Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)

Desember 2017

NorSIS
Norsk senter for informasjonssikring

Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)

Offentlig

Rapporten er utarbeidet på oppdrag fra Gjøvik kommune og Lillehammer kommune.

Ansvarlig: Peggy Sandbekken Heie
Forfattere: Bjarte Malmedal og Ole Anders Ulsrud
Layout og illustrasjoner: Maria Nyheim
Utgitt: Desember 2017
ISBN: 978-82-93651-01-7

Kontaktinfo NorSIS
Teknologiveien 22
2815 Gjøvik
Org.nr: 995 195 003
Telefon: 40 00 58 99
Nett: www.norsis.no

Forord

Lillehammer og Gjøvik kommuner har vært initiativtakere og oppdragsgivere for prosjektet som har vært finansiert av Fylkesmannen i Oppland. KS har deltatt i styringsgruppen og vært prosjekteier sammen med Gjøvik kommune og Lillehammer kommune.

Kontaktpersoner for prosjekteierne har vært Anne Mette Dørum fra KS, Eirik Haagensen fra Lillehammer kommune og Aasbjørn Pålshaugen fra Gjøvik kommune.

Mandatet for utredningen har vært forankret hos KommIT-rådet i KS gjennom en prosess hvor KS faggruppe for informasjonssikkerhet og personvern, Fylkeskommunalt IKT-forum, KINS, NORSIS, Lillehammer kommune, Gjøvik kommune, Cyberforsvaret og Fylkesmannen i Oppland har vært involvert.

Styrings- og referansegruppa har bidratt aktivt for å sikre at kommunenes behov har blitt ivaretatt og bidratt med sin kompetanse og erfaring i arbeidet.

Prosjektet har vært gjennomført av Bjarte Malmedal (prosjektleder) i samarbeid med Ole Anders Ulsrud.

Gjøvik, desember 2017

NorSIS

Sammendrag og konklusjoner

Kommunenes avhengighet av IKT for produksjon og leveranser av kommunale tjenester øker, samtidig som digitale trusler øker i både omfang og alvorlighet. Datakriminalitet, digital aktivisme og trusler fra fremmede stater kan føre til at kommunene ikke lenger kan levere de tjenestene som innbyggerne forventer på en effektiv måte.

Riksrevisjonen, Datatilsynet og Digitalt sårbarhetsutvalg har imidlertid påpekt en rekke brudd på personvernreglene, alvorlige svakheter i informasjonssikkerheten og kompetansemangel innen IKT-sikkerhet i kommunene.

KS' (kommunesektorens organisasjon) rolle er å samordne digitaliseringsarbeidet i kommuner og fylkeskommuner, å ivareta kommunesektorens behov i statens digitaliseringsaktiviteter og å sørge for gode rammevilkår for digitalisering i kommuner og fylkeskommuner.

Regjeringen la i 2016 frem Meld. St. 27 (2015-2016) Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet. Meldingen presenterer regjeringens overordnede politikk for hvordan vi kan utnytte IKT til samfunnets beste.

Satsingsområdene i Digital agenda for Norge har stor betydning for digitalisering av offentlig sektor. Kommunal sektor møter disse satsingsområdene koordinert og samordnet gjennom KS' Digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020, der regjeringens satsingsområder fra Digital agenda for Norge er hovedområdene for kommunal sektors digitale satsing i Digitaliseringsstrategien:

1. Brukeren i sentrum
2. Digitalisering er en vesentlig innsatsfaktor for innovasjon og økt produktivitet
3. Styrket digital kompetanse og deltakelse
4. Effektiv digitalisering av offentlig sektor
5. Informasjonssikkerhet, personvern og dokumentasjonsforvaltning

Nåsituasjonen i kommunal sektor viser at det er ingen aktører som i dag beskriver et helhetlig situasjonsbilde (trusler, sårbarheter, hendelser og sikkerhetstiltak) for sektoren, og det er heller ingen aktører som i dag har ansvar for varsling og informasjonsdeling mellom alle kommuner, fylkeskommuner og andre håndteringsmiljøer i sektoren.

Noe varsling og deling av informasjon finner sted, primært sentrert rundt eksisterende håndteringsmiljøer og i kommuner som har kompetanse og kapasitet til dette. Videre har kommunal sektor i dag ikke et felles ressurs- eller kompetansesenter som kan støtte kommunene med tekniske analyser, eller teknisk eller metodisk støtte ved håndtering av IKT-hendelser

Det er heller ikke formalisert et kontaktpunkt for kommunal sektor i den nasjonale CERT-strukturen. Deler av kommunal sektor dekkes gjennom kontaktpunktene i øvrige responsmiljøer som HelseCERT, KraftCERT og NorCERT.

Utredningen har kartlagt og beskrevet de felles behovene for støtte til håndtering av IKT-sikkerhetshendelser. Kommunal sektor har behov for støtte til håndtering av hendelser, etablering av et felles situasjonsbilde, støtte til analyser av digitale elementer, støtte til opplæring og kompetanseheving og støtte til veiledning, rådgiving og revisjon.

Basert på de felles behovene er det beskrevet tre løsningsalternativer for et mulig KommuneCSIRT. Alternativ 1 beskriver et håndteringsmiljø som er overordnet og koordinerende, mens

Alternativ 2 beskriver et håndteringsmiljø som er teknisk og utøvende. Ingen av disse miljøene dekker imidlertid det totale behovet for støtte til håndtering av IKT-hendelser i kommunal sektor. Alternativ 3 dekker tjenestene i både Alternativ 1 og 2, og dekker således alle felles behov.

Utredningen belyser i tillegg forhold knyttet til hvilken kapasitet et slikt senter kan ha, samt ulike løsninger for organisering, finansiering og lokalisering.

Basert på alle fakta som har fremkommet i arbeidet med utredningen, og basert på egen erfaring med kompetansemiljøer for håndtering av IKT-hendelser, har NorSIS gitt sin anbefaling til løsning. NorSIS anbefaler at kommunal sektor velger å etablere et håndteringsmiljø tilsvarende beskrivelsen for Alternativ 3, og at det i oppstartsfasen legges vekt på tjenestene som er beskrevet for Alternativ 1.

Kapiteloversikt

Begreper

IRT – Incident Response Team

Et team med kompetanse og mandat til å håndtere hendelser

CERT – Computer Emergency Response Team

Et begrep som er synonymt med IRT. Begrepet eies av Carnegie Mellon University / Software Engineering Institute. CERT-begrepet er lisensbelagt, og en må søke om tillatelse for å bruke det.

CSIRT – Computer Security Incident Response Team

Et begrep som er synonymt med IRT. CSIRT er ikke en lisensbelagt tittel.

Håndteringsenhet / Responsmiljø

Et begrep som i denne rapporten er synonymt med IRT.

SOC – Security Operations Center

En enhet som er involvert i de operative prosessene med å avdekke og håndtere IKT-hendelser. Et SOC kan inngå som en del av et IRT.

IKT sikkerhetshendelse

En avvikssituasjon hvor det er tap av konfidensialitet, integritet, og/eller tilgjengelighet for informasjon eller IT-ressurser. En IKT-sikkerhetshendelse kan oppstå som følge av et dataangrep, teknisk svikt, eller utilsiktede feilhandlinger.

Risiko

Potensial for uønskede hendelser eller tap ut fra verdi som skal beskyttes, trussel mot denne verdien og verdiens sårbarheter overfor den spesifiserte trusselen.

Sårbarhet

Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.

Trussel

Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet.

PGP – Pretty Good Privacy

Programvare som tilbyr kryptografisk funksjonalitet.

TLP – Trafikklys Protokoll

En avtale som regulerer hvordan informasjon kan fordeles og anvendes. Brukes ved informasjonsdeling.

SCADA

Supervisory Control and Data Acquisition. System eller nettverk som brukes til å kontrollere (industrielle) prosesser eller infrastrukturer

Sky-løsninger

Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse. Brukes ulikt av ulike leverandører, leveres via internett

Innhold

1 Innledning

1.1 Bakgrunn

Kommunene utgjør en kompleks sektor, og behovet for og forventningene til digitale kommunale tjenester er betydelig. IKT-kriminalitet eller bortfall av digitale tjenester vil kunne få store konsekvenser for evnen til å levere kommunale tjenester. Meld St. 27 (2015–2016)[1] tilkjennegir en klar ambisjon om at godt personvern og informasjonssikkerhet skal prioriteres i forbindelse med digitalisering av kommunesektoren [s. 12].

Riksrevisjonen, Datatilsynet og Digitalt sårbarhetsutvalg har imidlertid påpekt en rekke brudd på personvernreglene, alvorlige svakheter i informasjonssikkerheten og kompetansemangel i kommunene [s. 58]. I tillegg endres IKT trusselbildet svært raskt. Tiltak som tidligere var effektive kan dermed allerede være utilstrekkelige. Regjeringen vil derfor ha kontinuerlig innsats for bevisstgjøring og kompetanseheving, samt styrke beredskapen og innsatsen for å hindre IKT-kriminalitet [s. 156].

I Nasjonal strategi for informasjonssikkerhet (2012)[2] vektla regjeringen behovet for å etablere kapasitet til å koordinere og håndtere uønskede IKT-hendelser i alle samfunnssektorer. Disse varslingsmiljøene skal være strukturert slik at man tar hensyn til sektorens bruk av IKT-infrastruktur, hvordan infrastrukturen i sektoren er bygget opp og hvordan denne styres. Med utgangspunkt i den nasjonale strategien gjennomførte Norsk senter for informasjonssikring i 2015 en studie, på oppdrag fra Gjøvik og Lillehammer kommune, for å se nærmere på behovet for et eget respons- og kompetansesenter for IKT-sikkerhet i kommunesektoren. Utredningen anbefaler etablering av et slikt senter, spesielt da risikobildet overstiger den kompetansen og kapasiteten som finnes i de fleste kommuner. Videre viser erfaringer fra Forsvaret, HelseCERT, UNINETT CERT og FinansCERT at inngående kunnskap til egen sektor er en forutsetning for at et slikt senter skal lykkes. Studien klargjør også nødvendigheten av at senteret innrettes slik at det forholder seg til kommunenes etablerte avviks- og krisehåndteringsprosedyrer. Tilrådingen forsterkes og videreføres av Digitalt sårbarhetsutvalg i NOU 2015:13[3].

1.2 Mandat

Prosjektet skal utrede ulike alternative løsninger for et kompetansesenter for håndtering av IKT-hendelser i kommunal sektor som skal bidra til at kommunene har en robust evne til å forebygge og håndtere nåværende og fremtidige IKT-trusler.

I denne utredningen omtales kompetansesenteret som KommuneCSIRT.

1 Meld. St. 27 (2015–2016) Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet.

2 *Nasjonal strategi for informasjonssikkerhet*. Fornyings-, administrasjons- og kirkedepartementet. 2012.

3 *Norsk Offentlig Utredning*. NOU 2015:13 Digital sårbarhet – Sikkert samfunn.

1.3 Prosjektmål

1.3.1 Resultatmål

Prosjektet skal kartlegge og beskrive hvilke behov som er felles i kommunal sektor, og vurdere hvordan ulike typer responsmiljøer vil kunne møte disse behovene.

Prosjektets resultatmål fastsettes derfor som:

- Det skal gjennomføres en avgrenset kartlegging og beskrivelse av hvilke behov kommunesektoren har for støtte til håndtering av IKT-hendelser

- Det skal utredes ulike alternative løsninger av responsmiljø som kan imøtekomme behovene. Følgende faktorer skal inngå i utredningen:
  - Finansieringsmodell
  - Lønnsomhet (Kost/nytte)
  - Samfunnsøkonomiske gevinster
  - Strukturelle løsninger (knyttet til senteret og knyttet til omgivelsene)

- Forholdet til øvrige CERT-organisasjoner skal avklares nærmere, herunder hvordan tjenester fra disse kan utnyttes av, eller inngå i, responsmiljø for kommunal sektor.

1.3.1 Effektmål

Et KommuneCSIRT skal bidra til at kommunene har en robust evne til å forebygge og håndtere nåværende og fremtidige IKT-trusler.

Prosjektets effektmål fastsettes derfor som:

- Bidra til at kommunene har et beslutningsgrunnlag for å iverksette etablering av et ikt-hendelseshåndteringssenter som vil bidra til at slike hendelser ikke påvirker kommunenes tjenester, eller innbyggernes tillit til tjenestene, i betydelig grad.

- Bidra til at kommunene har et beslutningsgrunnlag for å iverksette etablering av et IKT-hendelseshåndteringssenter som vil bidra til at fremmedstatlige påvirkningsoperasjoner ikke fører til en betydelig endring av innbyggernes oppfatning av virkeligheten

1.4 Prosjektorganisasjon

Prosjekteier: KS ved Anne Mette Dørum
Prosjekteier (utøvende): Gjøvik Kommune ved Aasbjørn Pålshaugen
Prosjekteier (utøvende): Lillehammer Kommune ved Eirik Haagensen
Prosjektleder: NorSIS ved Bjarte Malmedal og Ole Anders Ulsrud

Styringsgruppen:

Prosjekteierne:
Gjøvik kommune ved Aasbjørn Pålshaugen (Leder styringsgruppen),
Lillehammer kommune ved Eirik Haagensen og
KS ved Anne Mette Dørum

KS' Faggruppe for informasjonssikkerhet og personvern:
Oslo kommune ved Lise Arneberg og Rune Hagen,
Trondheim kommune ved Ole-Bjørn Nordland,
Bergen kommune ved Gøran Breivik,
Moss kommune ved Terje Jensen,
Bærum kommune ved Trond Sundby,

Aust-Agder Fylkeskommune/IKT Agder ved Tonny Morewood,
Fylkesmannen i Oppland ved Asbjørn Lund og
KINS ved Steinar Nørstebø

Referansegruppen:
Kommunal- og Moderniseringsdepartementet,
Justis- og beredskapsdepartementet,
Nasjonal Sikkerhetsmyndighet,
Direktoratet for forvaltning og IKT,
Datatilsynet,
Cyberforsvaret,
Center for Cyber and Information Security,
KINS,
NorCERT,
KraftCERT,
HelseCERT,
FinansCERT og
UninettCERT

1.5 Møtestruktur

Dato	Møte	Hensikt
6. januar 2017	Avtaleinngåelse	Avtale om oppdrag signert av prosjekteiere og NorSIS. Deltakere: Prosjekteiere og Prosjektledelse.
7. mars 2017	Workshop 1	Informasjonsinnhenting om nåsituasjon og behov. Deltakere: Prosjekteiere, Prosjektledelse, Styringsgruppe og Referansegruppe.
20. april 2017	Møte styringsgruppen	Forventningsavklaring om det videre arbeidet. Deltakere: Prosjekteiere, Prosjektledelse og Styringsgruppe.
5. september 2017	Møte styringsgruppen	Gjennomgang og tilbakemelding på nåsituasjonsbeskrivelse og behovsbeskrivelse. Deltakere: Prosjekteiere, Prosjektledelse og Styringsgruppe.
13. september 2017	Workshop 2	Prioritering av felles behov i kommunal sektor. Deltakere: Prosjekteiere, Prosjektledelse og Styringsgruppe.
30. november 2017	Møte styringsgruppen	Gjennomgang og tilbakemelding på sluttrapport Deltakere: Prosjekteiere, Prosjektledelse og Styringsgruppe.

2 Metode

2.1 Kartlegging av nåsituasjon og behov

Nåsituasjonen og behovene er kartlagt gjennom en workshop der representantene i styringsgruppen og referansegruppen deltok, og gjennom dybdeintervjuer med den enkelte representant.

Prosjektmandatet slår fast at det skal gjennomføres en avgrenset kartlegging av behovet. NorSIS gjør oppmerksom på at det ikke er foretatt en kartlegging av behovene i et representativt utvalg av kommuner. Kommunene som er utvalgt til styringsgruppen er alle større kommuner, slik at mindre kommuner ikke er direkte representert i styringsgruppen. Imidlertid er KINS en del av styringsgruppen, og de representerer derfor i prinsippet kommuner av alle størrelser.

At mindre kommuner i noen grad er underrepresentert kan være en fare for at behovsbeskrivelsen ikke ivaretar spesielle behov som mindre kommuner har. NorSIS vurderer likevel risikoen som lav, både fordi NorSIS rapport fra 2015[4] innhentet informasjon fra slike kommuner, og fordi det legges til grunn at representantene i styringsgruppen har kjennskap til behovene i hele kommunal sektor. I tillegg har prosjektet via KINS sendt behovsvurderingen til 30 mindre kommuner for å innhente deres synspunkter på de behov som styringsgruppen har kommet frem til. Syv kommuner besvarte anmodningen om innspill.

2.2 Valg av rammeverk

Det eksisterer en rekke begreper og betegnelser på håndteringsenheter som er involvert i håndteringen av sikkerhetshendelser i IKT infrastruktur. Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), Incident Response Team (IRT), Security Operations Center (SOC) er alle i noen grad involvert i slik håndtering. Begrepene brukes i noen grad som synonymer, men begrepet CERT «eies» av Carnegie Mellon University og det må søkes om tillatelse for å benytte det. For denne utredningen benyttes begrepet KommuneCSIRT som betegnelse for et kompetansesenter for håndtering av IKT-hendelser i kommunal sektor.

Over tid har det fremkommet ulike veiledninger, standarder og rammeverk som beskriver hvilke tjenester slike håndteringsenheter kan ha og hvordan en kan etablere slike tjenester. Rammeverkene representerer en strukturert og anerkjent metode for planlegging og etablering av håndteringsenheter. Denne utredningen skal kartlegge og beskrive behovene for en slik håndteringsenhet i kommunal sektor. Det er derfor ønskelig å benytte et rammeverk som har et tjenestefokus slik at en får et godt grunnlag til å vurdere om løsningsalternativene møter behovene.

4 *Kommune CERT – behov og muligheter*. NorSIS rapport 2015.

Det er spesielt to rammeverk som har et tydelig tjenestefokus. CMU/SEI CERT[5] har omfattende veiledninger for etablering av CERT-enheter. En av veiledningene[6] beskriver hvilke tjenester et CERT kan levere til sine medlemmer. FIRST CSIRT Framework[7] er et annet rammeverk som strukturerer og beskriver CSIRT tjenester.

NorSIS vurderer FIRST CSIRT Framework å være best egnet for denne utredningen. Rammeverket har en tydelig struktur for sin beskrivelse av tjenestene. Og det fremheves spesielt at det har en hierarkisk oppbygning som gjør det enklere å fokusere på delprosesser når det er behov for det. NorSIS viser også til at KraftCERT har erfaring med, og anbefaler, rammeverket.

5 Carnegie Mellon University / Software Engineering Institute CERT

6 CSIRT Services. CMU/SEI. http://www.cert.org/incident-management/services.cfm?#vcoordination Hentet fra nett: 20.06.2017

7 FIRST CSIRT Framework. Version 1.1. https://www.first.org/education/csirt_service-framework_v1.1 Hentet fra nett: 20.06.2017

3 Nåsituasjonsbeskrivelse

3.1 Hensikt og mål med beskrivelsen

Hensikten med nåsituasjonsbeskrivelsen er å danne et helhetlig og omforent bilde på kommunesektorens utfordringer innen IKT-sikkerhetshendelser og evne til å håndtere disse.

Kommunal sektors bruk av IKT er kompleks og sammensatt, og er i noen grad avhengig av IKT-løsninger som formelt sett er underlagt myndighet og styring som ligger utenfor sektoren. Beskrivelsen omhandler derfor også aktører og strukturer som en normalt ikke vil betrakte som en del av kommunal sektor.

3.2 Håndtering av IKT-hendelser i en nasjonal kontekst

Det nasjonale samfunnssikkerhets- og beredskapsarbeidet er basert på fire prinsipper; ansvar, nærhet, likhet og samvirke. De tre første prinsippene ble introdusert i St.meld. nr. 17 (2001–2002) Samfunnssikkerhet – veien til et mindre sårbart samfunn. Det fjerde prinsippet, samvirkeprinsippet, ble introdusert i Meld. St. 29 (2011–2012) Samfunnssikkerhet. Prinsippene er beskrevet i Vedlegg 1.

Operasjonssenteret i Nasjonal sikkerhetsmyndighet (NSM) NorCERT, er Norges nasjonale senter for å koordinere håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon[8]. NSM NorCERT er et nasjonalt samlingspunkt og en koordinerende enhet for IKT-sikkerhetshendelser. NSM NorCERT er den operative delen av NSM, dedikert til cybersikkerhet og hendelseshåndtering.

I Risiko 2017 skriver NSM at evnen til å oppdage alvorlige cyberhendelser må styrkes, både på nasjonalt plan, gjennom sektorvise responsmiljøer og i virksomhetene. Virksomhetene bør legge til rette for rapportering av hendelser til sektorvise responsmiljøer, som igjen videreformidler til det nasjonale kontaktpunktet, NSM NorCERT.

NSM har redegjort for sine anbefalinger for opprettelsen av sektorvise responsmiljøer[9]. NSM forutsetter at de sektorvise responsmiljøene har ansvar for koordinering av IT-sikkerheten i

8 *Nasjonal sikkerhetsmyndighet.* Beskrivelse av NorCERT. https://nsm.stat.no/norcert. Hentet fra nett 24.05.2017

9 *Nasjonal Sikkerhetsmyndighet.* Etablering av sektorvise responsmiljøer. Brev til Justis- og beredskapsdepartementet og Forsvarsdepartementet. Deres referanse A03 – S:14/01790-6

sin sektor, og at de er NSM NorCERTs kontaktpunkt ved IT-sikkerhetshendelser. NSM redegjør ikke for hva de legger i begrepet «sektor», men viser til at sektormodellen har tre nivåer: Virksomhetsnivå, Sektornivå og Nasjonalt nivå. Responsmiljøene omtales som ekspertorgan og knutepunkt for informasjon og informasjonsflyt, både til og fra sektoren. NSM forutsetter videre at de sektorvise responsmiljøene har en myndighet innen sin sektor, og de kan pålegge tiltak både ved forebygging og håndtering. Det legges ikke føringer for organiseringen av slike miljøer, men NSM anbefaler at de sektorvise responsmiljøene har følgende kapabiliteter for informasjonsdeling:

- Saksbehandlingssystem
- Vakttelefon
- Verdivurdering for sektor
- Oversikt over objekter og verdikjeder
- Eskaleringsrutiner for sektor
- Varslingsrutiner
- Kontaktpunkt mot NSM
- Varslingspunkt for hendelser
- Kan bruke PGP-kryptering
- PGP-regime for sektor
- Benytte TLP[10] for deling av ugradert, sensitiv informasjon
- TLP-regime for sektor

For virksomhetene i sektoren anbefaler de logging av en rekke teknologier og IT-løsninger.

Det er i dag etablert en rekke sektor CERT'er og andre tilsvarende respons- og håndteringsenheter. For kommunal sektor er det primært NorCERT, HelseCERT og KraftCERT som utøver håndterings- og koordineringsaktiviteter som direkte berører kommunale tjenester. I tillegg legger vi til grunn at interkommunale og kommersielle selskaper også håndterer IKT-hendelser som en del av sine leveranser til kommunene.

Den helhetlige nasjonale evnen til å håndtere hendelser omfatter i tillegg håndteringsmiljøer i øvrige sektorer, bransjer, virksomheter og sikkerhetsselskaper. I våre samtaler med NorCERT, HelseCERT, KraftCERT, FinansCERT og UninettCERT fremkommer det en generell beskrivelse av et godt og tillitsbasert samarbeid mellom aktørene. Det er derfor ikke uvanlig at en sektor CERT har gode bilaterale samarbeid med andre sektorers responsmiljøer, eller at slike CERT'er deler informasjon med andre selv om det ikke foreligger en formell samarbeidsavtale. En fremtidig KommuneCSIRT vil i så fall inngå som et nytt medlem i en allerede eksisterende og godt fungerende nasjonal struktur for håndtering av IKT-hendelser.

3.3 Politiske føringer

Digitalisering i offentlig sektor følger sektorprinsippet, med hvert departement som ansvarlig for digitalisering hos underliggende organ i sin sektor. Kommunal- og moderniseringsdepartementet er ansvarlig departement for samordning av den offentlige IKT-politikken. Samordningsrollen innebærer ansvar for å identifisere sektorovergripende utfordringer, og for å initiere, koordinere og følge opp tverrgående tiltak i statsforvaltningen. Det framgår av Prop. 1 S (2015–2016) Kommunal- og moderniseringsdepartementet at departementet skal bidra til at statens styring av kommunesektoren er samordnet, helhetlig og konsistent.

Det presiseres at normal departementsstyring innebærer at hvert departement er ansvarlig for sine underliggende etater. Kommuner og fylkeskommuner styres ikke av noe departement, og er ikke del av dette sektorprinsippet eller sektorstyringen.

10 TLP – Trafikklys protokoll. Rammeverk for deling og bruk av informasjon.

KS' (kommunesektorens organisasjon) rolle er å samordne digitaliseringsarbeidet i kommuner og fylkeskommuner, å ivareta kommunesektorens behov i statens digitaliseringsaktiviteter og å sørge for gode rammevilkår for digitalisering i kommuner og fylkeskommuner. Felles organisering og styring av digitaliseringsarbeidet i kommunal sektor gjennom slik samordning og koordinering, vurderes som et vesentlig virkemiddel om kommunal sektor skal lykkes innen digitalisering. KS kan gjennom god koordinering og oversikt bidra til at kompetansen i kommunene og fylkeskommunene engasjeres i det samlede digitaliseringsarbeidet.

Hovedstyret i KS vedtok høsten 2015 at KS skal styrke det interessepolitiske og strategiske arbeidet med digitalisering, og samtidig videreføre det medlemsbaserte utviklingsarbeidet der det er nødvendig og ønskelig. KS har en viktig rolle i å sørge for samordning og koordinering av kommunal sektor på digitaliseringsområdet og bidra til samordning mellom kommunal sektor og staten i digitaliseringsarbeidet i offentlig sektor.

Regjeringen la i 2016 frem Meld. St. 27 (2015-2016) Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet. Meldingen presenterer regjeringens overordnede politikk for hvordan vi kan utnytte IKT til samfunnets beste. Regjeringens IKT-politikk trekker opp to hovedmålsettinger:

1. En brukerrettet og effektiv offentlig forvaltning
2. Verdiskaping og deltakelse for alle

KS' Digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020[11]

Satsingsområdene i Digital agenda for Norge har stor betydning for digitalisering av offentlig sektor. Kommunal sektor møter disse satsingsområdene koordinert og samordnet gjennom KS' Digitaliseringsstrategi for kommuner og fylkeskommuner 2017-2020[12], der regjeringens satsingsområder fra Digital agenda for Norge er hovedområdene for kommunal sektors digitale satsing i Digitaliseringsstrategien:

1. Brukeren i sentrum
2. Digitalisering er en vesentlig innsatsfaktor for innovasjon og økt produktivitet
3. Styrket digital kompetanse og deltakelse
4. Effektiv digitalisering av offentlig sektor
5. Informasjonssikkerhet, personvern og dokumentasjonsforvaltning

Digital agenda for Norge peker på at de fleste kritiske infrastrukturer og samfunnsviktige funksjoner er i dag digitalisert. Dette medfører nye sårbarheter i samfunnet. Digitalisering har medført at flere samfunnsområder er gjensidig avhengig av hverandre og situasjonen er blitt mer kompleks. Det er derfor en forutsetning at digitale systemer er sikre og pålitelige, og at virksomheter og privatpersoner har tillit til at systemer og nettverk fungerer som de skal. Informasjonssikkerhet skal ivaretas med en risikobasert tilnærming med utgangspunkt i oppdaterte trussel- og sårbarhetsvurderinger. Informasjonssikkerhet skal følges opp gjennom god internkontroll.

Digitaliseringsstrategien har på området informasjonssikkerhet, personvern og dokumentasjonsforvaltning følgende mål for kommuner og fylkeskommuner:

1. Kommunal sektor skal ivareta informasjonssikkerhet og personvern på alle områder
2. Kommunal sektor skal sikre at riktig informasjon er tilgjengelig for rett person
3. Kommunal sektor skal sørge for innebygd personvern i nye løsninger
4. Kommunal sektor skal ha styringssystem for informasjonssikkerhet

---

11 *Kommunesektorens organisasjon.* Digitaliseringsstrategi for kommuner og fylkeskommuner 2017–2020 http://www.ks.no/fagomrader/utvikling/digitalisering/digitaliseringsstrategien/ Hentet fra nett 20.06.2017

12 *Kommunesektorens organisasjon.* Digitaliseringsstrategi for kommuner og fylkeskommuner 2017–2020 http://www.ks.no/fagomrader/utvikling/digitalisering/digitaliseringsstrategien/ Hentet fra nett 20.06.2017

5. Kommunal sektor skal dele informasjon om sikkerhetshendelser de har vært utsatt for
6. Kommunal sektor skal ha helhetlig dokumentasjons- og arkivforvaltning

NOU 2015:13 Digital sårbarhet – Sikkert samfunn trekker også opp bekymringer på overordnet politisk nivå: *Digitalisering av samfunnet har skapt avhengigheter og sårbarheter som går på tvers av sektorer, ansvar og landegrenser. IKT-sikkerhet får stadig større oppmerksomhet. Spørsmålene står høyt på den politiske agendaen i mange land, og har forsvars- og sikkerhetspolitiske så vel som utenriks og handelspolitiske dimensjoner. Digital sårbarhet og IKT-sikkerhet blir i økende grad sett på som noe som omhandler beskyttelse av velstandssamfunnet i sin helhet, ikke bare som et teknologispørsmål.*

3.4 Regelverk og standarder

Justis- og beredskapsdepartementet arbeider med et nytt rammeverk for håndteringsmiljøer som skal inngå i den nasjonale CERT-strukturen. Vi har ikke fått innsyn i rammeverket, men vi forutsetter at rammeverket er relevant for et KommuneCSIRT. Representanter fra NSM har imidlertid uttalt at de ser det som en fordel at håndteringsmiljøene er utpekt av, eller knyttet til, et departement for å sikre en sektorvis tilhørighet. Det er foreløpig ikke fremkommet noe som kaster lys over hva en legger i en slik tilknytning, eller om dette legger noen føringer for organisering av et håndteringsmiljø i kommunal sektor.

Det finnes forøvrig en rekke standarder og veiledninger for hvordan en kan eller bør gå frem ved etablering av en enhet som skal håndtere IKT-hendelser.

Ved valg av standard/rammeverk for utredningen, er det hensiktsmessig å peke ut én standard slik at begrepsbruken blir mest mulig enhetlig. Der øvrig begrepsbruk, eksempelvis i forbindelse med beredskapssystemene i kommunesektoren, ikke samsvarer med den valgte standardens begrepsbruk vil dette redegjøres for i et eget kapitel om begreper.

3.5 Digitale trusler mot kommunal sektor

Vi har i dette arbeidet ikke avdekket at det er noen enkeltaktør som har beskrevet et helhetlig trusselbilde som er dekkende og spesifikt for kommunal sektor.

På nasjonalt nivå er det gitt Politiets sikkerhetstjeneste (PST) å forebygge, avdekke og etterforske trusler som angår rikets sikkerhet. I sin rapport Trusselvurdering 2017[13] definerer PST at norsk kritisk infrastruktur fortsatt vil være et etterretningsmål i 2017 (side 8), og at formålet med slike etterretningsoperasjoner vil både være å hente ut informasjon om selve infrastrukturen samt å legge til rette for å kunne manipulere data eller forberede sabotasje, dersom det oppstår en tilspisset utenriks- eller sikkerhetspolitisk situasjon. Systemer innenfor kraftsektoren og elektroniske kommunikasjonstjenester anses som spesielt etterretningsutsatt kritisk infrastruktur.

PST fremhever også at politiske prosesser og beslutninger vil være gjenstand for fremmed etterretning og for påvirkningsoperasjoner. PST skriver (side 8): «***Slik politisk etterretning rettes mot beslutningstakere, eller premissleverandørene til disse, og har som siktemål å innhente informasjon om norske standpunkter i aktuelle politiske spørsmål. Samtidig vil det også være tjenestenes mål å gjennomføre ulike former for påvirkningsoperasjoner i de ulike sakene. Dette er operasjoner som er ment å sikre eget lands interesser, som regel på bekostning av de norske interessene.***»

13 *Politiets sikkerhetstjeneste.* Trusselvurdering 2017. Publisert 01.02.2017. Hentet fra nett 24.05.2017

Etterretningstjenesten (ETJ) skal understøtte norske myndigheter med informasjon om utenriks-, sikkerhets- og forsvarspolitiske forhold, samt å fremskaffe informasjon og varsle om forhold som kan true Norge og norske interesser. Deres rapport Fokus 2017[14] beskriver tjenestens ugraderte trusselvurdering. ETJ fremhever at de mest alvorlige truslene mot digitale systemer i Norge fremdeles vil ha Russisk og Kinesisk opphav. Russland vil fortsette med omfattende etterretningsvirksomhet mot norske mål, og det vil bli gjort en mer intensiv og systematisk kartlegging av sårbare punkt i kritiske system. I tillegg vil Russland videreutvikle operasjonelle konsept for digital støttet sabotasje.

Kinesisk aktivitet vil være rettet mot styresmakter, industribedrifter og teknologiselskap.

Verken PST eller ETJ omtaler kommunal sektor spesifikt, men kommunale beredskap, tjenesteproduksjon og beslutningsprosesser er åpenbart avhengige av IKT. Lysne-I utvalget skriver[15]: «*Hendelser som gir utfall av strømforsyningen til et område, vil i stor grad ramme elektronisk kommunikasjon og datasystemer. Bortfall av elektronisk kommunikasjon har vist seg å forsterke konsekvensene av naturkatastrofer, da det kompliserer krisehåndteringen og samhandlingen mellom redningsmannskaper, kommuner og private.*» (pkt. 7, side 52).

I følge NSMs rapport Risiko 2017[16] ble det registrerte om lag 22.000 uønskede hendelser mot informasjonssystemer i Norge i 2016. Ca. 5.000 av disse ble prioritert for oppfølging i NSM. Den generelle tendensen er at antall hendelser er stigende. NSM vurderer cyberangrep fra fremmede stater som den høyeste IKT-risikoen for offentlig forvaltning. Kommunal sektor er ikke omtalt, men det er nevnt en IKT-sikkerhetshendelse i Oppland fylkeskommune.

Eksisterende håndteringsmiljøer som HelseCERT, KraftCERT og større private tjenestetilbydere har en viss oversikt over trusselbildet mot deres fag- eller ansvarsområde. Våre samtaler med representanter for kommuner og fylkeskommuner viser også at enkelte kommuner, fortrinnsvis de større kommunene, har en viss oversikt over det digitale trusselbildet mot egen kommune.

I våre samtaler med representantene blir både økonomisk motiverte trusler og trusler fra nasjonalstater trukket frem som en del av trusselbildet mot kommunene.

3.6 Kritisk IKT-infrastruktur i kommunal sektor

3.6.1 Oversikt over kritisk IKT-infrastruktur

Digitaliseringen av kommunale tjenester og verdikjeder betyr nødvendigvis at avhengigheten til IKT øker i takt med digitaliseringsgraden. Riksrevisjonen har gjennomført en undersøkelse av digitalisering av kommunale tjenester[17]. Undersøkelsen gjør rede for status for digitaliseringen av kommunale tjenester, og i hvilken grad digitalisering av kommunale tjenester har betydning for effektivitet og samhandling i kommunal tjenesteproduksjon.

Undersøkelsen ser videre på mulige hindringer for digitalisering av kommunale tjenester, og hvordan Kommunal- og moderniseringsdepartementets virkemiddelbruk bidrar til digitalisering av kommunale tjenester. Undersøkelsen viser at norske kommuner generelt er kommet kort i digitaliseringen av kommunale tjenester. Riksrevisjonen finner at det er færre små enn store kommuner som har startet digitaliseringen av kommunale tjenester.

14 *Etterretningstjenesten.* Fokus 2017. Publisert 20.02.2017. Hentet fra nett 24.05.2017.

15 *Norsk Offentlig Utredning.* NOU 2015:13 Digital sårbarhet – Sikkert samfunn

16 *Nasjonal sikkerhetsmyndighet.* Risiko 2017. Publisert primo 2017. Hentet fra nett 24.05.2017.

17 *Riksrevisjonen.* Riksrevisjonens undersøkelse av digitalisering av kommunale tjenester. Riksrevisjonen. Dokument 3:6 (2015–2016).

Riksrevisjonens undersøkelse viser at en gjennomsnittlig kommune har mellom 180 og 200 ulike IKT-systemer[18].

Riksrevisjonens undersøkelse identifiserer ikke direkte hvilke IKT-systemer som er kritiske for kommunenes evne til å levere tjenester til innbyggerne. Våre samtaler med representantene fra kommuner og fylkeskommuner indikerer at en må påregne at kompleksiteten og de mange gjensidige avhengighetene mellom IKT-systemer gjør det svært utfordrende å klassifisere hvilke systemer som er kritiske og hvilke som ikke er det. En slik klassifisering er i dag ikke utført. I samtalene hevdes det at kommuner og fylkeskommuner trolig må forebygge og håndtere IKT-hendelser i samtlige av kommunens IKT-systemer. Det hevdes at hendelser kan forekomme i alle IKT-systemer i kommunene, og at slike hendelser har et potensiale for å skade kommunale IKT-tjenester.

DSB vil i sin evalueringsrapport etter øvelsen IKT 2016 trolig også berøre dette tema. Det er foreløpig ikke avklart når rapporten vil bli publisert, men det antas at det vil skje før utredningen om et KommuneCSIRT ferdigstilles.

3.6.2 IKT-driftsleverandører i kommunal sektor

Kommuner og fylkeskommuner er selvstendige forvaltningsnivåer, og er ikke en del av den hierarkisk oppbygde statsforvaltningen. Kommunesektoren har et selvstendig ansvar overfor sine innbyggere for å løse oppgaver, yte tjenester, drive samfunnsutvikling og utøve myndighet. Kommunen må selv gjennomføre gode digitaliserings- og utviklingstiltak på sine ansvarsområder[19].

Det er kritisk for kommunal sektor hvis de registrene, systemene, tjenestene og nettene som staten eier og leverer, stopper opp eller går ned. Men det er ikke kommunal sektors ansvar, ettersom kommuner og fylkeskommuner er brukere («kunder») av løsningene.

En naturlig konsekvens av en slik autonomi er en stor variasjon i hvordan kommunene har implementert leveransene av de digitale tjenestene. I notatet[20] «Kommunale IKT-tjenester», utarbeidet for Kommunal og Moderniseringsdepartementet, fremgår det at ulike kommuner velger ulike driftsmodeller for IKT. Noen kommuner har interne IKT-kapasiteter som sørger for drift av kommunens basis- og fagsystemer, mens andre kommuner har satt ut drift for deler eller hele IKT-området. Våre samtaler med representanter fra utvalgte kommuner og fylkeskommuner bekrefter dette.

Driftsmodellene kan være sammensatte, altså en kombinasjon av at en kommune forestår noe drift av egne IKT-løsninger, mens det er valgt ulike sourcing-strategier, herunder bruk av skytjenester, av deler av IKT-området. IKT-driftsleverandørene kan eksempelvis være interkommunale selskap (vanligvis regionale) eller nasjonale eller globale aktører.

Ulike eierstrukturer, driftsmodeller og IKT- og sikkerhetsstyringssystemer vil kunne skape utfordringer for håndtering av IKT-hendelser som finner sted på tvers av slike «barrierer». NorSIS erfarer at ulike legale rammer (eksempelvis ulik praksis for samtykke om inngripende metoder), ulike tekniske løsninger og ulike metoder for håndtering av IKT-hendelser i noen grad kan forhindre en effektiv håndtering av hendelser dersom alle slike forhold ikke er avklart på forhånd. Dette gjelder spesielt håndtering på et mer teknisk nivå.

18 *Ibid.*

19 Meld. St. 27 (2015-2016) Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet. S.57

20 *NEXIA International.* Notat: Kommunale IKT-tjenester – muligheter for mer effektiv drift. 2015. Utarbeidet for Kommunal- og moderniseringsdepartementet. Hentet fra nett: 21.06.2017

3.7 Kommunal sektors egen evne til å håndtere IKT-hendelser

NOU 2015:13 Digital sårbarhet – Sikkert samfunn problematiserer kommunal sektors egen evne til å håndtere IKT-hendelser: Kommunal sektor har et generelt og grunnleggende ansvar for å ivareta befolkningens sikkerhet og trygghet innenfor sitt geografiske område. Gjennom kommunal beredskapsplikt er kommuner og fylkeskommuner blant annet pålagt et ansvar for å gjennomføre en helhetlig risiko- og sårbarhetsanalyse, herunder kartlegge, systematisere og vurdere sannsynligheten for uønskede hendelser som kan inntreffe i kommunen, og hvordan disse kan påvirke kommunen. Kommuner og fylkeskommuner har også et ansvar for å være forberedt på å håndtere uønskede hendelser, og skal med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen utarbeide en overordnet beredskapsplan. Kommunen/fylkeskommunens overordnede beredskapsplan skal samordne og integrere øvrige beredskapsplaner i kommunen/fylkeskommunen[21].

I NOU 2015:13 hevdes det videre at kommunene har i dag bare unntaksvis en tydelig sikkerhetsorganisasjon, og etterspør derfor i liten grad relevant kompetanse innen IKT-sikkerhet. Kommunene har stort sett små IKT-miljøer, der IKT-sikkerhetsarbeidet bare er én av mange oppgaver for IKT-personalet. Også fylkesmennene har små organisasjoner uten dedikert personell med kompetanse innen IKT-sikkerhet. Ansvaret for IKT-sikkerhet er ofte tillagt personale med andre hovedoppgaver, og som mangler nødvendig spisskompetanse på sikkerhet. Mange ledere har også for lav bevissthet om at de er ansvarlige for IKT-sikkerheten, og har verken vilje eller evne til å ivareta denne rollen[22].

Denne fremstillingen bekreftes i våre samtaler med representantene fra kommunene og fylkeskommunene.

Kommunene har ansvar for mange viktige samfunnsfunksjoner, som spenner vidt i fagområder og gjør at en kommunal kriseledelse må være forberedt på å håndtere hendelser av svært ulik karakter og med svært mange og ulike aktører. Sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt setter rammene for lokal krisehåndtering[23].

Forskrift om kommunal beredskapsplan § 4 slår fast at kommunen skal være forberedt på å håndtere uønskede hendelser, og skal med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen utarbeide en overordnet beredskapsplan. Kommunens overordnede beredskapsplan skal samordne og integrere øvrige beredskapsplaner i kommunen. Den skal også være samordnet med andre relevante offentlige og private krise- og beredskapsplaner[24].

NorSIS utredet[25] behov og muligheter for et KommuneCERT i 2015, på oppdrag fra Lillehammer og Gjøvik kommune. Som grunnlag for vurderingene, ble det gjennomført intervjuer med et utvalg kommuner og interkommunale selskaper. Rapporten viser til at intervjuobjektene ser viktigheten av å få en sentralisert enhet som kommer med entydige og klare anbefalinger tilpasset kommunesektoren knyttet til sårbarheter og trusler. Varsling har vært en tjeneste som alle kommunene har nevnt som grunnleggende å få igangsatt. En del kommuner mottar varsler fra HelseCERT, men disse er generelle.

Gjennom våre samtaler med representanter fra kommuner og fylkeskommuner fremkommer det at de fleste har god kjennskap til hvordan håndtering av IKT-hendelser skjer i egen kommune og fylkeskommune, og at de mener å ha en viss kjennskap til hvordan slik håndtering skjer i kommunal sektor for øvrig. Det er store forskjeller i hvordan kommunene har organisert IKT-området, og det vises til at modenheten for informasjonssikkerhet i kommunal sektor er varierende.

---

21 *Norsk Offentlig Utredning*. NOU 2015:13 Digital sårbarhet – Sikkert samfunn (Side 65/66)

22 *Ibid.* (Side 224)

23 *Ibid.* (Side 242)

24 *Lovdata*. Forskrift om kommunal beredskapsplan. Ikrafttredelse 07.10.2011

25 *Kommune CERT* – behov og muligheter. NorSIS rapport 2015.

Kommunene opplever en del uønskede hendelser som må håndteres. De største kommunene har evne til å håndtere en del av disse hendelsene selv, og det hevdes samtidig at situasjonen ofte ikke er slik for de mindre kommunene. Det vises til at mangel på ressurser og nødvendig kompetanse i de mindre kommunene forhindrer en effektiv håndtering av IKT-hendelser. I våre samtaler blir det også beskrevet et uformelt samarbeid mellom enkeltpersoner og mellom kommuner og andre aktører som HelseCERT. Ettersom samarbeidene i stor grad er uformelle, gir det også utfordringer med å holde oversikt over hvilke ressurser en har å spille på ved håndtering av IKT-hendelser. Realiteten for mange kommuner er at de er avhengige av ildsjeler som tar tak i de hendelsene som oppstår. Dette utgjør en stor sårbarhet for kommunene, dersom disse går over i nye stillinger.

Flere av representantene opplyser at IKT-hendelser gjerne håndteres som en del av det de omtaler som «vanlig drift», enten driften utføres av kommunene selv eller av eksterne IKT-driftsleverandører. Noen kommuner har vakt-funksjoner som kan respondere på henvendelser, mens andre ikke har noen utvidet beredskap på dette området. Det hevdes at et håndteringsmiljø må ha en viss størrelse for at det skal kunne håndtere IKT-hendelser på en effektiv og profesjonell måte, og at dette ikke er situasjonen i mange av kommunene i dag.

Det blir fremhevet at kommunene ikke har evne til de mer teknologiske delene av håndteringen, for eksempel malware-analyse og penetrasjonstesting. Dette kjøpes i noen grad i dag fra eksterne sikkerhets-leverandører, eller ved at kommunene mottar støtte fra andre håndteringsmiljøer, fortrinnsvis fra HelseCERT.

Representantene hevder videre at flere av de grunnleggende forutsetningene for en effektiv håndtering ikke er på plass. Spesielt fremheves det at trusselforståelsen er svært ulik fra kommune til kommune, og at det ikke finnes noen som har et helhetlig trusselbilde for sektoren. Det er heller ikke foretatt en komplett gjennomgang av hvilke IKT-systemer som faktisk finnes i sektoren ut over at det i beredskapssammenheng er ført noe oversikt over hvilke kritiske systemer kommunene har.

Noen av representantene opplever at kommuneledelsen har interesse for digitale trusler og utfordringer innenfor IKT-området, mens andre opplever det som mer krevende å nå frem med sikkerhetsbudskap til ledelsen.

3.8 Andre aktørers evne til å håndtere IKT-sikkerhetshendelser i kommunesektoren

Det er ikke foretatt en aktøranalyse for aktører som vil eller kan inngå i håndteringen av IKT-sikkerhetshendelser i kommuner og fylkeskommuner.

De eksisterende håndteringsmiljøene (f.eks. HelseCERT) har evne til å koordinere og håndtere IKT-sikkerhetshendelser som berører deres eget fagområde, og i begrenset grad gi støtte til håndtering av hendelser som går ut over deres eget fagområde. Håndteringsmiljøene inngår i den nasjonale CERT-strukturen, og mottar relevante varsler og annen bistand gjennom dette.

De fleste representantene for kommuner og fylkeskommuner som vi har snakket med fremhever samarbeidet med HelseCERT som det viktigste nåværende håndteringsmiljøet for dem. HelseCERT bidrar forebyggende ved å kartlegge sårbarheter i noen kommuner, og med sensoroverv̊aking for kommunenes primærhelsetjeneste. De bidrar også med støtte til håndtering gjennom å varsle om trusler og hendelser, og med noe teknisk analyse.

En bør her merke seg at flere av representantene vi har snakket med mener at ikke alle kommuner, og da fortrinnsvis de mindre kommunene, har tilstrekkelig kompetanse til å gjøre nytte av den hjelp som eksterne sikkerhetsaktører kan tilby.

I våre samtaler med representantene fra kommuner og fylkeskommuner vises det til at eksterne IKT-driftsleverandører har evne til å håndtere IKT-hendelser, men at det trolig er store variasjoner også her.

3.9 Kommunal sektors hovedutfordringer ved håndtering IKT-sikkerhetshendelser

Med bakgrunn i samtalene med representantene for kommuner og fylkeskommuner er dette de felles hovedutfordringer for kommunal sektors evne til å håndtere IKT-hendelser:

- Det er ingen aktører som i dag beskriver et helhetlig situasjonsbilde (trusler, sårbarheter, hendelser og sikkerhetstiltak) for kommunal sektor

- Det er ingen aktører som i dag har ansvar for varsling og informasjonsdeling mellom alle kommuner, fylkeskommuner og andre håndteringsmiljøer i sektoren. Noe varsling og deling finner sted, primært sentrert rundt eksisterende håndteringsmiljøer og i kommuner som har kompetanse og kapasitet til dette

- Kommunal sektor har i dag ikke et felles ressurs- eller kompetansesenter som kan støtte kommunene med tekniske analyser, eller teknisk eller metodisk støtte ved håndtering av IKT-hendelser

- Det er ikke formalisert et kontaktpunkt for kommunal sektor i den nasjonale CERT-strukturen. Deler av kommunal sektor dekkes gjennom kontaktpunktene i øvrige responsmiljøer som HelseCERT, KraftCERT og NorCERT.

4 Behovsbeskrivelse

4.1 Bakgrunn

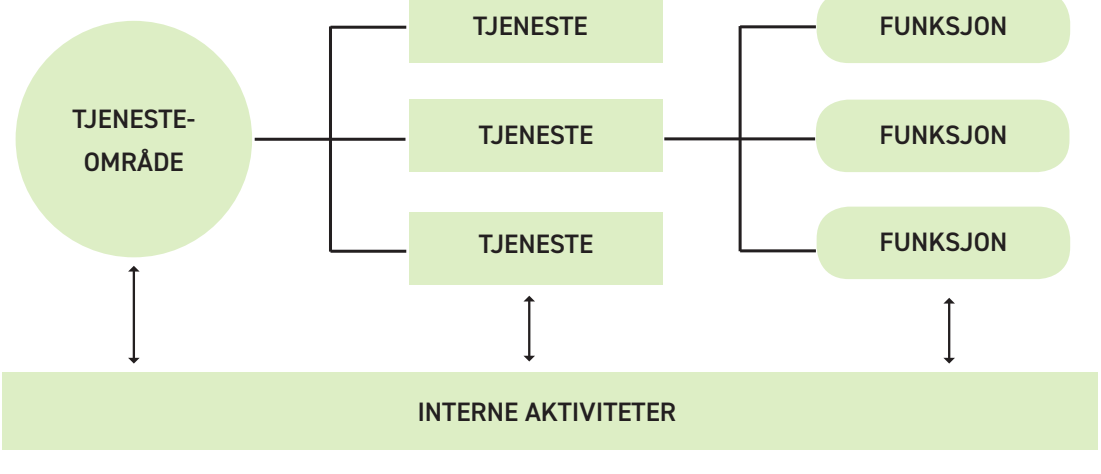
Behov knyttet til et KommuneCSIRT defineres av kommunal sektor. Kommunene som er pekt ut til å delta i prosjektets styringsgruppe er i prosjektmandatet gitt ansvar for å sikre at kommunenes felles behov blir ivaretatt. I tillegg kan representantene i prosjektets referansegruppe gi råd og veiledning til prosjektadministrasjonen.

Behovsbeskrivelsen presenterer målet med denne utredningen, og det gis en oversikt over de kartlagte behovene. Behovene struktureres iht. et anerkjent rammeverk for beskrivelse av CSIRT tjenester.

4.2 CSIRT tjenester

En måte å betrakte et CSIRT er hvilke tjenester det leverer til sine medlemmer. Et tjenestefokus basert på behovene muliggjør en strukturert tilnærming til etableringen av et CSIRT, herunder organisering og etablering av interne prosesser. FIRST CSIRT Framework benyttes som rammeverk for å beskrive tjenestene.

Rammeverket beskriver tjenestene i tre nivåer: Tjenesteområder, tjenester og funksjoner. Et tjenesteområde kan bestå av flere tjenester, som igjen kan bestå av flere funksjoner. Disse etableres gjennom interne aktiviteter.



Figur 1: Sammeheng mellom tjenesteområder, tjenester, funksjoner og interne aktiviteter

Et CSIRT kan levere innenfor alle tjenesteområder i rammeverket, eller bare en del av dem. For et gitt tjenesteområde betyr det at ulike CSIRT kan ha ulik kapabilitet til å levere tjenester. Dette kan illustreres ved at et CSIRT har evne til å utføre overfladiske malware analyser, mens et annet har evne til å utføre dyptgående analyser.

For et gitt tjenesteområde kan ulike CSIRT også ha ulike kapasitet, altså hvor «mye» av tjenesten de kan levere. Dette kan illustreres ved at et CSIRT har kapasitet til å utføre en malware analyse per tidsenhet, mens et annet CSIRT kan utføre et større antall.

Det er avhengigheter mellom enkelte tjenesteområder, slik at behov for et tjenesteområde kan medføre at et CSIRT også må etablere et annet tjenesteområde.

4.3 Kommunesektorens behov for CSIRT tjenester

Representantene i prosjektets styringsgruppe har ut fra sine respektive ståsteder bidratt til å beskrive kommunal sektors behov for CSIRT tjenester. I tillegg har NorSIS innhentet synspunkter og råd fra prosjektets referansegruppe, og fra eksisterende håndteringsenheter i Norge.

Prosjektmandatet slår fast at de behov som er felles i kommunal sektor skal kartlegges og beskrives. NorSIS tolker dette slik at det må være et flertall av de representerte kommunene som har uttrykt behovet, eller at behovet vurderes å ha nytte for alle kommuner. Dette innebærer at enkelte representanter kan ha ytret et behov, men at dette ikke anses å være et felles behov for kommunal sektor. Slike behov er likevel relevante fordi en må påregne at et CSIRT har et utviklings- og modenhetsforløp. Tjenester som ved etableringen av et CSIRT ikke vurderes som relevante, kan over tid vise seg å være nødvendige.

4.3.1 Felles behov

Støtte til håndtering av hendelser

Alle representantene i styringsgruppen anser støtte til håndtering av hendelser som et sentralt behov i sektoren. Det vises til at kommunene har mangelfull kunnskap om håndtering av hendelser, og at det vil være både ressursbesparende og effektivt å ha en sentral enhet som kommunene kan støtte seg på. Det fremheves at behovsnivået på støtten vil variere, fra kommune til kommune, og fra sak til sak.

Representantene forventer at et KommuneCSIRT skal bidra med samordning og koordinering i sektoren, og med øvrige håndteringsenheter i den nasjonale CERT-strukturen. Et KommuneCSIRT anses som et naturlig koordineringspunkt for sektoren ved nasjonale hendelser.

Informasjonsdeling, både innad i kommunal sektor og i den nasjonale CERT-strukturen, fremheves som et sentralt behov. Det forventes at et KommuneCSIRT skal dele informasjon om sårbarheter, trusler, hendelser og tiltak.

Etablering av et felles situasjonsbilde

Det er bred enighet om at kommunene mangler informasjon om digitale trusler og hendelser som kan ha betydning for deres evne til å levere kommunale tjenester. Det er derfor uttrykt et behov for et felles situasjonsbilde for kommunal sektor. Primært er det behov for et felles situasjonsbilde som inneholder informasjon om sårbarheter, trusler og hendelser.

Kommunene har behov for statistikk og annen informasjon som er egnet til å øke deres robusthet mot digitale trusler gjennom å bidra til en bedre forebygging mot slike.

Som et grunnlag for en relevant situasjonsforståelse i kommunene, mener også representantene at et KommuneCSIRT aktivt må kunne innhente informasjon om tekniske sårbarheter. Dette innebærer teknisk kartlegging av digitale infrastruktur (Sårbarhetsscanning) og penetrasjonstesting. Det kan også innebære teknisk sensor-overvåking i infrastrukturen, men NorSIS oppfatter ikke at dette er uttrykt som et felles behov av representantene.

Støtte til analyser

Representantene mener at et KommuneCSIRT skal kunne gi teknisk støtte i forbindelse med analyse av digitale elementer. Spesielt pekes det på analyse av tekniske sårbarheter og ondsinnet kode. I tillegg nevnes digital diagnosestilling og håndtering av digitale bevis som noe kommunene har behov for støtte til.

Støtte til opplæring og kompetanseheving

Det beskrives en situasjon hvor kunnskap om informasjonssikkerhet er mangelvare i mange kommuner. Representantene mener at et KommuneCSIRT må bidra til kompetanseheving av personell som har roller i forbindelse med informasjonssikkerhet i kommunene. Det er også uttrykt et behov for at et KommuneCSIRT bidrar med holdningsskapende aktiviteter, og med andre opplæringstiltak i kommunene generelt.

Veiledning, rådgiving og revisjon

Representantene mener at et KommuneCSIRT bør ha en veilederrolle overfor kommunene. Spesielt fremheves behovet for at et slikt kompetansesenter bør kunne gi råd og veiledning innen informasjonssikkerhet, og at dette vil bidra til forebygging av hendelser.

Det er også uttrykt et behov for at et sentralt kompetansesenter i kommunal sektor kan gjennomføre revisjoner i kommunene for å avdekke om lovkrav og regelverk etterkommes.

Representantene mener det er et behov for at et KommuneCSIRT kan støtte kommunene med risikovurderinger. Det fremheves at det er størst behov for støtte til risikovurderinger som er spesifikke for sektoren.

4.3.2 Andre behov

Det har fremkommet noen behov som ikke fremstår som felles for sektoren. Dette betyr ikke at behovene er irrelevante, spesielt om en tar høyde for at et KommuneCSIRT skal utvikle seg over tid.

Det er uttrykt et behov for at et KommuneCSIRT bør støtte kommunene med bestiller-kompetanse ved anskaffelser der informasjonssikkerhet er en del av vurderingene.

Det er også uttrykt et behov for at en sentral enhet bør etablere og opprettholde en oversikt over alle IT-systemer i kommunal sektor, og at et KommuneCSIRT bør ha egne sensorer som overvåker aktivitet i datanettverk og internettforbindelser.

4.3.3 Behov knyttet til kapasitet

I tilknytning til de ovennevnte behov, vil det alltid være et spørsmål om kapasitet. Hvor ofte skal situasjonsbildet oppdateres? Hvor mange hendelser skal et KommuneCSIRT være i stand til å håndtere samtidig? Hvor mye og hvor ofte skal ulike typer støtte gis til kommunene?

Representantene viser til at norske kommuner kjøper en del sikkerhetstjenester fra kommersielle aktører, og flere opplyser om at spesielt HelseCERT støtter noen kommuner med sikkerhets-

tjenester. NorSIS har imidlertid ikke avdekket at det finnes en oversikt over omfanget av slik støtte. En må også påregne at det er mørketall her, altså kommuner som ikke har fått støtte, men som burde hatt det.

Representantene mener at et KommuneCSIRT må kunne levere de viktigste tjenestene når hendelsene oppstår, eller når kommunene har behov for dem. Ettersom hendelser kan finne sted når som helst på døgnet, innebærer det at et KommuneCSIRT bør kunne tilby de viktigste tjenestene døgnet rundt. Det er ulike syn på hvorvidt det må være døgnbemanning, eller om det er tilstrekkelig med en døgnbasert vaktordning som kan eskalere en hendelse ved behov.

Responstid er en annen faktor i kapasitetsvurderingen. Representantene omtaler responstid som en faktor som trolig vil være kritisk for nytteverdien av et Kommune CERT. Det fremstår som åpenbart at støtte til analyse må skje synkronisert med beslutningsprosessene. Analyser som fremkommer etter at håndtering av hendelsen har funnet sted, har liten verdi. Det vil på forhånd være vanskelig å slå fast hvor stor kapasitet det må være for de enkelte tjenestene. Noen representanter i styrings- og referansegruppen har uttrykt at en må være forberedt på å dimensjonere kapasiteten etter behovet når en ser hva behovet faktisk er.

4.4 CSIRT tjenesteområder i et KommuneCSIRT

Med bakgrunn i de ovennevnte behov utledes det at et KommuneCSIRT må etablere følgende tjenesteområder for å dekke sektorens felles behov. Tjenesteområdene beskrives iht. strukturen i FIRST CSIRT Framework.

Tjenesteområde 1: Styring av hendelseshåndtering

Hendelseshåndtering er en hovedoppgave for et CSIRT, og omfatter følgende tjenester:

Tjeneste 1.1: Utføre hendelseshåndtering
Tjeneste 1.2: Analyse av hendelser
Tjeneste 1.3: Skadebegrensning og gjenoppretting

Tjenesteområde 2: Analyse

Ved håndtering av hendelser, er det påkrevd at et CSIRT analyserer digitale elementer (engelsk: artifacts) som er knyttet til hendelsen. Det finnes mange forskjellige typer digitale elementer, som hver krever ulike kompetanseområder og håndteringsmetoder. Tjenesteområdet omfatter følgende tjenester:

Tjeneste 2.1: Analyse av digitale elementer
Tjeneste 2.2: Analyse av digitale medier
Tjeneste 2.3: Analyse av sårbarheter

Tjenesteområde 3: Informasjonssikring

Et CSIRT har omfattende erfaring fra hendelseshåndtering, og gjennom dette en god forståelse for risikobildet. Det er derfor ønskelig å involvere CSIRT i risikovurderinger som er knyttet til IKT-tjenester. Dette tjenesteområdet beskriver tjenester som vil bidra til å forbedre slike risikovurderinger, og omfatter følgende tjenester:

Tjeneste 3.1: Risikovurdering
Tjeneste 3.2: Virksomhetsstøtte
Tjeneste 3.3: Støtte til virksomhetskontinuitet og «Disaster recovery» planlegging
Tjeneste 3.4: Støtte til utføring av teknisk sikkerhetsarbeid.
Tjeneste 3.5: Støtte til «patch management»

Tjenesteområde 4: Situasjonsforståelse

Et CSIRT må etablere en oversikt over digitale trusler både for å kunne fokusere sine egne aktiviteter, gi relevante råd, og for å kunne gi støtte til risikovurderinger.

Å etablere en situasjonsforståelse innebærer å følge med på trusselaktører, angrepsmetoder, egne sårbarheter og relevante hendelser. Situasjonsforståelsen oppstår i konteksten av de kritiske virksomhetsprosessene, og infrastrukturen som understøtter disse. Denne kunnskapen gir grunnlag for bedre beslutninger, høyere sikkerhetsbevissthet og at virksomheten kan operere med lavere risiko. Tjenesteområdet omfatter følgende tjenester:

Tjeneste 4.1: Operative metrikker (målinger)
Tjeneste 4.2: Sammenstilling og korrelering
Tjeneste 4.3: Utvikling og foredling av etterretninger

Tjenesteområde 5: Kommunikasjon

Et CSIRT har en erfaringsbasert og unik posisjon til å bidra med kunnskap om aktuelle trusler, og forebyggende og reaktive tiltak. Slik informasjon kan også inngå i grunnlaget for utarbeidelse av retningslinjer i virksomheten. Dette tjenesteområdet omfatter tjenester som bidrar til å heve den generelle forståelsen for trusselbildet og behovet for sikringstiltak. Disse er:

Tjeneste 5.1: Råd for heving av sikkerhetsbevissthet
Tjeneste 5.2: Råd vedrørende utvikling av informasjonssikkerhetspolicy
Tjeneste 5.3: Informasjonsdeling og publikasjoner

Tjenesteområde 6: Kapabilitetsutvikling

Det forventes at et CSIRT utvikles over tid, og at det holder seg oppdatert på relevante endringer i trussel og sårbarhetsbildet. Dette tjenesteområdet inneholder tjenester som utvikler CSIRT tjenestene og personellet. Disse er:

Tjeneste 6.1: Organisatoriske metrikker
Tjeneste 6.2: Gjennomføre utdanning og trening
Tjeneste 6.3: Gjennomføre øvelser
Tjeneste 6.4: Teknisk rådgiving
Tjeneste 6.5: Identifisere læringspunkter etter hendelseshåndtering

4.5 CSIRT Tjenesteområder det ikke er behov for

Det er ikke uttrykt eller utledet behov for følgende tjenesteområde:

Tjenesteområde 7: Forskning og utvikling

Utvikling av ny kunnskap kan være nødvendig for utviklingen av et CSIRT. Dette tjenesteområdet inneholder følgende tjenester:

Tjeneste 7.1: Utvikle metoder for sårbarhetsanalyser
Tjeneste 7.2: Utvikle prosesser og teknologi for innhenting, sammenstilling og korrelering av etterretninger
Tjeneste 7.3: Utvikle digitale verktøy

4.6 Prioritering av felles behov

Styringsgruppen har prioritert de ovennevnte behov iht. kritikalitet, altså hvilke behov som ansees som de viktigste for kommunal sektor. Prioriteringen kan ansees som en «retning» for arbeidet med å etablere et KommuneCSIRT, der det bør legges vekt på å først etablere de tjenestene det er størst behov for. Følgende viser tjenesteområdene i prioritert rekkefølge:

Tjenesteområde 4: Situasjonsforståelse
Tjenesteområde 5: Kommunikasjon
Tjenesteområde 3: Informasjonssikring
Tjenesteområde 6: Kapabilitetsutvikling
Tjenesteområde 1: Styring/Ledelse av hendelseshåndtering
Tjenesteområde 2: Analyse

5 Løsningsalternativer

Ved utarbeidelse av løsningsalternativer legges hovedfokuset på hvilken kapabilitet og kapasitet et KommuneCSIRT kan ha. I tillegg belyses organisering, finansiering og lokalisering.

For kapabilitet vurderes det om alternativene møter kommunal sektors felles behov, gjennomførbarhet og kostnad.

5.1 Kapabilitet

Kommunal sektors felles behov for støtte til håndtering av IKT-hendelser er beskrevet i kapitel 4. Når en betrakter eksisterende håndteringsmiljøer i andre sektorer er det imidlertid klart at slike kan etableres på ulike vis. Noen håndteringsmiljøer er mer overordnet og koordinerende, mens andre er mer teknologiorientert og utøvende. Det som skiller dem fra hverandre er hvilke kapabiliteter håndteringsenheten har og, som en følge av dette, hvilke tjenester den tilbyr.

Å velge et alternativ ved etablering av et KommuneCSIRT utelukker ikke det å utvide tjenesteporteføljen på et senere tidspunkt, men det gir en prioritet ved etableringstidspunktet.

5.1.1 Alternativ 1 – Overordnet og koordinerende

Alternativ 1 beskriver et KommuneCSIRT som har et overordnet og koordinerende fokus, der tjenesteområdene 4 *Situasjonsbilde* og 5 *Kommunikasjon* inngår. Gjennom innsamling og bearbeiding av relevant informasjon skal KommuneCSIRT kunne etablere et felles situasjonsbilde for kommunal sektor, der fokuset er rettet mot digitale trusler, digitale sårbarheter, relevante hendelser og tiltak. KommuneCSIRT distribuerer fortløpende et situasjonsbilde og aktuelle råd om sikringstiltak og annen informasjon som er egnet til å øke evnen til å oppdage og håndtere hendelser i kommunal sektor, samt å forebygge mot slike. Det forutsettes at KommuneCSIRT har kunnskap om den generelle situasjonen og utfordringer i kommunal sektor. Det forutsettes også at tjenesteområde 6 *Kapabilitetsutvikling* inngår.

NorSIS vurderer at Alternativ 1 møter de felles behovene som representantene i styringsgruppen vurderer som de mest kritiske, men behov som er knyttet til utførelse av hendelseshåndtering og tekniske undersøkelser og analyser møtes ikke direkte. Sistnevnte behov kan i noen grad løses ved at et KommuneCSIRT koordinerer teknisk støtte til kommunene gjennom avtaler med kommersielle leverandører, eller gjennom avtaler med øvrige håndteringsmiljøer som NorCERT eller HelseCERT. NorSIS vurderer at det omfattende teknologiske mangfoldet medfører at det er lite trolig at hendelseshåndtering, tekniske undersøkelser og analyser kan utføres i samtlige IKT-løsninger i kommunal sektor.

Dersom Alternativ 1 velges legger dette ingen hindringer for at et KommuneCSIRT kan utvides til å omfatte alle tjenesteområdene (i realiteten Alternativ 3) på et senere tidspunkt. Alternativ 1 gir mulighet til å etablere en overordnet og helhetlig oversikt over utfordringer og muligheter i kommunal sektor, slik at dette kan danne grunnlag for en videreutvikling av tjenestene i KommuneCSIRT.

NorSIS vurderer at Alternativ 1 har høy gjennomførbarhet da det ikke er kjent at det er lovmessige eller teknologiske hindringer for at en etablering skal kunne finne sted.

En kostnadsmessig vurdering må gjøres i sammenheng med kapasitetsvurderinger rundt bemanning og beredskap. Om en tar i betraktning hvordan andre håndteringsmiljøer[26] har etablert tilsvarende funksjoner, ansees en minimumsbemanning på 3 personer for å kunne levere tilfredsstillende på de to nevnte tjenesteområdene. Et nøkternt kostnadsoverslag viser en årlig kostnad pålydende 5 MNOK som skal dekke lønnsutgifter, driftsutgifter og utgifter til infrastruktur og lokaler. Kostnadsoverslaget er usikkert, og vil kunne påvirkes av geografisk betingede lønnsutgifter og ambisjoner knyttet til bemanning og beredskap.

Oppsummert:
- Overordnet fokus på situasjonsforståelse, informasjonsdeling og kommunikasjon
- Møter de mest kritiske behovene i kommunal sektor
- Høy gjennomførbarhet
- Kostnadsoverslag på 5 MNOK første år

5.1.2 Alternativ 2 – Teknisk og utøvende

Alternativ 2 beskriver et KommuneCSIRT som har et teknisk og utøvende fokus, der tjenesteområdene 1 *Styring av hendelseshåndtering* og 2 *Analyse* inngår. KommuneCSIRT utfører egne tekniske undersøkelser og analyser som en del av hendelseshåndtering, eller som støtte til kommunene. Slike undersøkelser kan omfatte støtte til sårbahetsmåling, penetrasjonstesting, logg-analyse, nettverksovervåking, analyse av digitale medier og digital bevissikring. Det forutsettes at KommuneCSIRT har inngående kunnskap om de tekniske løsningene de skal utøve støtte i, og om de tekniske metoder som trusselaktørene kan anvende mot kommunal sektor. Det forutsettes også at tjenesteområde 6 *Kapabilitetsutvikling* inngår.

NorSIS vurderer at Alternativ 2 møter de felles behovene som representantene i styringsgruppen vurderer som de minst kritiske. Behov som er knyttet til situasjonsforståelse og informasjonsdeling i kommunal sektor møtes ikke direkte. Kommunal sektor vil kunne motta generell trussel- og sårbarhetsinformasjon fra NorCERT, uten at denne blir bearbeidet i et KommuneCSIRT. Det nevnes at NorCERT ikke har tilrettelagt sine tjenester til å direkte støtte kommunal sektor i dag, slik at det i så fall må inngås egne avtaler om dette. Kostnadene knyttet til en slik avtale vil ikke være kjent før det eventuelt er forhandlet frem en slik avtale med NSM.

Dersom Alternativ 2 velges legger dette ingen hindringer for at et KommuneCSIRT kan utvides til å omfatte alle tjenesteområdene (i realiteten Alternativ 3) på et senere tidspunkt. Alternativ 2 gir mulighet til å etablere en bedre forståelse av utfordringer og det som faktisk skjer på et teknologisk nivå. Dette kan bidra til å danne et grunnlag for å etablere en overordnet forståelse for situasjonen i kommunal sektor, og videre danne grunnlag for en videreutvikling av tjenestene i KommuneCSIRT.

NorSIS vurderer at Alternativ 2 har lav til moderat gjennomførbarhet da det er kjent at det er visse teknologiske hindringer for at tjenestene skal kunne leveres i alle IKT-systemer i kommunal sektor. Det teknologiske mangfoldet i kommunal sektor er stort. I en undersøkelse fra Riksrevisjonen fremkommer det at en gjennomsnittlig kommune har mellom 180 og 200 ulike

26 Eksempelvis HelseCERT, FinansCERT og KraftCERT

IKT-systemer[27]. Det antas at mange av disse er basert på samme teknologi (eksempelvis systemer og programvare levert av Microsoft), men en må påregne at mange systemer er basert på teknologi som krever at personellet i et KommuneCSIRT må ha egen og inngående opplæring for å kunne yte tjenester i disse systemene, herunder det å kartlegge et hendelsesforløp gjennom analyse av logger, nettverksdata og andre digitale enheter. SCADA og sky-løsninger nevnes som eksempler, og det er i tillegg kjent at det finnes en del egenutviklede systemer i enkelte kommuner. I tillegg er det et stort mangfold også for IKT-infrastruktur i kommunal sektor.

En kostnadsmessig vurdering må gjøres i sammenheng med kapasitetsvurderinger rundt bemanning og beredskap. Både mangfoldet i teknologiske løsninger og omfanget av støtten vil dimensjonere behovet for bemanning. Usikkerhet knyttet til dette gjør kostnadsoverslaget usikkert. Om en tar i betraktning hvordan øvrige håndteringsmiljøer[28] har etablert tilsvarende tjenester, ansees en minimumsbemanning på 5–7 personer for å kunne levere tilfredsstillende på de to nevnte tjenesteområdene. Et nøkternt kostnadsoverslag viser en årlig kostnad pålydende 9 MNOK som skal dekke lønnsutgifter, driftsutgifter og utgifter til infrastruktur og lokaler. Kostnadsoverslaget er usikkert, og vil kunne påvirkes av geografisk betingede lønnsutgifter og ambisjoner knyttet til bemanning og beredskap. Kostnader knyttet til lisenser og teknisk utstyr representerer også en usikkerhet.

Oppsummert:
- Fokus på støtte til tekniske undersøkelser og analyser
- Møter ikke de mest kritiske behovene i kommunal sektor
- Lav til moderat gjennomførbarhet
- Kostnadsoverslag på 9 MNOK per år

5.1.3 Alternativ 3 – Komplett tjenestespekter

Alternativ 3 beskriver et KommuneCSIRT som dekker alle felles behov. Dette omfatter både de overordnede tjenesteområdene knyttet til situasjonsforståelse og kommunikasjon, og de tekniske tjenesteområdene knyttet til utførelse av hendelseshåndtering og analyse. I tillegg støtter KommuneCSIRT innen tjenesteområde 3 *Informasjonssikring*. Det forutsettes også at tjenesteområde 6 *Kapabilitetsutvikling* inngår.

NorSIS vurderer at Alternativ 3 møter alle felles behov som representantene i styringsgruppen har definert. Når det gjelder vurdering knyttet til gjennomførbarhet er Alternativ 2 dimensjonerende, slik at alternativet vurderes å ha lav til moderat gjennomførbarhet da det er kjent at det er visse teknologiske hindringer for at tjenestene skal kunne leveres i alle IKT-systemer i kommunal sektor.

En kostnadsmessig vurdering må gjøres i sammenheng med kapasitetsvurderinger rundt bemanning og beredskap. Både mangfoldet i teknologiske løsninger og omfanget av støtten vil dimensjonere behovet for bemanning. Usikkerhet knyttet til dette gjør kostnadsoverslaget usikkert. Om en tar i betraktning hvordan øvrige håndteringsmiljøer har etablert tilsvarende tjenester, ansees en minimumsbemanning på 10–12 personer for å kunne levere tilfredsstillende på alle tjenesteområdene. Et nøkternt kostnadsoverslag viser en årlig kostnad pålydende 16 MNOK som skal dekke lønnsutgifter, driftsutgifter og utgifter til infrastruktur og lokaler. Kostnadsoverslaget er usikkert, og vil kunne påvirkes av geografisk betingede lønnsutgifter og ambisjoner knyttet til bemanning og beredskap. Kostnader knyttet til lisenser og teknisk utstyr representerer også en usikkerhet.

27 *Riksrevisjonen*. Riksrevisjonens undersøkelse av digitalisering av kommunale tjenester. Riksrevisjonen. Dokument 3:6 (2015–2016).

28 Eksempelvis MilCERT, NorCERT og HelseCERT

Oppsummert:
- Fokus på å levere innen alle tjenesteområdene
- Møter alle felles behov i kommunal sektor
- Lav til moderat gjennomførbarhet
- Kostnadsoverslag på 16 MNOK per år.

5.2 Kapasitet

Representantene i styringsgruppen har påpekt at hendelser kan oppstå til alle døgnets tider, og at en forutsetning for en døgnåpen digital forvaltning er at hendelser blir håndtert så raskt som mulig. Økt bemanning og beredskap medfører imidlertid økte kostnader, og det kan være utfordrende å vite på forhånd hvor stort behovet vil være. Kommunal sektor må ta stilling til om bemanning og beredskap skal dimensjoneres etter det daglige behovet for CSIRT tjenester, eller om det skal dimensjoneres etter de mest alvorlige hendelsene som kan inntreffe.

Behov for bemanning og beredskap ut over alminnelig arbeidstid kan realiseres på ulike måter. Ett alternativ er å inngå en avtale om beredskapsvakt med de ansatte. Slike avtaler kan inneholde ulike grader av tilgjengelighet for personellet, og vil komme med en kostnad i form av økonomisk kompensasjon til de ansatte.

Et annet alternativ er å fremforhandle en avtale om skiftarbeid, enten for hele eller deler av døgnet. En kan ikke på forhånd si hva kostnaden vil være for en slik avtale før den er fremforhandlet, men det finnes tilsvarende ordninger som kan fungere som en pekepinn for de eventuelle kostnadene. Eksempelvis har Forsvarets Avdeling for beskyttelse av kritisk infrastruktur («MilCERT») en døgnbemannet kapasitet bestående av 6-9 personer. Dette blir av dem ansett for å være et minimum av det må ha for å kunne levere en stabil tjeneste gjennom hele året, herunder ferieavvikling og høytider. Det ansees imidlertid ikke som tilstrekkelig robust ved langvarig sykefravær eller dersom større hendelser oppstår. Forsvaret anser det heller ikke som ønskelig med en så lav bemanning av HMS-hensyn, da personellet må arbeide alene på kveld og natt over lengre perioder.

Andre håndteringsenheter, som FinansCERT, KraftCERT og HelseCERT, har ikke døgnbemanning for sine tjenester.

Slike vakt- og skiftordninger kommer gjerne i tillegg til den ordinære bemanningen på dagtid, og medfører derfor i stor grad en tilleggskostnad. Hvor stor kostnaden blir vil imidlertid ikke kunne fastsettes før arbeidstidsavtalene er fremforhandlet.

5.3 Organisering

Det eksisterer ulike modeller for organisering av et KommuneCSIRT. Organiseringsmodellen må gi tydelighet i forhold til eierstruktur, styringslinjer og mandat for et KommuneCSIRT. Noen håndteringsmiljøer har kun en rådgivende rolle, mens andre er gitt et mandat til å kunne ta beslutninger og å pålegge skadereduserende tiltak i de innledende fasene av håndteringen av en hendelse. Eierstruktur og styringslinjer vil også kunne gi føringer for hvilke oppgaver håndteringsenheten skal ha, og hvordan den skal være oppbygget for å løse oppdraget.

For kommunal sektor kan det tidligere omtalte rammeverket for håndteringsenheter i den nasjonale CERT-strukturen bli en utfordring for autonomiteten til den enkelte kommune og fylkeskommune dersom det legges til grunn at det skal være styringslinjer fra et departement til håndteringsenheten. Denne utfordringen må adresseres ved valg av organisering, og det bør avklares nærmere hva som menes med departementstilknytning når rammeverket fra justissektoren for håndteringsmiljøer som skal inngå i den nasjonale CERT-strukturen foreligger.

5.3.1 Om modeller for interkommunalt samarbeid

Kommunesektoren har en lang tradisjon med ulike former for interkommunalt samarbeid. Ikke minst i IKT-sektoren er det i dag et utstrakt samarbeid mellom mange kommuner og fylkeskommuner. Samarbeidet er etablert i flere varianter hvor graden av samarbeid og deltakerkommunenes involvering er innrettet på ulike måter.
KS advokatene har derfor utarbeidet en rapport[29] hvor de går nærmere inn på noen sentrale rettslige spørsmål som oppstår når kommuner samarbeider på IKT-området.

Rapporten omhandler modeller som har en organisatorisk overbygning. Det gjelder blant annet modeller for interkommunalt samarbeid som er regulert i lov og som bare kan ha kommuner som deltakere, herunder interkommunalt selskap (IKS), felles styre etter kommuneloven § 27 og vertskommunesamarbeid etter kommunelovens kapitel 5A.

5.3.2 Om modeller benyttet av private rettssubjekter

Når det gjelder organisering og drift av administrative støttetjenester har kommunene i utgangspunktet samme frihet til å organisere driften av virksomheten som private rettssubjekter. Ut fra hva som anses hensiktsmessig, kan i utgangspunktet derfor også ansvarlig selskap (ANS), eventuelt med delt ansvar (DA), kommandittselskap, aksjeselskap, allmennaksjeselskap, forening og samvirkeforetak (SF) være mulige modeller for etablering av et KommuneCSIRT.

Begrensningen ligger i at fordi kommunene ikke er private rettssubjekter, men offentlige organ, gjelder det særlige regler som begrenser denne handlefriheten. Særlig representerer regelverket for offentlige anskaffelser en slik begrensning som må vurderes konkret i det enkelte tilfelle.

Hvilken modell som skal legges til grunn ved etablering av et KommuneCSIRT, må avklares gjennom en konkret vurdering i etableringsfasen.

5.3.3 Om modeller for utvidelse av eksisterende håndteringsmiljø

Flere av representantene i styringsgruppen har påpekt at det vil være ressursbesparende å utvide et eksisterende håndteringsmiljø, og det er spesielt pekt på NorCERT og HelseCERT som mulige kandidater.

NSM NorCERT som er den operative delen av Nasjonal sikkerhetsmyndighet (NSM) er Norges nasjonale CERT og cybersenter. NSM er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. NSM etatsstyres av Forsvarsdepartementet og har en faglinje til Justis- og Beredskapsdepartementet.

HelseCERT er en del av Norsk Helsenett, et statsforetak som eies av Helse- og Omsorgsdepartementet.

Felles for både NorCERT og HelseCERT er at de med dagens eier- og styringsstruktur ikke har et mandat eller oppdrag om å støtte kommunal sektor med håndtering av IKT-hendelser. En eventuell utvidelse av disse enhetene krever et større arbeid som blant annet vil omfatte ny styringsdialog og eventuelt endringer i relevante lover/forskrifter.

29 *KS Advokatene*. Interkommunalt samarbeid om IKT – rettslige rammer for organisering. 2015. http://www.ks.no/contentassets/865fecf1adb24126b83ab225991493c6/interkommunalt-samarbeid-om-ikt---rettslige-rammer-for-organisering.pdf

5.4 Finansiering

Ved etablering av et KommuneCSIRT bør en både tenke på stabilitet i selve etableringsfasen, og en finansieringsmodell i driftsfasen som muliggjør at KommuneCSIRT kan vokse og endre seg i takt med behovet i sektoren over tid.

En finansieringsmodell kan være sammensatt av flere av de følgende elementene, og den kan også endre seg når man går fra en etableringsfase til en driftsfase. Representantene i styringsgruppen har nevnt følgende muligheter for finansiering:

5.4.1 Per Capita finansiering

Dette er en finansieringsmodell som fordeler den økonomiske byrden basert på innbyggerantallet i kommunene. Ved å bidra med et lite beløp per innbygger, vil kommunene kunne finansiere både etablering og drift av et KommuneCSIRT. De store kommunene har imidlertid påpekt at belastningen for dem blir stor og at det derfor kan være en lite attraktiv løsning for dem.

5.4.2 Finansiering per bruk av tjenester

En annen modell kan være å prisfastsette de ulike tjenestene som et KommuneCSIRT tilbyr. Når en kommune benytter seg av tjenester, faktureres de så for dette. Modellen er trolig usikker og ustabil ettersom man i dag ikke har oversikt over hvilke tjenester kommunene vil etterspørre på eget initiativ, eller i hvor stort omfang de vil bli etterspurt.

5.4.3 Statlig finansiering

Flere av representantene i styringsgruppen har pekt på statens rolle i å sørge for at kommunal sektor har et håndteringsmiljø for IKT-hendelser. En åpenbar mulighet er da at staten går inn med finansiering av et KommuneCSIRT, så lenge dette kommer alle kommuner til gode.

En kan tenke seg ulike modeller for statlig finansiering. En mulig modell er at staten går inn med et etableringsbidrag som sikrer finansiering i etableringsfasen. En annen modell er at etableringen dekkes av sektoren selv og at staten går inn med driftstilskudd, fortrinnsvis over statsbudsjettet. En tredje modell er at staten tar fullt ansvar for både etablering og drift.

5.4.4 Fase-inndelt finansiering

En mulig løsning er å tenke seg en finansieringsmodell bestående av ulike løsninger for etableringsfasen og driftsfasen. I den hensikt å fremskynde etablering av et KommuneCSIRT kan en se for seg at enkeltkommuner og fylkeskommuner påtar seg det finansielle ansvaret for etableringsfasen, samtidig som det arbeides med å finne en løsning for finansiering av den påfølgende driftsfasen.

5.5 Lokalisering

Riktig lokalisering kan potensielt forsterke effekten av de tjenester som et KommuneCSIRT leverer. Lokalisering kan komme som en følge av organiseringen, men en kan også velge å samlokalisere KommuneCSIRT med andre fag- og kompetansemiljøer for å skape synergier.

Lokalisering kan også ha betydning for tilgang på arbeidskraft. Det må vurderes om situasjonen i arbeidsmarkedet vil kunne få betydning for rekruttering og å beholde personellet. Nærhet til utdanningsinstitusjoner bør vurderes med tanke på tilgang til arbeidskraft.

Et KommuneCSIRT kan samlokaliseres med et eksisterende håndteringsmiljø for å skape synergier ved å dra på deres kompetanse i en oppstartsfase. Det er spesielt to miljøer som har utpekt

seg i dette arbeidet. NorCERT, som er etablert på Bryn i Oslo, og HelseCERT som er etablert i Trondheim. Det må utarbeides en gjennomføringsanalyse før en kan slå fast om det er et reelt alternativ å samlokalisere et KommuneCSIRT ved et av disse, og hvor stor synergien eventuelt er. I forkant av dette bør det inngås en intensjonsavklaring med de aktuelle håndteringsmiljøene for å avklare om det er ønskelig med en slik samlokalisering.

Et annet alternativ er å samlokalisere et KommuneCSIRT med eksisterende fag- og forskningsmiljøer, for å skape synergier ved å sørge for tilgang på oppdatert fagkunnskap over tid. Det er flere mulige fag- og forskningsmiljøer som er aktuelle. Sintef i Trondheim, Simula i Bergen og NTNU Gjøvik/CCIS har alle fagkompetanse som kan være nyttig for et KommuneCSIRT. Det må også her utarbeides en gjennomføringsanalyse før en kan slå fast om det er et reelt alternativ å samlokalisere et KommuneCSIRT ved et av disse, og hvor stor synergien eventuelt er. Også her bør det inngås en intensjonsavklaring med de aktuelle fagmiljøene i forkant for å avklare om det er ønskelig med en slik samlokalisering.

6 Anbefaling

6.1 Innledning

Basert på alle fakta som har fremkommet i arbeidet med utredningen, og basert på egen erfaring med kompetansemiljøer for håndtering av IKT-hendelser i privat og offentlig sektor, beskriver NorSIS sin anbefaling til kommunal sektor.

NorSIS tilkjennegir i dette kapitel sin begrunnelse for anbefalt alternativ, og presenterer sitt syn på en mulig etableringsprosess, herunder organisering, finansiering, kost/nytte vurdering og en mulig struktur for et KommuneCSIRT..

6.2 Anbefalt alternativ

Representantene fra kommunal sektor har i dette prosjektet bidratt på en svært god måte til å fastslå hva som er det felles behovet i sektoren. Behovet har et relativt bredt omfang, og inkluderer både et overordnet fokus på situasjonsforståelse, koordinering og informasjonsdeling, og et teknisk fokus på avdekking av sårbarheter i tekniske løsninger og håndtering av hendelser.

Dersom en ser på andre håndteringsenheter vises flere muligheter for å velge ulike tilnærminger til oppbygging av et responssenter. KraftCERT og FinansCERT er i hovedsak fokusert mot det overordnede, mens HelseCERT og NorCERT også har noe fokus mot det tekniske.

I denne utredningen trekker Alternativ 1 og Alternativ 2 opp to ulike tilnærminger. Det førstnevnte alternativet har fokus på det overordnede, mens det sistnevnte har fokus på det teknologiske. Ingen av alternativene dekker den fulle bredden i det felles behovet i sektoren, og det vil av den grunn ikke være ønskelig å anbefale at kommunal sektor avgrenser seg til et av disse to alternativene.

NorSIS anbefaler derfor at kommunal sektor velger å etablere en håndteringsenhet som skal ivareta tjenesteområdene som er beskrevet i Alternativ 3. NorSIS anbefaler videre at kommunal sektor velger en etableringsprosess som beskrevet i pkt. 6.3.

6.3 Om etableringsprosessen

Å etablere en effektfull håndteringsenhet er en omstendelig prosess som innebærer en utvikling innen områdene Prosess, Teknologi og Organisasjon. Det kan på forhånd være utfordrende å kartlegge og beskrive alle forhold fordi utvikling, endring og modning er en forutsetning for å nå ønsket ambisjon.

NorSIS anbefaler derfor at kommunal sektor ser på etableringen av et KommuneCSIRT som en prosess der det planlegges en rekkefølge for innføring av de ulike tjenesteområdene. Dette betyr at det må besluttes om Alternativ 1 eller Alternativ 2 bør etableres først. Selv om sluttresultatet er det samme, bør det utarbeides en etableringsplan som minimerer risiko samtidig som det gis effekt ut til den enkelte kommune og fylkeskommune i hele landet.

NorSIS mener at det er betydelig større risiko knyttet til Alternativ 2 enn til Alternativ 1. Det foreligger ikke en helhetlig oversikt over hvilke teknologiske infrastrukturer og systemer som er i bruk i kommunal sektor i dag. Det foreligger heller ikke en oversikt over hvilke behov hver av kommunene har for støtte til håndtering og beskyttelse eller hvilke kompetansekrav og teknologiske sikkerhetsløsninger som et KommuneCSIRT må ha for å kunne gi støtte. Dette er en oversikt som kommunal sektor bør bygge opp, og et KommuneCSIRT kan gis et slikt oppdrag. Imidlertid mener NorSIS at en forutsetning for å etablere en slik oversikt er at det allerede foreligger en viss helhetlig oversikt over utfordringene i sektoren i tillegg til en oversikt over «IKT-landskapet» i den enkelte kommune.

Det presiseres at Alternativ 1 beskriver en minimumsløsning, og en må påregne at denne må utvikles videre. En kan se på Alternativ 1 som en forutsetning for å utvikle kapabilitetene i retning av Alternativ 2. Når disse er ferdig utviklet vil kommunal sektor i realiteten ha en kapabilitet som beskrevet for Alternativ 3, og som dekker alle de felles behovene som er kartlagt.

NorSIS anbefaler derfor at tjenesteområdene som beskrevet i Alternativ 1 etableres først, og at tjenesteområdene som beskrevet i Alternativ 2 deretter gradvis innføres etter en kost/nytte vurdering.

6.4 Om organisering

Ved valg av organiseringsform ønsker NorSIS å belyse noen problemområder.

Hendelser i det digitale rom har ofte en tids-komponent som kan være kritisk. Ulike typer dataangrep, for eksempel informasjonstyveri, kan kreve en hurtig respons for å begrense skadevirkningene. Det er derfor vanlig at håndteringsenhetene avklarer hvilken beslutningsmyndighet de har til å pålegge strakstiltak ved slike hendelser. Autonomiteten i kommunal sektor utfordrer denne tankegangen fordi det trolig ikke er naturlig at et KommuneCSIRT skal ha myndighet til å pålegge enkeltkommuner å iverksette tiltak. NorSIS mener imidlertid at dette spørsmålet må avklares ved etablering av et KommuneCSIRT.

Valgt organiseringsform må sørge for at et KommuneCSIRT inngår som en del av den nasjonale CERT-strukturen. Dette er nødvendig for en effektiv informasjonsflyt med de øvrige sektorvise håndteringsenhetene og med NorCERT. NSM har i forbindelse med sitt nye rammeverk for håndteringsmiljøer uttalt at de forutsetter at disse utpekes av sine respektive departement. Det er imidlertid ikke klart hva som menes med en slik utpeking, eller hva det innebærer for valgt organiseringsform. Dette må avklares før KommuneCSIRT etableres.

6.5 Om finansiering

Et KommuneCSIRT må gis solide og forutsigbare rammer, herunder en forutsigbar finansiering. Samtidig viser behovsbeskrivelsen i denne utredningen at kommunal sektor trenger en håndteringskapasitet som kan bidra til å redusere digital risiko i den enkelte kommune og fylkeskommune. Noen finansieringsmodeller vil ta tid å etablere, og NorSIS mener at risikobildet tilsier at det haster med å starte etableringen av et KommuneCSIRT.

Kommunal sektor bør derfor vurdere om det er mulig å sikre en finansiering for en etableringsfase som kan iverksettes på kort sikt, samtidig som det arbeides med å sikre en stabil langsiktig finansiering.

6.6 Om nytteverdi

Det forutsettes at etablering av et KommuneCSIRT vil bidra til bedre forebygging og håndtering av IKT-hendelser i kommunal sektor, og at skadefølgene av slike hendelser dermed reduseres. Det er flere faktorer som avgjør nytteverdien av et KommuneCSIRT.

Hvilke tjenesteområder som etableres vil gi innvirkning på nytteverdien. Denne utredningen har kartlagt hvilke behov kommunal sektor har, og NorSIS legger til grunn at nytteverdien for et KommuneCSIRT øker jo flere behov som møtes. Representantene i styringsgruppen har i tillegg vektet behovene innbyrdes, slik at vi må konkludere med at det å etablere et felles situasjonsbilde og en effektiv informasjonsdeling i sektoren vil ha størst nytteverdi.

En måte å betrakte nytteverdi er å evaluere om etableringen av et KommuneCSIRT har hatt noen effekt for de kommunale tjenestene som understøttes av IKT. Det bør derfor planlegges med en evaluering i forkant av etableringen slik at effekten kan anslås. Evalueringen bør omfatte kommunens syn på egen evne til å beskytte tjenestene mot digitale trusler, den faktiske endringen i de kommunale tjenestenes sikkerhet (tilgjengelighet, integritet, konfidensialitet). Befolkningens trygghet for at kommunene behandler og beskytter informasjon om dem kan også være en del av dette bildet.

Etablering av et KommuneCSIRT kan også gi økonomisk innsparing ved at tjenester som tidligere ble kjøpt av den enkelte kommune, kan inngå i en større avtale som KommuneCSIRT forvalter. Slike stordriftsfordeler kan blant annet omfatte kjøp av tjenester for sikkerhetsmessig overvåking, sårbarhets- og penetrasjonstester, analyse av digitale elementer, sikker sletting mm.

IKT-hendelser kan også medføre økonomiske følger for kommunene. Mørketallsundersøkelsen[30] 2014 gir et overslag for hva datakriminalitet koster det norske samfunnet, og blant annet vises det til at Center for Strategic Studies har estimert de norske tapene til 0,64% av BNP, altså 19 mrd. NOK i 2014. Undersøkelsen oppgir ikke hva de økonomiske tapene innebærer for kommunal sektor, men NorSIS legger til grunn at IKT-hendelser i kommuner og fylkeskommuner medfører både direkte og indirekte økonomiske tap. Kartlegging av økonomiske tap, både direkte og indirekte, bør inngå i evalueringen som er nevnt over.

6.7 Om valg av rammeverk

I denne utredningen har NorSIS valgt et rammeverk fra FIRST som beskriver hvilke tjenesteområder et CSIRT kan ha. FIRST-rammeverket forteller *hva* et CSIRT skal gjøre, men ikke *hvordan* tjenestene kan bygges opp. NorSIS har derfor evaluert aktuelle rammeverk som kan brukes ved etableringen av et CSIRT, altså et som har fokus på de interne etableringsprosessene for de valgte tjenesteområdene.

6.7.1 Rammeverk for etablering

NorSIS er kjent med at det finnes flere ulike rammeverk en kan benytte seg av. De mest sentrale rammeverkene er omtalt i Vedlegg 2. For noen organisasjoner kan kjennskap til ett rammeverk være avgjørende, mens det for andre kan være av vesentlig betydning at rammeverket harmonerer med øvrige rammeverk innenfor deres styringssystem for informasjonssikkerhet.

30 *Næringslivets Sikkerhetsråd.* Mørketallsundersøkelsen 2014. https://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf

NorSIS har i denne utredningen avdekket at flere av representantene vi har snakket med viser til at kommunene har et forhold til ISO/IEC 27001 og 27002, som beskriver et styringssystem for informasjonssikkerhet. Selv om flere også viser til at det eksisterer andre styrende dokumenter, er det vår oppfatning at nevnte ISO-rammeverk legges til grunn for sikkerhetsstyringen i de fleste kommuner. ISO/IEC 27035 *Principles of incident management. og Guidelines to plan and prepare for incident response* ble utgitt i november 2016, og beskriver hvordan en håndteringsenhet kan etableres, og hvordan en kan planlegge for og utøve aktiviteter innenfor de tjenesteområdene som denne utredningen beskriver. Rammeverket inngår i det mer overordnede rammeverket en finner i ISO/IEC 27001 og 27002, slik at en kan forvente at begrepsbruken er avstemt og at de beskrevne prosesser passer sammen i et virksomhetsperspektiv.

ISO/IEC 27035 beskriver prosesser som kan legges til grunn for alle tjenesteområdene som er beskrevet for Alternativ 3. NorSIS anbefaler derfor at ISO/IEC 27035 legges til grunn ved etableringen av et KommuneCSIRT.

6.7.2 Rammeverk for situasjonsbilde

Ved etablering av et felles situasjonsbilde mener NorSIS at det er avgjørende at riktig informasjon samles inn, og at denne bearbeides og presenteres på en måte som gir økt forståelse i den enkelte kommune og fylkeskommune. Situasjonsforståelse kan beskrives i tre nivåer:

1. Å oppfatte at en hendelse har funnet sted i tid og rom
2. Å forstå hva det betyr for virksomheten at hendelsen har funnet sted
3. Å forutse hva hendelsen vil kunne føre til

Det er vanlig at det i virksomheter er ulike syn på hvilken informasjon som bør inngå i et situasjonsbilde. Personell som er den del av de operative sikkerhetsprosessene ønsker seg gjerne detaljert informasjon om tekniske hendelser i IKT-infrastrukturen, mens beslutningstakere gjerne ønsker seg mer overordnet informasjon om konsekvensene for virksomheten.

NorSIS anbefaler at kommunal sektor analyserer hvilken informasjons som er nødvendig for å ta gode beslutninger om både forebygging og tiltak i hendelseshåndtering. Dette bør resultere i et omforent informasjonsbehov som legges til grunn for etableringen av situasjonsbildet. En mulig tilnærming er å legge til grunn de dataklassene som er beskrevet i artikkelen *Operational Data Classes for Establishing Situational Awareness in Cyberspace*[31] som ble presentert på International Conference on Cyber Conflict i Tallin i 2014. Dette rammeverket kan integreres i det overordnede rammeverket ISO/IEC 27035.

6.8 Om mulig struktur for et KommuneCSIRT

Det finnes ulike måter å strukturere et CSIRT, der faktorer som størrelse og valgt organiseringsform spiller inn. Dersom denne anbefalingen tas til følge, vil tjenesteområdene i Alternativ 1 etableres først. Dette innebærer videre at KommuneCSIRT i oppstarten er en liten organisasjon som både leverer innen tjenesteområdene samtidig som den videre utviklingen av enheten planlegges og iverksettes.

NorSIS anser en bemanning på 4 personer å være et minimum av det et KommuneCSIRT må ha av bemanning for å kunne utføre ovennevnte oppgaver i en oppstartsfase. Dette innebærer at et KommuneCSIRT har en leder, og tre ansatte som har som sine oppgaver å levere på tjenesteområdene 4 *Situasjonsbilde,* 5 *Kommunikasjon* og 6 *Kapabilitetsutvikling.*

31 *Operational Data Classes for Establishing Situational Awareness in Cyberspace.* 2014 6th International Conference on Cyber Conflict. (Judson Dressler. William Moody. Calvert L. Bowen, III. Jason Koepke)

ISO/IEC 27035 Del 2 Kapitel 7 beskriver nærmere hvilke kompetansekrav en kan stille til ulike roller i et CSIRT.

6.9 Oppsummering

NorSIS anbefaler at kommunal sektor beslutter å etablere et KommuneCSIRT som beskrevet for Alternativ 3, og at det i etableringsfasen legges vekt på tjenesteområdene som er beskrevet for Alternativ 1.

Det bør vurderes om det kan fremskaffes finansieringsløsninger som sikrer en hurtig igangsettelse, samtidig som det arbeides med en langsiktig og forutsigbar finansiering for responssenteret.

Vedlegg 1 – Prinsipper for samfunnssikkerhet

Ansvarsprinsippet betyr at den myndighet, virksomhet eller etat, som til daglig har ansvaret for et område, også har ansvaret for nødvendige beredskapsforberedelser og for den utøvende tjeneste ved kriser og katastrofer. Dette ansvaret omfatter også å planlegge hvordan funksjoner innenfor eget ansvarsområde skal kunne opprettholdes og videreføres dersom det inntreffer en ekstraordinær hendelse.

Likhetsprinsippet betyr at den organisasjon man opererer med under kriser skal være mest mulig lik den organisasjon man har til daglig. Likhetsprinsippet er en utdyping av ansvarsprinsippet, nemlig en understreking av at ansvarsforholdene internt i virksomheter/organisasjoner og mellom virksomheter/organisasjoner ikke skal endres i forbindelse med krisehåndtering.

Nærhetsprinsippet innebærer at kriser organisatorisk skal håndteres på et lavest mulig nivå. Den som har størst nærhet til krisen, vil vanligvis være den som har best forutsetninger for å forstå situasjonen og dermed er best egnet til å håndtere den. Nærhetsprinsippet må også sees i sammenheng med ansvarsprinsippet. En krise innenfor en kommunes eller annen virksomhets ansvarsområde er i utgangspunktet kommunens eller virksomhetens ansvar å håndtere. Nærhetsprinsippet gjelder ikke ved sikkerhetspolitiske kriser.

Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. For å sikre best mulig utnyttelse av ressurser på tvers av sektorer, er det behov for samarbeid på tvers av ansvarsområder. Samvirkeprinsippet innebærer ikke noen endringer i de grunnleggende ansvarsforholdene, men understreker behovet for at alle virksomheter og nivåer har et aktivt og bevisst forhold til gjensidige avhengigheter og hvilke aktører det vil være nødvendig å samhandle med, både når det gjelder forebyggende arbeid og i beredskapssituasjoner.

Vedlegg 2 – Oversikt over aktuelle standarder og veiledninger for etablering av håndteringsenheter (IRT, CERT, CSIRT og tilsvarende)

Det finnes en rekke standarder og veiledninger for hvordan en kan gå frem når en skal etablere en enhet som skal håndtere IKT-hendelser. Flere av disse har relevans for dette prosjektet. Det er ikke utpekt en standard i prosjektets oppdragsbeskrivelse, men RFC-2350 (Expectations for Computer Security Incident Response) er nevnt som en mulig metode i prosjektmandatet.

Dette vedlegget gir en kort beskrivelse av de ulike standardene og veiledningene.

RFC-2350 Expectations for Computer Security Incident Response

Publisert: IETF, 1998
https://www.ietf.org/rfc/rfc2350.txt

Dokumentet er publisert som en «Best current practice», og beskriver overordnet et CSIRT's struktur, prosesser og tjenester. Dokumentet er tydelig på at det ikke er en autoritativ beskrivelse, og at enhver organisasjon må tilpasse beskrivelsene til sine behov. Seksjon 3.5 beskriver mulige CSIRT tjenester, men er ikke eksplisitt på om de skal forstås i en overordnet eller teknisk kontekst. RFC-2350 kan derfor ha relevans ved etablering av et KommuneCSIRT. Det er forøvrig verdt å merke seg at dokumentet er gammelt og at det derfor ikke omtaler prosesser som NorSIS mener er helt avgjørende for en moderne håndteringsenhet. Det viktigste vi peker på her er integreringen av et etterretningsbasert forsvar mot digitale trusler, spesielt i en sikkerhetspolitisk situasjon der det er sannsynlig at fremmede nasjoner vil forsøke å gjennomføre påvirkningsoperasjoner og sabotasje mot tjenester som er kritiske for befolkningen.

Incident Management: CSIRT Development

Publisert: Software Engineering Institute (SEI/CMU), 2017 (Web)
http://www.cert.org/incident-management/csirt-development/index.cfm
http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
SEI har publisert en serie guidelines for etablering og drift av et CSIRT. I tillegg er det publisert case studies hvor en kan ta del i andre organisasjoners lærdom i tilsvarende prosesser.
Publikasjonene er kategorisert som følger:

- Creating a CSIRT: Getting started
- Operating and Staffing your CSIRT
- Developing Incident Handling Cost Models
- Collecting Evidence/Forensics
- Incident Management and General CSIRT Publications.

Under hver av disse kategoriene er det publisert en stor mengde dokumenter som går i dybden på ulike områder. Publikasjonene er samlet sett relevant for en etablering av et KommuneCSIRT. Publikasjonene fremstår som oppdatert i forhold til dagens trusselbilde, og de inneholder vesentlig mer informasjon enn det RFC-2350 gjør.

CSIRT Setting up guide

Publisert: Enisa, 2006
https://www.enisa.europa.eu/publications/csirt-setting-up-guide
Dokumentet er en steg-for-steg veiledning for etablering av et CSIRT. Det beskriver organi-

satoriske forhold, tjenestekatalog, kompetansekrav, samarbeidsprosesser m.m. Dokumentet fremstår som helhetlig og egnet for etableringen av et KommuneCSIRT. Dokumentet har en rekke eksempler, og inneholder også et forslag til prosjektplan for etableringen.

Computer Security Incident Handling Guide

Publisert: NIST, 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
Dokumentet beskriver organisering av et CSIRT, og hvilke prosesser og tjenester et CSIRT bør ha. Dokumentet fremstår som helhetlig og egnet for etableringen av et KommuneCSIRT.

Incident Handler's Handbook

Publisert: SANS Institute, 2011
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
Dokumentet har fokus på prosessen med å sette et CSIRT-team i stand til å håndtere hendelser, og ikke på å etablere en slik kapabilitet i en organisasjon. Dokumentet fremstår ikke som helhetlig, og vil ha størst nytte for håndtering av hendelser i et KommuneCSIRT.

ISO/IEC 27035

Publisert: ISO, November 2016
http://www.iso27001security.com/html/27035.html
IOC/IEC 27035 er foreløpig delt inn i to deler: Del 1 har tittelen Principles of incident management. Del 2 har tittelen Guidelines to plan and prepare for incident response. NorSIS mener at rammeverket har stor relevans for etableringen av et KommuneCSIRT da den inneholder en beskrivelse av etablering av en håndteringsenhet, samt flere andre relevante tema. I tillegg er rammeverket avstemt med øvrige ISO-rammeverk, som f.eks. ISO/IEC 27001 og 27002 som omhandler styringssystem for informasjonssikkerhet.

Det er også igangsatt et arbeide med en Del 3 som foreløpig har tittelen *Guidelines for incident response operations*. Det er ikke angitt når denne vil utgis. Vi antar at også dette dokumentet vil være til nytte for et KommuneCSIRT.

NSMs kvalitetsordning for hendelseshåndtering

Publisert: NSM, 2016
https://nsm.stat.no/globalassets/dokumenter/soknads-og-kravdokument-for-publisering.pdf
Dokumentet beskriver søknadsprosessen for håndteringsenheter som ønsker å inngå i Nasjonal sikkerhetsmyndighet sin kvalitetsordning for håndteringsenheter. Seksjon 3.5 beskriver de krav som NSM har fastsatt for enhetene som ønsker å inngå i kvalitetsordningen. Kravene er relevante for prosjektet uavhengig om det er tenkt å søke om å inngå i ordningen, fordi kravene er basert på både best practice og de eksisterende samarbeidsprosessene med NSM/NorCERT. Dokumentet er relevant for etableringen av et KommuneCSIRT.

FIRST Best Practice Guide Library

Publisert: FIRST, Ulike publiseringsdatoer
FIRST har samlet et sett veiledninger og guider som er nyttig for etablering og drift av håndteringsenheter. Følgende kan være relevante for prosjektet:

- CERT-in-a-box (National Cyber Security Centre of The Netherlands beskriver sine erfaringer med etablering av deres GOVCERT.NL)
- CSIRT Case Classification (Example for enterprise CSIRT, CISCO)

- CSIRT Setting up Guide (Enisa, tidligere beskrevet)
- APWG and the eCrime Exchange: A Member Network Providing Collaborative Threat Data Sharing
- How RIPE NCC Tools and Data Sets Can Help with Online Investigations
- Incident Response Dealing with the Whole Country
- OPSEC. Against APT's reconnaissance phase
- TheHive: A Scalable, Open Source and Free Incident Platform

Deler av biblioteket er relevant for etableringen av et KommuneCSIRT.