenser seg oftest til en liten del av IT-sjefens stilling. Antallet kommuner der informasjonssikkerhet er satt på dagsorden har økt de senere årene, ikke minst takket være KINS.

3. Utvikling av nettverket for informasjonssikkerhet i innlandet

3.1 Innledning

I dette avsnittet skal vi spesielt beskrive enkelte hovedpunkter i prosessen som førte fram til etableringen av Norges første masterstudium i informasjonssikkerhet, som igjen førte til et enda bredere samarbeid i det nettverket som i 2003 fikk betegnelsen ”Bluelight”. Dette betyr at det er de siste årene som er i fokus, og ikke de mange uformelle kontakter som det har vært i regionen mellom personer spesielt fra Jørstadmoen, Telenor og leverandører, som går atskillig lenger tilbake i tid. I Forsvaret på Jørstadmoen har det vært engasjement rundt sambands- og kommunikasjonsspørsmål siden 2. verdenskrig. De har hatt et sterkt fagmiljø, og andre personer har blitt utdannet der og startet i andre funksjoner i regionen blant annet i Televerket/Telenor. Innenfor ”gamle Televerket” ble flere spesialistfunksjoner flyttet fra Oslo til Lillehammer på 1980-tallet. Flere av disse hadde med sikkerhet og kommunikasjon å gjøre, blant annet fagenheter for driftskontroll og alarmoverføring.

Et utgangspunkt for satsingen på informasjonssikkerhet i Innlandet var at det i innledende arbeid i 2001, blant annet gjennom markedsundersøkelser, ble identifisert minst 40 aktører som hadde stor fokus på informasjonssikkerhet. Derfor ble et arbeid satt i gang, der første mål var etablering av utdanningstilbud. Først i neste fase ble samarbeidet utvidet til et mer generelt innovasjonsnettverk.

3.2 Initiativtakerne

Det er litt nyanser mellom informantene med hensyn til når startskuddet for nettverket var, og ”hvem som tok hvilke telefoner”. Hos enkelte i Telenor, Jørstadmo-miljøet og hos leverandøren Thales, hadde det i lengre tid vært snakket om ”å få til noe innen informasjonssikkerhet i Innlandet”. Den som flest nevner som en nøkkelperson i starten er sikkerhetsdirektør Jan Erik Svensson i Telenor. Han har bakgrunn fra Jørstadmo-miljøet (i likhet med flere andre) og deretter Telenor. Hans innsats blir spesielt knyttet til utviklingen av Masterstudiet i informasjonssikkerhet, som var målsetting for den første fasen av samarbeidet. I det videre løp for utvikling av nettverket er også Svein Pettersen/GKP og Eivind Petershagen/Innovasjon Norge viktige personer. Flere av de som nå er sentrale i styringskomitéen, har tidligere vært kolleger av Svensson, eller vært forretningspartnere. Eksempler på dette er nettopp Svein Pettersen ved Gjøvik Kunnskapspark/HiG (tidligere medarbeider hos Svensson), og Morten Schjelderup i Norsk Tipping, som tidligere har vært sikkerhetssjef i Telenor Mobil. Han hadde da en god del faglig samarbeid med Svensson.

En litt alternativ historie om oppstarten fikk vi av en av Innovasjon Norge sine representanter som sa at informasjonssikkerhet dukket opp som et satsingsområde (ved siden av e-læring og medieproduksjoner) under arbeidet i en regional arbeidsgruppe der blant annet Otto Kaltenborn fra Østlandsforskning og Bjørn Nørstegård/Lillehammer Kunnskapspark deltok. Dette var våren 2000. Det var også dette året at Jan Erik Svensson første gang tok kontakt med SND. Det synes derfor å være et sammenfall av satsing både fra INNOVASJON NORGEog fra bransjen selv.

Vi kommer tilbake til initiativtakernes motivasjoner senere i kapitlet.

3.3 Faser og viktige milepeler

Arbeidet med nettverket kan deles i tre faser: forstudie, forprosjekt og hovedprosjekt. De to første fasene er spesielt knyttet til utvikling av Master-studiet, mens hovedprosjektet er knyttet til Arena-satsingen til Innovasjon Norge med formål å utvikle et bredere innovasjonsnettverk.

Forstudie

En forstudie om temaet startet primo 2001. Et viktig møte som initierte dette skjedde 9. januar 2001 hos daværende SND. Jan E. Svensson i Telenor hadde tatt kontakt med INNOVASJON NORGEved Kristin Malones, og Høgskolen i Gjøvik. INNOVASJON NORGEhadde begynt å identifisere området som interessant. I 2000 hadde det også vært litt møteaktivitet, men arbeid ble ikke satt i gang for alvor før i 2001 i påvente av finansiering.

Forprosjekt

Dette varte fra mai 2001 til høst 2002 og hadde finansiering fra Kommunal og regional departementet. Hovedfokus var etablering av Masterstudium.

Forprosjektgruppe ble dannet fra høsten 2001. Svein Pettersen kom inn som "daglig leder" fra Gjøvik Kunnskapspark medio 2001, direkte fra sikkerhetsstaben i Telenor. Utdanning var sentralt i forprosjektet. I september 2001 var det "workshop" der Telenor, Høgskolen i Gjøvik og Jørstadmoen var noen av deltakerne. Jørstadmoen hadde planer om en "Bachelor" innen sikkerhet. Det ble derfor enighet om å satse på et nytt Master studium. En skisse til studieplan ble klar i februar 2002, og studieplanen ble vedtatt våren 2002. Nye aktører ble dratt inn i forbindelse med utviklingen av studieplanen, blant annet sikkerhetsdirektør Morten Schjelderup i Norsk Tipping. Studieoppstart skjedde samme høst, allerede i 2002 kun ett år etter at planleggingen hadde begynt. Studiet ble en konkurrent av studier ved UNIK/Kjeller og NTNU, men særtrekket ved HiG-studiet er breddeprofilen med fokus på blant annet teknologi, jus og sikkerhetsledelse. Finansieringskilder av forprosjektet var Telenor, Norsk Tipping, Morgenlandet og SND. En viktig aktør i forprosjektet var også Høgskolen i Gjøvik. Det lyktes ikke å etablere samarbeid med en norsk universitetspartner. Derfor ble HiG's allerede eksisterende kontakter med Kungliga Tekniska Högskolan i Stockholm benyttet. Rektor på HiG spilte en aktiv rolle; Det ble brukt midler fra nedlegging av skogavdeling på Brandbu, og det ble søkt omstillingsmidler for blant annet stillinger. Det ble tatt en risiko ved å satse på området, men alle trender, til og med egeninitierte markedsundersøkelser, viste at dette var et område i sterk vekst.

Vi har beskrevet innholdet i Masterstudiet foran i avsnitt tre. Så langt har studiet vært en suksess: Det har vært stor søknadsmasse de to første årene, og de første kandidatene blir uteksaminert i år. Både studenter og lærerstab virker fornøyde, og studiet har hatt ringvirkninger i form av blant annet etableringen av NISlab.

Hovedprosjekt

Der det er oppnådd mest konkrete resultater så langt er i forprosjektet som førte til etableringen av Masterstudiet. Mye av vurderingene rundt suksessen av nettverkssamarbeidet er nok også basert på erfaringene fra etableringen av studiet.

Den tredje fasen som skulle bringe samarbeidet videre utover "bare" utdanning var i form av et hovedprosjekt. Dette ble knyttet opp mot den såkalte "Arena satsingen. Hovedprosjektet ARENA

Informasjonssikkerhet ble initiert sommeren 2002. ARENA Informasjonssikkerhet er en regional innovasjonspilot i ARENA-programmet som er operativt ledet av Innovasjon Norge og som gjennomføres i samarbeid med Norges Forskningsråd og SIVA. Høsten 2002 ble prosjektet organisert. Det ble dannet en styringsgruppe for å ta seg av de strategiske spørsmål. Videre ble det etablert en såkalt drivernode, som skulle være det operative organet for å iverksette styrings-komitéens strategier samt spille inn saker til styringskomitéen. Drivernoden skulle være en kjernegruppe i prosjektet som i hovedsak skal adressere strategi/handlingsplan, kompetanseforvaltning/-spredning, vedlikehold av eksternt nettverk og initiering, gjennomføring og terminering av sentrale prosjektaktiviteter. Drivernoden ble som nevnt nedlagt i mars 2004, etter et drøyt års eksistens. Hovedbegrunnelsen for dette var blant annet at strategiske spørsmål også kom opp her, og fordi variasjonen i problemstillinger ble for stor til å håndtere i en gruppe. Det som nettverket vil sitte tilbake med er ett strategisk organ (nemlig styringskomitéen) samt mer spesialiserte faggrupper.

Styringskomitéen hadde sitt første møte i desember 2002. I møtene som ble avholdt utover i 2003, var det enighet i prosjektet om viktigheten av å gå relativt bredt ut i dette første året av hovedprosjektet. Så ville man i videre prosjektutvikling fra 2004 måtte prioritere og fokusere enkelte områder på bekostning av andre. I 2003 var det mye fokus på visjoner, målsettinger, aktivitetsplaner for nettverket, samt en "brandingprosess". Sistnevnte aktivitet var den som ga mest synlige resultater på kort sikt. Begrepet *"NIS-nettverket: næringsklynge for informasjonssikkerhet"* var for komplisert. Etter en kreativ prosess, ble begrepet "Bluelight" tatt i bruk fra midten av 2003, med undertittel: "enabling security".

3.4 Motivene for deltakerne

Vi skal nå gå inn på noen av resultatene fra intervjuundersøkelsen vi har hatt med sentrale deltakere i Bluelight. Disse intervjuene ble tatt opp for ca ett år siden, på våren 2003. Deres svar om erfaringer må sees i lys av tidspunktet, og erfaringer er nok i stor grad knyttet til erfaringene med å få til Masterstudiet. Arbeidet med nettverket for øvrig var i en tidlig fase.

Behov for kompetanseutvikling i bransjen og for den enkelte bedrift har nok vært den viktigste motivasjonen i startfasen for de aller fleste deltakerne. Telenor sier for eksempel at deres viktigste motiv for deltakelse har vært å tilgodese eget behov for kompetanseutvikling innen informasjonssikkerhet, samt å ivareta Telenors samfunnsansvar for å bedre sikkerhetsholdninger/-kompetanse. Å øke bevisstheten om informasjonssikkerhet i samfunnet er nok også et motiv hos flere aktører. Flere påpeker at de så dette som en mulighet til å få til en nasjonal satsing innen informasjonssikkerhet. At så mange sentrale miljøer/personer ble med, var fordi de så at "nå gikk det et tog" innenfor dette fagområdet.

Flere av aktørene har støttet Master-studiet økonomisk med betydelige summer. Disse har forventninger om at samarbeid i nettverk kan gi "payback" i form av raskere produktutvikling, næringsutvikling og eksport. Deltakerne ser utviklingen av nettverket som et viktig verktøy for å få til ting som de enkeltvis ikke klarer, dvs skape vinn-vinn situasjoner. En aktør som Thales sier at deres viktigste mål med nettverket er at det skal gi grunnlag for eksport av produkter, der kunnskap, idéer og penger er forutsetninger. Nettverk er positivt fordi det gir mulighet for erfaringsutveksling, synergier og vinn/vinn situasjoner, det kan gi større legitimitet, og man kan oppnå noe som er vanskelig å gjøre alene. *"I nettverk snakker vi uten penger, med åpenhet og tillit, og ikke som i et leverandør/kundeforhold"*, sa en av informantene. Samtidig kan et nettverk også gi mulighet for leverandører å få fram brukerreaksjoner. Et nettverk kan også være velegnet, gjennom sin legitimitet, for å fremme krav mot myndigheter for å påvirke rammebetingelser, FOU mv.

For leverandører som Thales og Ibas er nok deres motiver mer knyttet til markedsføring/salg og profilering innen informasjonssikkerhet. Medlemskap i Bluelight gir også økt legitimitet. For Forsvaret antas det at deltakelse i nettverket gir økte kontaktmuligheter mot private bedrifter. For de private bedriftene er kontaktmulighetene den motsatte veien.

Vi merket oss også en uttalelse på et møte i styringskomitéen om at Jørstadmoens deltakelse i nettverket er positivt fordi deltakelse gir legitimitet til deres miljø og er et argument for fortsatt lokalisering til Jørstadmoen. Det er sannsynlig at dette motivet også gjelder for andre av de aktørene som har base i Innlandet, som f.eks Telenor Sikkerhet, selv om dette ikke ble nevnt eksplisitt i intervjuet med sikkerhetsdirektør Svensson.

Fra Innovasjon Norge (tidligere SND) sin side var grunner til at de satset på nettverk innen dette fagtema at de fant spiren til et kompetansemiljø i området, spesielt rundt Jørstadmoen. Det talte også positivt at det var engasjement blant bedriftene f.eks hos Telenor. Bluelight har vært en prioritert aktivitet hos Innovasjon Norge de senere år.

Andre motiver for bedriftene er ekstern profilering, og å vise sosial ansvarlighet. Slike "ikke-rasjonelle" motiver, både organisasjonsmessige og personlige, knyttet til regionalt engasjement og idealisme for næringsutvikling i Innlandet, ble nevnt av flere.

3.5 Aktørene i nettverket - utvelgelse og sammensetning

De kriteriene som har styrt valg av aktører i nettverket har vært å få inn sentrale miljøer med kompetanse innen området, og som jobber målrettet. Det har vært lagt vekt på å få med både lokale/regionale- og nasjonale aktører, og med ulik tilnærming til informasjonssikkerhet, både leverandører og brukere. I utvelgelsen av deltakere har eksisterende personlige nettverk vært viktige. Mange av deltakerne har sin bakgrunn i Forsvaret/Jørstadmoen, men flere jobber nå i andre posisjoner. Eksempler på dette er for eksempel de tidligere nevnte Morten Schjelderup i Norsk Tipping (tidligere i Telenor Mobil) og Svein Pettersen ved Gjøvik Kunnskapspark (tidligere i Telenor Konsernstab sikkerhet). Det har også i lengre tid vært gode forretningsrelasjoner mellom aktører som Telenor Sikkerhet, Thales og Forsvaret.

Det har vært lagt vekt på at de som har deltatt har kunnet bidra med noe, både kompetansemessig og/eller finansielt. Dette har vært viktigere enn hvor personene kommer fra. Kriterier for å ta opp nye medlemmer av drivernoden ble for øvrig diskutert høsten 2003. Det har også skjedd mindre justering av styringskomitéen ved tre anledninger: spesielt for å styrke kommersialiseringskompetanse (Homb fra Gjøvik kunnskapspark), for å styrke sentrale aktører (få inn Helle fra PWC) og styrke forbindelsen mellom FOU og innovasjon ved å få inn professor Audestad fra HiG inn i styringskomitéen i mars 2004.

Ingen føler at det er noen problemer med samarbeid mellom nasjonale og lokale aktører. Dette kan også skyldes at informantene i stor grad representerer begge deler. Det er derfor problematisk å si om de store aktørene er lokale, regionale, nasjonale eller internasjonale. De fleste av de toneangivende aktørene i nettverket opererer i alle disse rollene. Som sikkerhetsdirektøren i Norsk Tipping sa: vi betrakter oss primært som nasjonal aktør, deretter som lokal aktør og tertiært som internasjonal aktør. Han anslo sin arbeidsfordeling til å være 60% nasjonalt, 10% regionalt og 30% internasjonalt. Det er mulig at det er noenlunde tilsvarende også for Telenor sikkerhetsstab.

I målsettingene for Bluelight er det nedfelt at nettverket er både lokalt, regionalt og internasjonalt. Dette framheves av mange som en styrke. Vi merket litt ulik vektlegging av prioritering mellom regionale og nasjonale aktører. Dette er naturlig og synes ikke som noe problem. Det eneste må være av praktisk art, som prioriteringsproblemer av møtene på grunn av mye reising. Høsten 2003 var et par av deltakerne i styringskomitéen ofte forhindret fra deltakelse.

3.6 Grad av suksess: hva er oppnådd og forklaringsfaktorer fra aktørene

De fleste av informantene mener at Master studiet er det viktigste som er oppnådd så langt. Dette var jo også primærmålet for forprosjektet. Det er mange som synes at dette var en lur prioritering fordi dette gav en konkret gevinst i starten, alle anså dette som nyttig og det var ukontroversielt. NIS-lab (dvs forskningsstudioet ved HiG) nevnes også av flere som like viktig, selv om dette kun er i startfasen ennå. Det virker også som det er noe ulikt grad av engasjement for NIS-lab. Men det aksepteres fordi det er nødvendig for Master-statusen. Av flere legges det vekt på at dette må være praktisk orientert og skape resultater.

Det er kun Norsk Tipping som eksplisitt nevner arbeidet med Security Partner som en viktig milepel,. Security Partner er som nevnt kommersialiseringsprosjektet i regi av Bluelight, der produktet som skal selges er metoder og verktøy for analyse av behov for informasjonssikkerhet i organisasjoner. Den beskjedne prioritering skyldes antagelig at prosjektet var i tidlig kommersialisering da vi intervjuet. Da mange av aktørene betoner mer vektlegging på forretningsutvikling og produktutvikling, er det nok egentlig flere som ser Security Partner som viktig, enn uttrykt i intervjuene. Responsen i de senere møtene, etter intervjuene, kan tyde på dette. Samtidig er det fremdeles usikkerhet rundt hva marked og økonomi er i dette prosjektet. Enkelte lurer også på om Security Partner kan bli problematisk fordi en slik virksomhet kan komme i konkurranse med produkter fra enkeltaktører i nettverket.

Flere informanter nevner at et viktig resultat som er nådd er at man har klart å etablere et samarbeid der mange aktører er aktivt engasjert. Det har fått oppmerksomhet i opinionen og er i ferd med å få legitimitet i bransjen. Det understrekes at det også har vært viktig å få utviklet/videreutviklet de personlige nettverkene. De personlige møtene har stor betydning i denne sammenheng, og disse gir påfyll både faglig og sosialt.

Oppsummeringsmessig kan vi si at de viktigste faktorene som har medvirket til suksessen så langt er de følgende:

- konkret fokus og vektlegging av å oppnå gevinster også på kort sikt (”quick wins”) eksemplifisert med Master-studiet
- mål, resultater og kompetanse i fokus, ikke lokalisering og ”overdrevne prosesser”
- bra sammensatte prosjektgrupper med kompetanse og ressurser, og der flere av disse kjente hverandre i utgangspunktet selv om de var i ulike organisasjoner. Disse personlige nettverkene, med blant annet gamle kjente i nye posisjoner, gjorde det lettere å rekruttere aktører, og som gjorde samarbeidet lettere fordi tillit var på plass i en tidlig fase
- dette er et fagområde i vekst, som har gjort det lettere å argumentere for ressurser
- ”timing” har også vært gunstig, fordi hendelser som datavirus, 11. september etc har vist at samfunnet har blitt mer sårbart.
- næringslivsstyring, der bedriftene har definert prosjektet og vært i føringen. Store bedrifter med ressurser har vært engasjert. Disse har gjort tingene raskt, og har fått med seg de offentlige etater som Innovasjon Norge og HiG (men ikke alle, som f.eks Nærings- og Handelsdepartementet).
- at det ble dratt inn samarbeidspartnere utenfor regionen (både internasjonalt som KTH, og nasjonalt som konsulentselskapene) for i startfasen å supplere regional kompetanse, som også må være der. Et nettverk bør dannes på områder der det er noe basiskompetanse allerede i regionen.
- prosjektledelse som har hatt legitimitet og profesjonalitet.

4 Analyse av Bluelight

4.1 Innledning

I dette avsnittet vil vi analysere nærmere noen variabler og karakteristika ved Bluelight for å vurdere dets måloppnåelse så langt. Vi betrakter perioden under ett, selv om det hadde gitt et mer nyansert bilde å skille mellom perioden før og etter hovedprosjektets oppstart, dvs før og etter start av Master-studiet. Hovedprosjektet er likevel kommet såpass kort at det ikke er naturlig med en totalevaluering allerede. Likevel vil vi på et par punkter differensiere vurderingen mellom de to fasene, for eksempel når det gjelder målsettingsprosessen.

Analysene er til dels teoretisk begrunnet, ved at vi fokuserer på variabler som har vært sentrale i tidligere nettverksstudier. Andre faktorer er slike vi har merket oss gjennom intervjuer og observasjon i møtene, men som vi foreløpig ikke har teoretisk begrunnelse for fra andre studier. Det er mange mulige variabler vi kunne valgt ut, men de vi ser nærmere på er:

- målsettinger for nettverket
- karakteristika ved aktørene, som for eksempel grad av homogenitet/heterogenitet, personlige faktorer, lokalisering, aktørenes motiver og – kompetanse
- prosjektledelsen
- tillit i nettverket
- bruk av ulike kommunikasjonsmedier og spesielt om møtene

4.2 Målsettinger for nettverket

Bluelight har vært veldig fokusert på konkrete resultater, på en effektiv måte, med framdrift. De skal være nyttige for aktørene både på kort og lang sikt. Tidlig i nettverksprosessen, i forprosjektet, ble det enighet om at den viktigste målsettingen på kort sikt var å etablere et studietilbud. Relativt raskt ble det også enighet om at dette skulle være et Masterstudium. Dette valget var vellykket fordi da fikk man et konkret mål å jobbe mot, noe som ofte er et problem i nettverksdannelser der det er aktører med forskjellig bakgrunn, interesser og motiver. Målet ble oppfattet som nyttig av aktuelle aktører, og samtidig var det et ”ukontroversielt tema” som alle kunne enes om. Det var samtidig et tema for å oppøve nettverkstrening på områder litt i periferien av aktørenes kjernekompetanse, og som er gunstig for videre samarbeid Haugland (1996) påpeker også viktigheten av dette i samarbeidsnettverk). På denne måten ble det bygd opp ytterligere kjennskap og tillit til hverandre. Men tillit mellom aktørene ser egentlig aldri ut til å ha har vært et problem, noe som nok skyldes at flere/mange kjente hverandre fra før. Målsettingsprosessen i Bluelights tidlige fase, i forprosjektet, anses derfor som meget vellykket. Målsettingen var konkret, ukontroversiell, og ble også betraktet som viktig av alle involverte.

Når det gjelder målsettingsprosessen i Bluelights hovedprosjekt har dette vært en mer omfattende, langvarig og mer kompleks prosess. Vi har redegjort for målene i avsnitt tre. Alle involverte er ikke like enige i alle mål nå, og det er nyanser i prioritering av f.eks produktutvikling mot kompetanseutvikling. Noen mål blir for spesielle til at de vekker entusiasme hos alle aktørene. Men målene er godt gjennomdrøftet, de er konkrete og det har vært en omfattende nedbrytingsprosess fra visjoner til konkrete målsettinger. Det som fremdeles er spennende, som nettverket har diskutert flere ganger tidligere, er om det er nok samsvar mellom de ambisiøse visjonene og målsettingene og de ressurser som er tilgjengelig.

Totalt kan vi derfor si at det har vært gode målsettingsprosesser i Bluelight, der vi først senere kan bedømme dette skikkelig for hovedprosjektet sin del. I følge Våland (2004) er en felles forståelse for nettverksbegrunnelse viktig for selve legitimiteten i nettverket som påvirker nettverkets overlevelsesevne på sikt. Den prosess som er kjørt har derfor vært viktig og nødvendig.

4.3 Aktørene i nettverket

Det som har vært avgjørende for rekrutteringen av medlemmer til Bluelight har vært fagkunnskapen, uansett hvor aktørene har jobbet organisasjonsmessig eller geografisk. I noen eller stor grad har det vært tidligere nettverk som har vært utslagsgivende for utvelgelse. Dette har hatt stor betydning for på et tidlig stadium å etablere *tillit* i nettverket. Basis i nettverket er derfor personer med interesse, kunnskap og "glød" for fagfeltet. Flere av de sentrale personene har sin bakgrunn fra Forsvaret (dvs Jørstadmoen) og Telenor, selv om de nå jobber i andre selskaper. Det har derfor vært en gunstig *jobbmobilitet:* Felles faglig plattform gir homogenitet, men de har blitt mer heterogene ved at de nå jobber både i privat og offentlig sektor. Heterogeniteten er også ivaretatt ved at både leverandører, brukere og offentlige aktører (f.eks HiG og Innovasjon Norge) er med i nettverket. Den første problemstilling knyttet til aktørene er derfor om homogenitet vs heterogenitet.

Homogenitet eller heterogenitet i sammensetning av nettverk?

En problemstilling i nettverk, som også behandles i andre teorier som f.eks teamforskning, er spørsmålet om hvor like/ulike nettverksaktører skal være. Haugland (1996) sier at nettverksaktører må ha en del fellestrekk. Dette taler for homogenitet. Det at temaområdet for nettverket er såpass klart definert, er en styrke for Bluelight. Det er enighet om hva som ligger i temaet informasjonssikkerhet. Samtidig vet vi at for å få til innovasjon, må det være noe ulikheter blant aktørene også. Dette representeres i Bluelight av at det er aktører fra både leverandører, brukere, offentlig virksomhet, FOU, regionale og nasjonale/internasjonale aktører. Sånn sett tror vi at sammensetningen av nettverket er bra. Vi har dratt i gang diskusjoner ved et par anledninger i styringskomitéen om at nettverket har for få kvinnelige deltakere, og at dette gir for lite heterogenitet. Det har blitt lite debatt rundt dette.

Betydningen av personlige faktorer, enkeltpersoners bidrag

Bluelight viser at *personfaktoren(e*) er viktig ved dannelse av nettverk. Det er enkeltpersoner i de deltakende organisasjoner som er drivkrefter. Selv om det er store organisasjoner som deltar, er fagmiljøene i både Telenor, Norsk Tipping, og konsulentselskapene ikke spesielt store. Derfor er personer og personnettverk viktig. Dette er nok undervurdert i studier av innovasjon, der fokus på organisasjoner og rammebetingelser (dvs makro faktorer) er mer fokusert. I den grad personfaktorer fokuseres, er det om personlige egenskaper hos gründeren. Det er lite om innovatøren i nettverk og som medlem av en organisasjon eller nettverk av organisasjoner. Uten initiativrike enkeltpersoner ville ikke Bluelight ha eksistert, i hvert fall ikke så vellykket.

Aktørenes motiver: forbedring av egen "bunnlinje" er ikke nok

I samtalene med nøkkelpersonene i styringskomitéen kom de fram at foruten rasjonelle motiver som å skape arbeidsplasser regionalt og nasjonalt, bidra til verdiskaping og eksport, er det hos flere av de regionale aktører, som f.eks Telenor og Norsk Tipping, en uttalt målsetting å bidra til

regional utvikling. Begge disse to aktørene er tungt representert i regionene, men de har primært et nasjonalt ansvar. Likevel har de begge balansert målstyring der det som betegnes "corporate social responsibility" er noe som fokuseres for øyeblikket. Bedrifters samfunnsansvar er også framtredende hos andre aktører i nettverket. I tillegg til målsettinger på bedriftsnivå, er det også vårt inntrykk at flere nøkkelpersoner har som personlig engasjement at dette initiativet skal bli vellykket.

De to siste punktene over støtter funn som Ostrom (1990) har om sosialt entreprenørskap.

Aktørenes kompetanse

I enkelte (regionale) innovasjonsstudier brukes begrepet "mottakerkompetanse" (f.eks Engen 1994). Han definerer mottakerkompetanse som evnen til å organisere, koordinere og mobilisere allerede tilgjengelige ressurser og kunnskap på en slik måte at ny virksomhet kan adopteres og integreres i et samfunn. I Bluelight sammenheng vil vi si at dette betyr at aktørene i en region må ha en basiskompetanse for å kunne motta, bearbeide og samhandle med aktører som er lokalisert andre steder. I tilfellet "Bluelight" har det i lengre tid eksistert en basiskompetanse gjennom fagmiljøet ved f.eks Jørstadmoen og Telenor. Flere har kommet til de siste 5-10 årene. Det regionale miljøet er derfor i stand til å motta ny kunnskap. Samtidig har jo situasjonen vært slikt at initiativet har vært fra regionale aktører og til og med mot sentrale aktører, dvs proaktive handlinger. Kompetanseoverføring går både inn og ut av regionen.

Aktørenes lokalisering

Deltakerne i Bluelight er lokalisert i de tre Mjøsbyene, samt Kongsvinger og Oslo. Det er i utgangspunktet både regionale og nasjonale aktører, men det er få av aktørene som kun har regionalt marked. En av disse er Krogh & Hansen på Kongsvinger. Verdt å merke er at noen nasjonale aktører som er representert i Bluelight (ref f.eks PWC og SecureGroup) ikke har personer med spesialkompetanse i Innlandet. Det er så kort avstand mellom Oslo og Innlandet, at de reiser etter behov. Dette til forskjell fra Thales som har opprettet eget Lillehammer-kontor, med et par ansatte.

Det debatteres i nettverks- og klyngeteorier om lokalisering og geografisk plassering av nettverksaktørene. Stadig flere teorier heller nok til at det er viktig både å ha med lokale aktører og nasjonale/internasjonale aktører, eksempelvis Bathelt, H.; Malmberg. A., Maskell, P. (2002). Bluelight bekrefter viktigheten av dette. Men det er viktige forskjeller fra blant annet studien til Bathelt m.fl:

- det er få av aktørene i Bluelight som kun opererer i de lokale markedene
- mange av aktører er både lokale og nasjonale
- de lokale aktørene er ikke samlokalisert på et sted i Innlandet, men er spredt i alle de store/mellomstore stedene (Lillehammer, Gjøvik, Hamar, Kongsvinger mv)

Bathelt m.fl (2002) hevder at de lokale kontaktene ordner seg selv fordi disse treffes automatisk, mens innovasjonspolitikken må gå ut på å støtte etablering av det de kaller "the global pipelines". Erfaringene fra Bluelight skiller seg noe fra dette, fordi de lokale firmaene ikke er samlokalisert og initialt hadde flere/like mange kontaktpunkter ut av regionen som innen regionen. Det trenges derfor organiserte tiltak regionalt for å knytte disse sammen, som Bluelight har bidratt til. De nasjonale og internasjonale kontaktene har de allerede, men kanskje Bluelight kan bringe dem enda videre også på disse områder?

Tillit og kjennskap til hverandre

Når det har vært snakk om bedriftnettverk og klynger er tillit et av de ordene som nevnes oftest. Ofte er litteraturen om tillit ganske generell *("tillit er viktig"),* men det er forsket enormt på begrepet tillit, i mange ulike fagområder. Det er mange definisjoner på begrepet, og at tillit reduserer usikkerhet i relasjoner er noe som går igjen i definisjoner. Vi har observert at tillit er viktig også i Bluelight. Nettverket sparte på en måte tid ved at flere i nettverket kjente hverandre fra tidligere. Og da valgte de også ut en del partnere ut fra kjennskap til personers fagkunnskaper og personlighet. Dermed var en tillitsbase tilstede allerede fra starten av. Dette sammen med en effektiv målsettingsprosess og en relativt homogen medlemmasse i nettverket, var gunstig for målrealisering. Også Våland (2004) fremhever betydningen av å kjenne hverandre i nettverket som et fundament for et godt nettverk: *"Et godt nettverk bygger på en erkjennelse av gjensidighet. En forutsetning for dette er at man har tilstrekkelig informasjonsflyt mellom selskapene slik at man kjenner hvordan de andre aktørene opererer.*

Ville aktørene kjent hverandre like godt uten nettverket?". Vi har ikke spurt aktørene i Bluelight direkte, men svaret er antagelig nei..

Tilliten har også utviklet seg over tid: alle kjente hverandre ikke like godt fra starten av. Som observatør i styringskomitéen og drivernoden det siste trekvart året har det vært interessant å følge følgende endringer:

- adferden i møtene er mye mer avslappet enn i starten, noe som også er understøttet av at møtene gir mer tid til diskusjoner og spontane innspill. I starten av arbeidet med hovedprosjektet var det mye mer informasjonsspredning og mindre prosesser. Dette viser også at prosesser tar tid og at personlige møter trengs i nettverk.
- et ytterligere bevis på hvordan tilliten har økt/kommunikasjonen har endret seg er at deltakerne i langt større grad bruker fornavn om hverandre i møtene.
- pausene i møtene har også endret seg: de har blitt lengre for å fremme uformell kommunikasjon, hvor de er arenaer for personlig fordypning, sosialisering, og oppfølging av prosjektidéer

4.4 Kommunikasjon og medievalg i Bluelight

Våland (2004) understreker betydningen av effektiv kommunikasjon i nettverk. Det legges vekt på at denne skal være effektiv og regelmessig. I hans studie var kommunikasjonen i stor grad knyttet opp til elektroniske løsninger som Internett og epost. Våland hevder at nettverk, spesielt de som har teknologiutvikling som formål, er helt avhengig av moderne kommunikasjonsteknologi for å sikre effektiv samhandling. Ansikt til ansikt kontakt er mindre brukt, selv om han generelt betrakter dette som viktig for oppbygging av tillit. Ansikt til ansikt kommunikasjon gjennom fysiske møter anses også som viktig for overføring av taus og kompleks informasjon og kunnskap.

I Bluelight står fysiske møter og fysiske møteplasser sentralt. Når det gjelder elektronisk kommunikasjon synes det å være en kommentar fra informantene om at potensialet er begrenset i Bluelight på grunn av at det er mange aktører i forskjellige organisasjoner, og også at temaet sikkerhet krever mer fysiske møter nettopp av sikkerhetshensyn. Så langt har epost vært brukt for rutinemessig kommunikasjon før og etter møter, og Internett-sider/hjemmesider har vært lite utviklet. Telefon og mobiltelefon har nok vært viktige kommunikasjonsredskaper, uten at vi kjenner detaljer i dette. Selv om hele Bluelight ikke er samlokalisert til ett sted, er det relativt

korte avstander slik at reiseavstand kun er i overkant av to timer mellom ytterpunktene. Dermed er det ikke problematisk å ha personlige møter hvis det gjøres litt planlegging.

4.5 Prosjektledelse

I dette avsnittet konsentrerer vi oss om prosjektledelsen. Det betyr fokus på Gjøvik kunnskapspark- som er prosjektleder.
Teorier om bedriftsnettverk er egentlig lite konkrete når det gjelder hvordan slike skal styres. Mye å studiene er fokusert på hvordan skape tillitt hos aktørene. Suksessen til Bluelight kan likevel også forklares gjennom den daglige oppfølgingen av prosjektleder Svein Pettersen. Ryddighet, samvittighetsfull, og legitimitet i alle leire, er ord som nevnes eller fornemmes fra deltakerne. Utgangspunktet med at Pettersen sitter i en kunnskapspark har gitt legitimitet og tillit både mot de private leverandørene, de offentlige myndighetene, FOU-miljøet, brukerne mv. I tillegg kjenner han fagfeltet godt. Og for det tredje har han gode administrative evner. Dette gir seg utslag at det ennå ikke i det året undertegnede har vært observatør i Bluelight, har vært noen alvorlige administrative bommerter.

Prosjektleder Svein Pettersen sier om sin ledelsesfilosofi knyttet til Bluelight at denne er karakterisert som: "tilretteleggende". Han lar bevisst aktørene "fronte" og komme til orde. Han ønsker å være inkluderende, dvs lytter til aktører og ønsker nye aktører velkommen. Videre legger han stor vekt på forankring underveis og mellom møtene, og han sier at det meste av det reelle arbeidet skjer mellom møtene. Da utarbeider han for eksempel forslag/utkast som han forankrer hos noen utvalgte før møtebehandling. Det er han som er referatskriver fra møtene. Når det gjelder noder og delprosjekter tilstreber han at disse skal ledes av andre enn han, for eksempel: "3-1 prosjektet og informasjonssikkerhet" ledes av Telenor, kommuneforeningen KINS ledes av Sits, og møteplassen "Forum Sikkerhet" av Telenor og Jørstadmoen.

Våland (2004) er opptatt av at det settes av *nok ressurser* til ledelse/administrasjon av et nettverk. Han sier at "en nettverkskaptein på deltid sannsynligvis ikke er tilstrekkelig til å sikre utviklingen i nettverket tatt i betraktning det store medlemstallet og medlemmenes forventninger". I Bluelight har det også vært stilt spørsmål om det er samsvar i mellom de ambisiøse målsettingene og de ressurser som er tilgjengelige. Veldig mange av oppgavene er knyttet til navnet Svein Pettersen. Og da kan det bli sårbart. Han jobber tross alt på fulltid med Bluelight, miljøet rundt NISlab teller etter hvert flere personer, og det er aktive personer i flere av deltakerbedriftene som for eksempel Telenor. Bluelight må nok kontinuerlig vurdere sammenhengen mellom ambisjoner, prioriteringer og ressursbruk.

Det bør også nevnes Innovasjon Norge sin viktige rolle som prosjekteier. De har prioritert et relativt utradisjonelt område, og det virker som at de har gode kanaler mot ulike sentrale miljøer.

4.6 "Bred medvirkning" og Bluelight

En av de viktigste filosofiene bak prosjektet VS 2010 er at bred medvirkning blant partene i arbeidslivet skal gi grunnlag for innovasjon og verdiskaping. Begrepet "bred medvirkning" har flere betydninger. For det første kan det dreie seg om at mange aktører innen et temaområde er engasjert. Anvendt på Bluelight betyr det at mange potensielle aktører engasjerer seg. I Bluelight må det sies at medvirkningen er stor ut fra denne fortolkningen av begrepet: Sentrale aktører rundt nettverket kommer fra både næringsliv (brukere, leverandører, konsulenter), videre akademiske institusjoner både i Norge og Sverige, samt utviklingsaktører som Innovasjon Norge, Norges

Forskningsråd og Gjøvik Kunnskapspark. Både Nærings- og handelsdepartementet (NHD), Forsvarsdepartementet og Justisdepartementet støttet etableringen av Masterstudiet i sin tid. Spesielt NHD holdes løpende oppdatert med hensyn til studiets utvikling, samt arbeidet i Bluelight generelt. NHD sluttførte i fjor sin nasjonale strategi for informasjonssikkerhet, og Bluelight har som mål å bli en viktig partner i gjennomføring og oppfølging av denne.

En annen fortolkning av "bred medvirkning" er knyttet til representasjonen av arbeidslivets organisasjoner og parter i de styrende organisasjoner i Bluelight, for eksempel styringskomitéen. Så langt er verken LO eller NHO representert her. Spørsmålet har vært tatt opp, men svaret har vært at spørsmål med betydning for LO og NHO tas opp i den enkelte bedrift.

En tredje fortolkning av "bred medvirkning" dreier seg om hvordan ansatte i bedrifter kan engasjeres i spørsmål rundt informasjonssikkerhet. Mye fokus har vært rundt tekniske aspekter. Likevel sies det at 80% av arbeidet med informasjonssikkerhet i bedrifter dreier seg om å jobbe med holdninger blant ansatte og ledelsen. Bluelight vil jobbe med disse spørsmål både gjennom seminarer, gjennom Security Partner sine produkter, og gjennom planer om et samfunnsvitenskapelig studium innen informasjonssikkerhet.

5 Avslutning og konklusjoner

Dette kapitlet har i stor grad vært en beskrivelse av fagfeltet informasjonssikkerhet generelt, beskrivelse av aktører og samarbeidsaktiviteter knyttet til informasjonssikkerhet i Innlandet. Nettverkssamarbeidet Bluelight er beskrevet, både status, mål og historien bak denne. Til slutt har vi gjort en del analyser av en del trekk ved Bluelight, med vekt på målsettinger, karakteristika ved aktørene, kommunikasjonsbruk og ledelse.

5.1 Hva kan andre nettverk lære av Bluelight?

Ethvert nettverk må vurdere hvilke av de tiltak som Bluelight har gjort som passer i den konkrete konteksten. De faktorene som vi trakk fram tidligere, bør vurderes også i andre nettverksdannelser:

- ha konkret fokus og vektlegging av å oppnå gevinster også på kort sikt gjennom samarbeid på "ukontroversielle områder"
- mål, resultater og kompetanse må være i fokus, ikke lokalisering og "overdrevne prosesser"
- vurder nøye sammensetning av prosjektgruppene: kompetanse og ressurser, betydning av personfaktoren, homogenitet vs heterogenitet, lokalisering, offentlig/privat, leverandører, brukere
- hvordan bygge tillit på rask og god måte
- hvordan skaffe prosjektledelse som har legitimitet og profesjonalitet
- grad av næringsdeltakelse og - styring
- et nettverk bør dannes på områder der det er noe kompetanse allerede i regionen, men med samarbeid utover regionen

Vi merker oss viktigheten av at både lokale/regionale og nasjonale aktører er med i et nettverk. Erfaringene fra Bluelight er også at de lokale prosesser ikke gjør seg selv, lokale aktører er også nasjonale og har like mye/mer kontakt ut av regionen som internt.

Samtidig skal en være varsom med at alle nettverk skal kopiere Bluelight. Situasjonen i andre bransjer i Innlandet er svært forskjellig fra informasjonssikkerhet. Situasjonen for eksempel fra nettverkene innen treindustrien i Glåmdalen viser en veldig forskjellig situasjon. Her er det eldre industri med mange etablerte bedrifter og relativt lav kompetanse, lav FOU-andel og problemer med incitamenter, tradisjoner og personer til å drive nettverksarbeid, i et marked med begrenset vekst og ikke det mest spennende image. Innen informasjonssikkerhet ser vi at nettverket fungerer, men selve næringen er liten. På en måte skal det avledes næringsvirksomhet av nettverksarbeidet, nesten det motsatte av treindustrien i Glåmdalen.

5.2 Utfordringer som Bluelight står ovenfor, noen utviklingsområder

Utgangspunktet er at Bluelight så langt har vært en suksess. Alle de intervjuede er enige om at Bluelight har nådd langt på kort tid, at masterstudiet har vært vellykket, at det har vært positivt med de møteplassene som er opprettet, at nettverket har blitt kjent innenfor fagmiljøet og mot noen offentlige institusjoner, og at mange aktiviteter/prosjekter er satt i gang.

Som indikert av mange av informantene er det langt igjen til visjonene er oppfylt. Og veien framover er antagelig langt mer utfordrene enn den veien som er gått så langt. Flere sier at det blir

en større utfordring å få mer bedriftsetableringer enn å etablere studiet. Et spørsmål som stilles av enkelte er egentlig hvor sterk informasjonssikkerhet er i Innlandet? En utfordring er å få til enda mer samhandling og læring, også utover møtene i de ulike fora. Læring skjer best gjennom konkrete case, for eksempel gjennom utviklingsprosjekter som Security Partner. En annen utfordring som nevnes av en deltaker er å få finansiering av utviklingsprosjekter, slik at bedriftsdeltakere kan frikjøpes for å delta i prosjekter. De viktigste utfordringene er generelt: penger/finansiering, kompetanse, ideer, samt prioritering. Det vil kreves offentlige midler for å finansiere FOU og studier. Finansiering er kritisk: uten finansiering er målene "skydotter". Det har vært en bra begynnelse, men det er langt igjen . Vi har "gått 100 meter av et løp på 10 km", sier en av informantene. Det er generelt mye av de samme utfordringene som nevnes av de fleste informantene.Men vi føler kanskje at det er en liten forskjell mellom intervjuobjektene om hvor langt igjen det er til målet, og hvor sterke vi i Innlandet er på området.

I løpet av høsten 2003 ble det en problemstilling som har blitt nevnt av stadig flere; Behovet for å prioritere sterkere blant et stort antall foreslåtte og igangsatte aktiviteter. Det stilles spørsmål om det er nok ressurser til å gjennomføre aktiviteter, og om aktivitetene er for spredt slik at en ikke har det fellesfokus som Masterstudiet representerte. Men alle de vi har snakket med hevder at nettverket er nyttig, og at det er i ferd med å skape seg en sterk identitet og bli en nasjonal og skandinavisk aktør som fagmiljøet kjenner. Potensialet er stort for å bli en aktør i forbindelse med nylig etablerte Nasjonal strategi for informasjonssikkerhet, å videreutvikle satsningen mot kommunal sektor og å videreutvikle posisjonen ytterligere som utdannings- og FoU-aktør. Når det gjelder det siste fikk NIS-lab ved HIG tildelt betydelige forskningsmidler i 2003. Og satsingen mot å bli et nasjonalt ekspertsenter for informasjonssikkerhet kan bli det samlende målet som løfter og motiverer Bluelight, slik som Masterstudiet gjorde. Når det gjelder øvrige mål, vises til avsnitt tre i dette notatet. Disse målene er også svar på flere ting som i dag kan betraktes som en svakhet ved Bluelight.

Som nevnt tidligere er det nok vanskeligere å drive innovasjon og produktutvikling i nettverk enn å drive kompetanseutvikling. Det blir spennende om nettverket har god nok kommersialiseringskompetanse, da faglig kompetanse om fagfeltet utvilsomt er der. I første fase av hovedprosjektet har Bluelight hatt mye fokus på visjoner og mål. Nå blir det en utfordring å realisere disse. Et spennende felt er også knyttet til prosesser i nettverk. Bluelight har vært veldig målrettet, samstemt og suksessrikt så langt, med gode strukturer. Hvordan vil nettverkt kunne møte eventuell motgang og konflikter?

Utfordringer i følge evalueringsrapport fra Ekebacka KonsultAB (notat fra Bo Lindestan 26 jan 2004)

Etter litteraturstudier, deltakelse på styringskomitémøte i Bluelight i januar, og møte med prosjektledelsen i Bluelight, har evaluatorene for Arena-programmet kommentert en del punkter rundt Bluelight. Vi skal trekke fram noen av disse: Evaluator Lindestan skriver at fagområdet informasjonssikkerhet er et stort område, men ingen steder finnes et forsøk på nedbryting og grov klassifisering. På dette punktet er vi enig med Lundestam. Det er lite data tilgjengelig om markedet for informasjonssikkerhet, og det er behov for å få fram bedre data om dette. Slike data vil også ha betydning for eksempel for markedsvurderingene for Security Partner, som også Lindestan etterlyser. En tredje etterlysning som Lindestan gjør er at han savner mer detaljerte beskrivelser for hvordan de opplistede bedriftene skal samarbeide, og spesielt hva de skal bidra med. Etter det vi forstår er det i liten grad formelle avtaler om hva en skal bidra med i prosjektet, kanskje bortsett fra bidrag til Masterstudiet. Tillit ser ut til å være det viktigste styringsredskapet. Men er det behov for mer formalisering?

De andre punktene dreier seg også mye om behov for markedskunnskap, behov for mer ekstern orientering og klarere angivelse av hvem som skal inneha kompetanse om fagfeltet ("kompetanse-bærere"). Dessuten er det en god del refleksjon om Security Partner og om behov for

konkretisering av forretningsmodell og markedsgrunnlag. Det stilles spørsmål om markedet er stort nok.

Det viktigste i det Lindestan skriver er knyttet til behov for mer markedsdata og om behov for mer formalisering i samarbeidet. Derfor er også dette noe av det vi vil bidra med i det videre arbeid. Og det gleder oss at det også fra NHD's sin side vil bli prioritert arbeid med å få fram statistikk om informasjonssikkerhet (ifl foredrag av Dreyer fra NHD på KINS- konferanse Lillehammer i mars 2004).

Referanser

Bathelt, H.; Malmberg. A., Maskell, P. (2002): Clusters and knowledge: local buzz, global pipelines and the process of knowledge creation, Danish Research Unit for Industrial Dynamics, working paper no 02-12

Ericsson B. m.fl (2002): Regionale innovasjonspiloter, næringsanalyse for mediesektoren i Hedmark-Oppland, ØF-rapport 2002/10

Dahler, Torgeir m.fl (2002): Håndbok i datasikkerhet: informasjonsteknologi og risikostyring, Tapir akademisk forlag

Engen, O. A (1994): Evne til å ta imot?, arbeidsnotat RF 205/94, Stavanger, Rogalandsforskning

FD, NHD og JPD (2003): Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet (2003): Nasjonal strategi for informasjonssikkerhet: utfordringer, prioriteringer og tiltak

Haugland S (1996): Samarbeid, allianser, nettverk, Tano Aschehoug

Hærens samband på Jørstadmoen: http://www.mil.no/haren/sbuks, 8. feb 2004

Ostrom, E. (1990): Governing the commons: the evolution of institutions for collective action, Cambridge University Press

PricewaterhouseCoopers (2003): Information security: a strategic guide for business, PricewaterhouseCoopers Global Technology Centre, San Jose, USA , Nov 2003

Våland, Terje I (2004): Industrielle nettverk- innovasjon og kommersialisering, Magna nr 1/2004

I tillegg: forprosjektrapporter, og en mengde interne dokumenter fra NIS-nettverket/Bluelight

Vedlegg 1 Informanter

Svein Pettersen, Gjøvik kunnskapspark/Høgskolen i Gjøvik

Eivind Petershagen, Innovasjon Norge

Jan Erik Svensson, Telenor (og andre personer i sikkerhetsstaben i Telenor)

Morten Schjelderup, Norsk Tipping

Arne Johan Helle, Price Waterhouse Coopers

Tor Arne Johansen, Ibas/Kongsvinger

Jan Erik Krogh, Krogh& Hansen, Kongsvinger

Nils Klippenberg, Thales

Kristin Malones, Innovasjon Norge

Roger Johnsen, Forsvaret/Jørstadmoen

Narvin Tangen, Sits (Senter for IT-samhandling)

I tillegg: uformelle samtaler med personer i drivernode og fagpersoner under seminarer og nettverksmøter

Bluelight: nettverk for informasjonssikkerhet
- historien og kritiske suksessfaktorer

Innlandet har i lengre tid hatt en god del aktører med spisskompetanse innen informasjonssikkerhet. Fra 2001 er det skjedd en rekke aktiviteter for å få til økt formelt samarbeid mellom de 40 aktørene i Innlandet.
Det største resultatet så langt av dette er opprettelsen av Masterstudium i informasjonssikkerhet ved Høgskolen i Gjøvik høsten 2002.
Nettverket har nå betegnelsen Bluelight, og ble fra høsten 2002 en del av Innovasjon Norge sitt Arena Program.
Her beskrives status og mål for samarbeidet i Bluelight.
Vi gir en oversikt over sentrale aktører, og historien bak nettverket presenteres.
Til slutt gjør vi en analyse av nettverket, der spesielt kritiske suksessfaktorer trekkes fram.

ØF-Notat nr.: 04/2004
ISSN 0808-4653