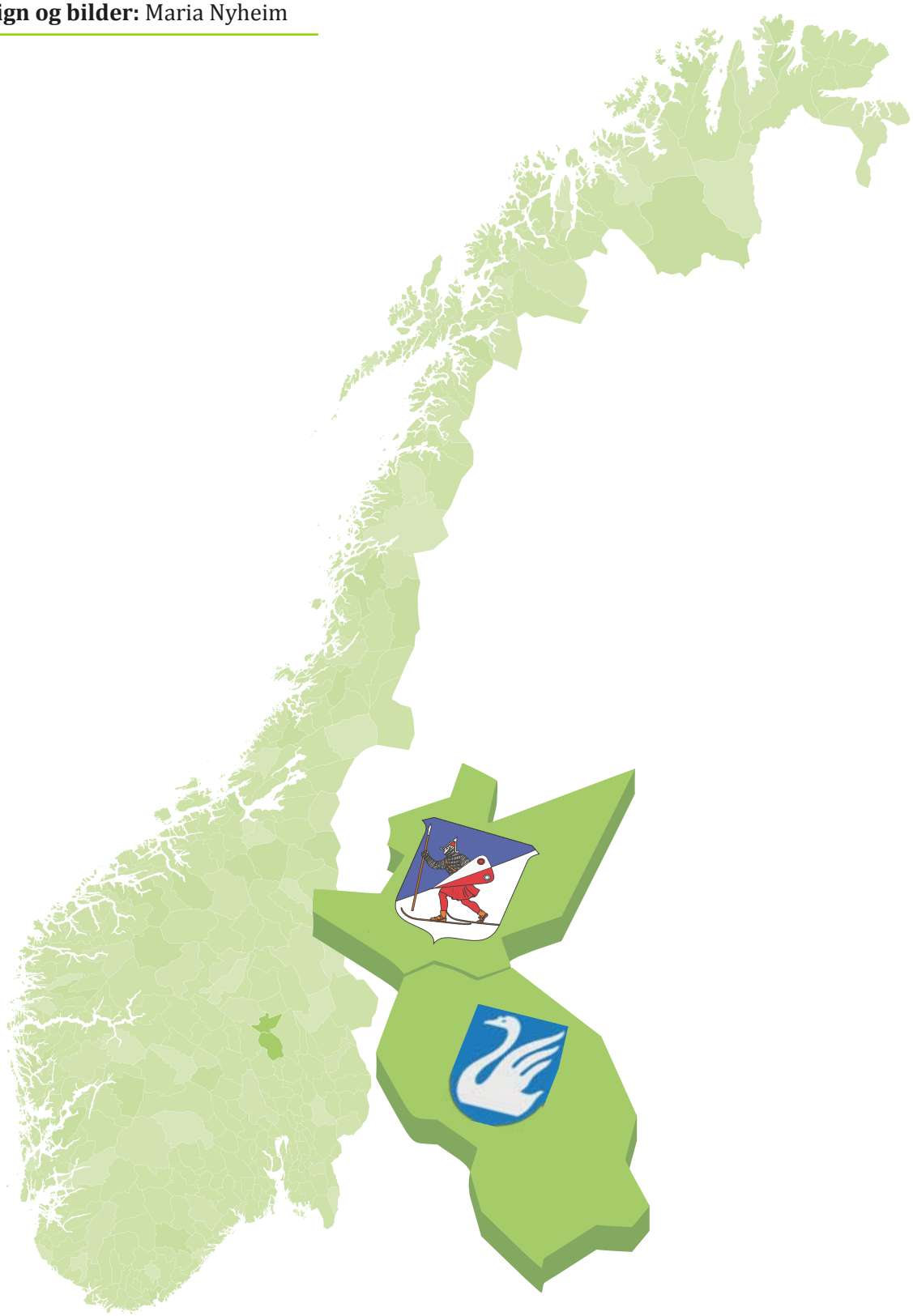
NorSIS
Norsk senter for informasjonssikring

# Kommune CERT

–utredning av behov og muligheter

**Design og bilder:** Maria Nyheim



# Innhold

# SAMMENDRAG

Digitaliseringen av samfunnet skaper forutsetninger for innovasjon, verdiskaping og kvalitet både i offentlige og privat sektor. 95% av alle husstander er på nett og Norge er det femte mest digitaliserte landet i verden. Myndighetene har derfor uttrykt en klar målsetting om at digitale tjenester skal være et førstevalg for norske innbyggere.

Kommunesektoren er enhver regjerings redskap for å realisere morgendagens velferdssamfunn. e-kommunekartleggingen viser derimot at kommunene har en vei å gå når det gjelder full utnyttelse av potensiale som ligger i digitale tjenester. På den annen side uttrykker kommunene stor interesse og vilje til å utnytte teknologien for å bli mer tilgjengelig, effektive og innbyggerrettet. Digitaliseringen har derfor kommet langt innen mange av kommunenes ansvarsområder.

Omfanget av personopplysninger og annen sensitiv informasjon kommunene behandler og utveksler elektronisk, er allerede svært stort. I tillegg styres stadig flere kommunale tjenester digitalt. Datakriminalitet, sabotasje av og hærverk på kommunale IKT-systemer vil derfor kunne få store samfunnsmessige konsekvenser. Samfunnet må derfor være forberedt på alvorlige IKT-hendelser. Det synes imidlertid uhensiktsmessig at alle landets kommuner skal utvikle og etablere kompetanse og benytte ressurser på nivå med en CERT-funksjon for å møte disse utfordringene.

NorSIS har i samarbeid med Lillehammer og Gjøvik kommune utredet behovet for en egen enhet for å forebygge og håndtere IKT-hendelser i kommunene. Etter intervjuer med et utvalg kommuner og interkommunale selskaper, ildsjeler og organisasjoner, nasjonale og internasjonale CERT-miljøer, har vi kommet frem til følgende anbefaling;

Gevinstene av digitalisering av kommunene er stor. Risiko forbundet med datakriminalitet og andre IKT-hendelser er derimot betydelig. Tilliten til digitaliseringen er i betydelig grad avhengig av evnen til å forhindre at IKT-hendelser får kritiske konsekvenser for kommunale tjenester. Håndtering av IKT-hendelser krever betydelig innsikt i kommunal virksomhet, avviks- og krisehåndtering. Vi anbefaler derfor at det etableres et eget CSIRT for kommunene.

Kommune CSIRT bør etableres som et interkommunalt selskap, finansiert delvis med sentralt tildelte øremerkede midler og delvis med medlemsavgift. Selskapet bør bemannes og organiseres for å ivareta ledelse, rådgivning, analyse- og informasjonsvirksomhet. Tekniske funksjoner og overvåking av infrastrukturen anbefales anskaffet i markedet fra anerkjente leverandører.

Styringsgruppen for utredningen har bestått av Raymond Pettersen fra Lillehammer kommune, Aasbjørn Pålshaugen fra Gjøvik kommune, Roger Johnsen fra NorSIS og Jan Erik Svensson. Prosjektleder for utredningen har vært Peggy Sandbekken Heie fra NorSIS.

En rekke personer har bidratt med viktig informasjon og analyser i utredningen. En ekstra takk til lederne av sektor-CERTene, styremedlemmer i Kins, representanter fra KS og DIFI, ildsjeler i Bergen og Bærum kommune. I tillegg rettes det en stor takk til alle deltakere fra kommuner og interkommunale selskaper vi har intervjuet.

*Status kommune-Norge og*

# HVA ER ET CERT

## 1. Bakgrunn utredning

Norsk senter for informasjonsikring (NorSIS) har sammen med Lillehammer og Gjøvik kommune utredet behovet for å etablere et senter for forebygging, varsling og støtte ved håndtering av cybersikkerhetshendelser i kommunesektoren. Utredningen ser i tillegg på mulige organisasjonsformer, oppgaver, kompetansebehov og finansiering av en slik kapasitet.

## 2. En kommunes virkelighet

Norske innbyggere er mye på nett. Dette gir gode muligheter for tilrettelegging av digitale tjenester. Myndighetene har uttalt at digitale tjenester skal være et førstevalg for norske innbyggere. Effektivisering og forenkling skal øke arbeidskapasitet og redusere saksbehandlingstiden i kommuner og fylkeskommuner. Bidrag som vil øke velferd og verdiskaping i samfunnet.

Digitale tjenester skal være et førstevalg for norske innbyggere.

Statistisk Sentralbyrå sitt "Mediebarometer" for 2014 viser at 88 prosent av befolkningen mellom 9 og 79 år benytter seg av internett minst en gang pr. dag. Tiden som benyttes på internett har også økt, fra 112 minutter i 2013 til 120 minutter i 2014[1]

*-Kommunesektoren er enhver regjerings redskap for å realisere morgendagens velferdssamfunn*, sa administrerende direktør i KS, Lasse Hansen, under åpningen av eKommune-konferansen 2015[2].

Kommunesektoren er enhver regjerings redskap for å realisere morgendagens velferdssamfunn

1 https://www.ssb.no/kultur-og-fritid/statistikker/medie/aar/2015-04-14

2 http://ks.no/fagomrader/utvikling/digitalisering/kommit/fremtidens-ekommune/

KS utførte i 2014 "e-kommunekartleggingen" for å undersøke status for digitaliseringsarbeidet i kommune-Norge[3] . Resultatene i undersøkelsen bekrefter at kommunene har en vei å gå når det gjelder full utnyttelse av potensialet som ligger i digitale tjenester. Undersøkelsen viser at styringssystemer, strategier og prosedyrer for informasjonssikkerhet er i mange kommuner mangelfullt eller ikke utarbeidet. Tendenser som er avdekket indikerer at dette synes å gjelde flere små enn store kommuner.

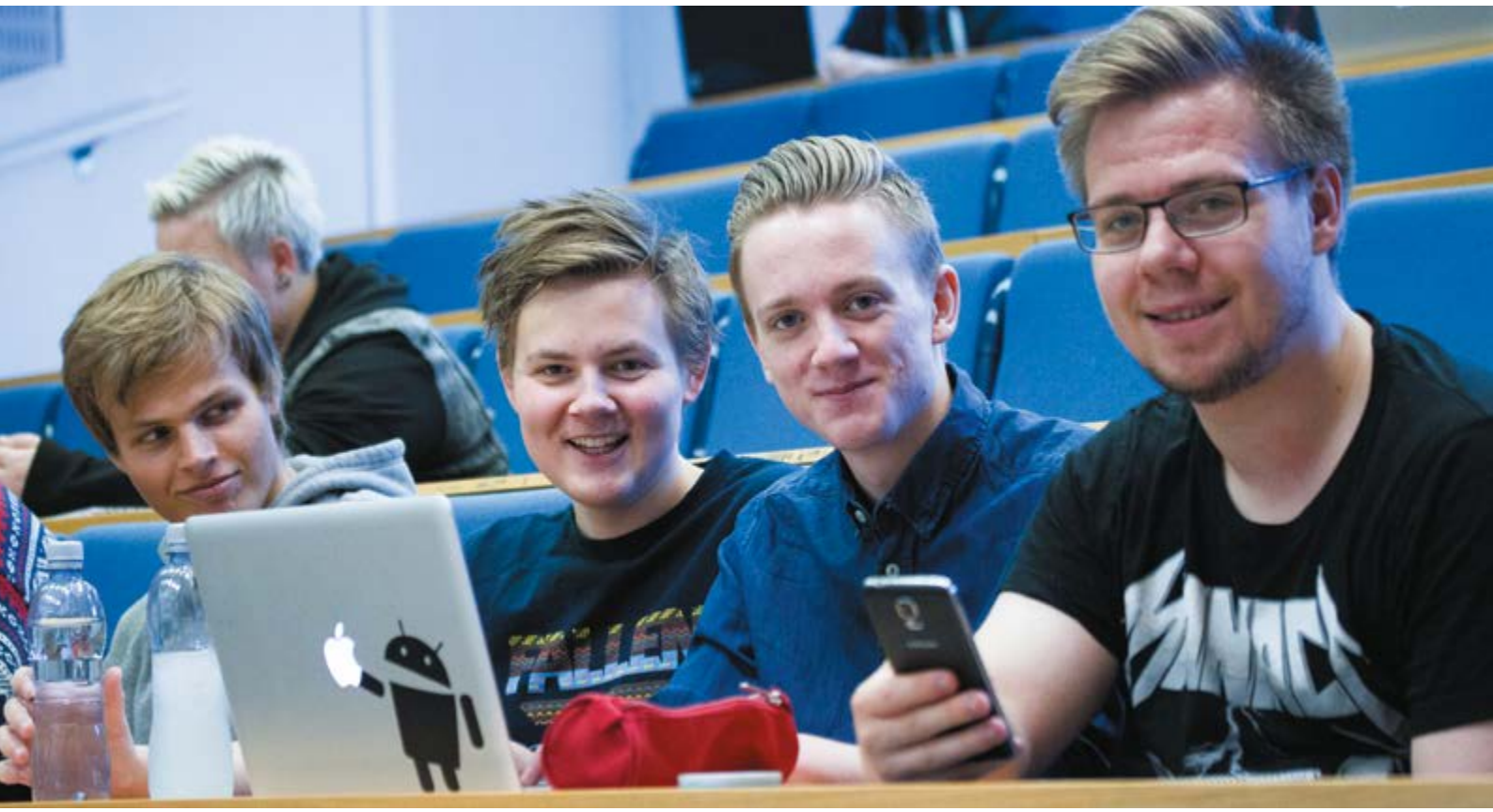
Styringssystemer, strategier og prosedyrer for informasjonssikkerhet er i mange kommuner mangelfullt eller ikke utarbeidet.

Tillit til digitale tjenester er et av fundamentene for utnyttelse av internett som kanal mellom innbyggere og kommunale etater. Tillit bygges over tid, og det vil være veldig uheldig hvis tillit til digitale tjenester blir fraværende eller reduseres grunnet lange nede-tider, utilsiktet offentliggjøring av sensitiv informasjon, spredning av virus fra web-sider eller lang og mangelfull saksbehandling.

I mange tilfeller vil mangelfull eller feil informasjon føre til fare for liv og helse, eller redusert livskvalitet.

Det vil også være uheldig hvis de ansatte i kommunale tjenester mister tillit til sine fagsystemer og de digitale tjenestene til innbyggerne. I mange tilfeller vil mangelfull eller feil informasjon føre til fare for liv og helse, eller redusert livskvalitet.

3 KS, e-kommunekartlegging 2014, Personvern og informasjonssikkerhet



Digitale tjenester medfører mye behandling av personinformasjon i kommunenes fagsystemer. Det stilles strenge krav til behandling av sensitive personopplysninger. For å ivareta kravene er det nødvendig å ha styringssystemer som ivaretar hele prosessen knyttet til informasjonsbehandling og lagring.

Alle virksomheter som behandler personopplysninger i Norge har lovkrav å følge. Det vil kunne føre til mistillit, ikke bare til systemene, men også til ledelsen i en kommune, hvis kommunen som enhet ikke følger krav til behandling av personopplysninger i sine systemer. Datatilsynet er det organet i Norge som fører tilsyn med kommunene om krav til personvern etterleves. Datatilsynet så seg i 2009 nødt til å iverksette overtredelsesgebyr som sanksjonsmiddel for brudd på personopplysningsloven. Sanksjonsmiddelet er ifølge Datatilsynet[4] nødvendig siden tidligere tiltak ikke har hatt ønsket allmennpreventiv effekt. En kommune kan risikere betydelige bøter for ikke å ha rutiner knyttet til behandling av personopplysninger på plass.

Informasjonssikkerhet er nødvendig for å ivareta tilfredsstillende behandling og oppbevaring av personopplysninger. Hvordan ledelsessystemene fungerer, hvilke svar en risikovurdering gir, hvordan etablere

Informasjonssikkerhet er nødvendig for å ivareta tilfredsstillende behandling og oppbevaring av personopplysninger.

4 www.datatilsynet.no/regelverk og avgjørelser/Tilsynsrapporter og vedtak/2015, publisert 1.6.15

og iverksette tiltak, tilfredsstillende rutiner og prosedyrer for drift og sikkerhet er alle deler av en prosess som må være etablert og innarbeidet i en kommune for å ivareta informasjonssikkerhet. Klassisk beskrivelse av informasjonssikkerhet er alle de tiltak som sikrer konfidensialitet, integritet og tilgjengelighet. Informasjonssikkerhet er en nødvendighet og en suksessfaktor for at kommunene skal kunne levere trygge og pålitelige digitale tjenester til innbyggerne.

Informasjonssikkerhet er en suksessfaktor for at kommunene skal kunne levere trygge og pålitelige tjenester til innbyggerne.

Informasjonssikkerhet er etter hvert blitt noe som «alle» må forholde seg til. Bloomberg[5] har publisert statistisk materiale fra 2014 over utbredelsen av nettbruk og bredbånd i verden. Norge topper statistikken, hele 95% av norske husholdninger er på nett.

95 % av norske husholdninger er på nett.

Privatpersoner og ansatte i virksomheter er mer og mer avhengig av IKT og internett-tilgang. Nordmenn generelt er raske til å ta i bruk ny teknologi, og mange bytter telefoner og PC-er fordi det har kommet en ny modell.

Internett åpner for et aktivt samspill mellom mennesker, tingene som omgir oss og informasjon. Vi vil se at dette i økende grad vil bli anvendt for å utnytte potensialet for verdiskapning og brukeropplevelse som ligger i teknologien. Neste generasjons velferdsteknologi vil i betydelig grad bygge på disse mulighetene. Likeledes digitaliseringen av det offentlige Norge. Fordelen vil være en døgnåpen forvaltning.

Digitalisering muliggjør en døgnåpen og brukertilpasset forvaltning.

*«World Economic Forum har dokumentert at 10% økning i digitaliseringen gir en vekst i BNP per innbygger på 0,75%[6] . I 2014 ville dette medført en vekst på 24 milliarder kroner i Norge».*

Samtidig må vi erkjenne at massiv registrering og sammenstilling av informasjon, både vil sette personvernet under press og åpne for målrettet kriminalitet. Det vil også stilles betydelige krav til tjenestetilbyderne om tilpasset funksjonalitet og sikkerhet i løsningene[7]. Det digitale samfunnet har også sine digitale kriminelle. Datakriminalitet medfører en utfordring for samfunnet og ordensmakten. Kriminaliteten utføres i det skjulte og skjer på tvers av landegrenser og uten fysisk tilstedeværelse. Gevinsten er høy og risiko for å bli tatt er lav.

5 http://www.bloomberg.com/visual-data/best-and-worst/most-wired-in-the-world-countries

6 The global information technology report 2013, World Economic Forum

7 Trusler og trender 2015, NorSIS

En rapport fra Center for Strategic and International Studies anslår at nettkriminalitet koster verdensøkonomien svimlende 3.000 milliarder kroner årlig.

Datakriminalitet kostet det norske samfunnet 19 milliarder kroner i 2014.

Mørketallundersøkelsen, utgitt av Næringslivets sikkerhetsråd, viser at datakriminalitet kostet det norske samfunnet 19 milliarder kroner i 2014.

Målrettede angrep over nettet blir mer og mer vanlig. Vår personlige informasjon som e-postadresser, bilder, kredittkortinformasjon og lignende er blitt en kapitalvare på nettet.

Personlig informasjon er blitt en kapitalvare på nettet.

*Vi logger ikke av internett når vi går fra jobb – så det du praktiserer på jobb, bør du også gjøre hjemme.* - NorSIS

Den mest omfattende trusselen er trolig tap og tyveri av mobiltelefon, datamaskiner og minnepinner.

Trusselen kommunene står overfor er sammensatt[8] . Tap og tyveri av mobiltelefon, datamaskiner og minnepinner er trolig den mest omfattende. Gjennom slike hendelser vil sensitiv informasjon kunne komme på avveier, med betydelige konsekvenser for innbyggernes personvern, merkantile forhold og kommunens anseelse. Deretter utgjør hacking og skadevare en betydelig trussel. Krypteringsvirus har de senere årene forårsaket driftsavbrudd og tap av viktig informasjon både i offentlig og privat sektor. Tjenestenektangrep og ulike former for datavirus er fortsatt en kilde til forstyrrelser og tyveri av informasjon. Nettsvindel i form av falske fakturaer, ID-tyveri og sosial manipulering inntreffer daglig. Ansatte og innbyggere forventes å kunne beskytte seg mot både tekniske og sosiale trusler. Mange av disse truslene gjennomføres med teknikker som gjør de svært vanskelig å avsløre.

Mange av truslene gjennomføres med teknikker som gjør de vanskelig å avsløre.

Trend Micro viser i sin analyse av datakriminalitet at det er helsesektoren, utdanningssektoren og offentlige myndigheter som er mest berørt. Vann, avløp og helsetjenester er kritiske funksjoner som i større eller mindre grad faller inn under kommunenes ansvar. Sabotasje av eller hærverk på datasystemer som styrer disse områdene vil kunne få store samfunnsmessige konsekvenser. Heldigvis har Norge vært forskånet fra slike hendelser. Satsningen på digitalisering tilsier derimot at vi som samfunn bør være forberedt på alvorlige IKT-hendelser.

Sabotasje av eller hærverk på IKT-systemer vil kunne få svært store samfunnsmessige konsekvenser.

Alvorlige hendelser krever involvering og håndtering av en etablert kriseledelse. Mindre hendelser må også håndteres, men kan ivaretas og håndteres uten å benytte krisedefinisjonen, men hendelseshåndtering.

Samfunnet må være forberedt på alvorlige IKT-hendelser.

8 Trend Micro, september 2015 "Follow the data; Dissectiong Data Breaches and Debunking the Myths"

Formålet med all hendelseshåndtering er å redusere skadeomfang og gjenopprette til normal drift raskest mulig.

Sikkerhetsselskapet mnemonic[9] oppsummerer tre hovedårsaker til at man overlever hendelser uten store konsekvenser;

**A.** Hell i uhell: På bakgrunn av heldige sammentreff reduseres konsekvensene.

**B.** Enkeltperson med ekstraordinær kunnskap og kapasitet: Til alt hell har organisasjonen spesialkompetanse som kan håndtere hendelsen.

**C.** Systematisk prosess og organisert kompetanse: Organisasjonen er forberedt, har lagt planer, har øvd og har nødvendige hjelpemidler tilgjengelig. De evner å lære av øvelser og hendelser, utbedrer feil og foredler kunnskap og erfaring.

En gruppe som håndterer hendelser på en systematisk og organisert måte omtales som et Computer Emergency Response Team (CERT). De vil også kunne bidra med kompetanse ut til virksomheter når en hendelse inntreffer. Beskrives nærmere i neste kapittel.

En gruppe som håndterer hendelser på en systematisk og organisert måte omtales som et Computer Emergency Response Team (CERT) eller Computer Security Incident Response Team (CSIRT).

9 http://www.mnemonic.no/Faglig/Fagartikler/IRT-Elin-i-Computerworld/

# 3. Beskrivelse av CERT (Computer Emergency Response Team)

Enheter som håndterer informasjonssikkerhetshendelser er ofte etablert som CERT og CSIRT (Computer Security Incident Response Team). Dette er begreper som i realiteten dekker samme funksjon. I enkelte sammenhenger benyttes kortbegrepet IRT (Incident Response Team). Forskjellen mellom CERT og CSIRT er at CERT er et registrert varemerke tilhørende Carnegie Mellon University (CMU) [10] . Det kreves akkreditering av Carnegie Mellon University for å benytte CERT tittelen. CSIRT er til fri benyttelse. CSIRT begrepet benyttes derfor videre i dette dokumentet som en betegnelse på et hendelseshåndteringsteam for kommunene.

Et CERT er et beskyttet varemerke fra Carnegie Mellon University.

Bakgrunnen for etablering av CERT hos Carnegie Mellon University var for å håndtere hendelser i kjølvannet av virusangrep på 80-tallet.

Et CSIRT kan ved hjelp av analogi forklares som et digitalt brannvesen[11]. Et brannvesen har et nødnummer som du kan ringe hvis du har eller har mistanke om en brann, tilsvarende et CSIRT har et nummer og en e-postadresse som du kan kontakte for å få hjelp hvis du har eller mistenker å ha blitt utsatt for en sikkerhetshendelse. En CSIRT-tjeneste vil ikke nødvendigvis respondere ved å dukke opp på dørstokken (selv om noen tilbyr denne tjenesten); de kan utføre sine tjenester via telefon eller på nett.

Et CSIRT kan ved hjelp av analogi forklares som et digitalt brannvesen.

En annen likhet mellom et brannvesen og CSIRTs er at de utfører flere tjenester enn å reagere på kriser. Det er like viktig å gjennomføre preventive tiltak slik at man forhindrer at kriser oppstår. Et brannvesen tilbyr kompetansebygging innen brannsikkerhet for å øke bevissthet og stimulere til god praksis. Likeledes vil et CSIRT også produsere veiledninger, maler og teknisk dokumentasjon og gjennomføre utdanning og opplæringsprogrammer for sitt formål. I tillegg vil begge instanser arbeide for utvikling og forbedring av lover og sikkerhetsstandarder.

Et CSIRT produserer også veiledninger, teknisk dokumentasjon og gjennomfører utdanning- og opplærings-programmer.

I Norge er det etablert sektor-CERT for helse, finans, justis, kraft og høyskole/universiteter. I tillegg har leverandører som EVRY, Basefarm og Telenor egne team med tjenester som kan høre inn under et CERT-begrep. Sikkerhetsselskaper som mnemonic, NTT Com Security og WatchCom m. fl. tilbyr også CERT-tjenester. Den nasjonale CERT-funksjonen ivaretas av NSM NorCERT I forhold til sektor-CERT-ene er NSM NorCert en paraplyorganisasjon og har jevnlige møter med de andre sektor-CERTene. I forbindelse med denne utredningen er det gjennomført arbeidssamlinger

I Norge er det etablert sektor-CERT for helse, finans, justis, kraft og høyskole/universiteter.

10 http://www.cert.org/faq/

11 http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

med de fleste sektor-CERT-ene. Formålet med møtene har vært å se på hvordan de ulike sektorene blir ivaretatt av "sine" egne CERT, og hvilke tjenester de kan tilby sine medlemmer.

Operasjonssenteret i Nasjonal sikkerhetsmyndighet, NSM NorCERT, er Norges nasjonale senter for å koordinere håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon[12]. 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.

## CERT-funksjoner

Carnegie Mellon University, som etablerte CERT- begrepet deler funksjonene til et CERT inn i tre kategorier:

### Reaktive tjenester.

Utløses av en hendelse eller varsel om angrep, ondsinnet programvare, sårbarheter i programvare eller forsøk på innbrudd. Reaktive tjenester er grunnleggende i CSIRT arbeid.

### Proaktive tjenester.

Disse tjenestene gir hjelp og informasjon til å forberede, beskytte og sikre systemer i påvente av angrep, problemer eller hendelser. Proaktive tjenester har som hensikt å redusere antall hendelser i fremtiden.

12 http://nsm.stat.no/tjenester/handtering/

## Ledelsessystemer for sikkerhet

Disse tjenestene er uavhengig av hendelser. Formålet med slike tjenester er å gi utvidet forståelse og god informasjon til ledelsen slik at man kan iverksette proaktive tiltak og utvikle eksisterende organisasjon til bedre å håndtere hendelser i fremtiden. En CERT-funksjon kan bidra med synspunkter og kompetanse slik at en virksomhet er i bedre stand til å ivareta generell sikkerhet i organisasjonen og identifisere risiko, trusler og systemsvakheter. Disse tjenestene er generelt proaktive, men bidrar indirekte til å redusere antall hendelser.

Tjenestene er listet opp i tabellform nedenfor[13].

| Reaktive tjenester | Proaktive tjenester | Ledelsessystemer |
|---|---|---|
| • Varsling | Kunngjøringer | Risikoanalyser |
| • Hendelseshåndtering<br>-Analyse<br>-Utrykning<br>-Bistand<br>-Koordinering | Trusselbildet | Katastrofe- og beredskapsplanlegging |
| | Sikkerhetsrevisjon | |
| | Konfigurering og vedlikehold av sikkerhetsverktøy, systemer og infrastruktur | Sikkerhetsrådgivning |
| • Sårbarhetshåndtering<br>-Analyse<br>-Håndtering/utrykning<br>-Koordinering | | Bevisstgjøring |
| | Utvikling av sikkerhetsverktøy | Opplæring/øving |
| • Artifakthåndtering<br>-Analyse<br>-Håndtering/utrykning<br>-Koordinering | Overvåking (IDS) | Produktevaluering eller sertifisering |
| | Formidling av sikkerhetsrelatert informasjon | |

En pragmatisk organisering av de forskjellige tjenestene har vist seg å være ISAC (Information Sharing and Analysis Centre), IRT (Incident Response Team) og SOC (Security Operations Centre), eller en kombinasjon av disse. Flere anerkjente organisasjoner har valgt en eller flere slike funksjoner for sine sentre, og har dannet "best practice". Begrepet CERT var fra opprinnelsen kun hendelseshåndtering (IRT), men har med årene blitt utvidet til også å inkludere ISAC og SOC-tjenester.

13 http://www.cert.org/incident-management/services.cfm

Tabell over myndighets- og sektor-CERTene i Norge og deres tjenestetilbud;

| CERT | ISAC | IRT | SOC |
|---|---|---|---|
| NorCERT | Analyse og varsling | Koordinere | VDI |
| UninettCERT | Analyse og varsling<br>Rådgivning<br>Utvikling<br>Sikkerhets-arkitektur | Koordinering og assistanse | Overvåker forskningsnettet |
| HelseCSIRT | Analyse og varsling<br>Etablere Nasjonalt kompetanseforum e-sikkerhet(helse/omsorg) | Råd og bistand | Overvåker Norsk Helsenett<br>Inntrengnings-testing |
| FinansCERT | Analyse, rapportering og varsling<br>Katastrofeplaner | Råd og koordinering<br>Øvelser | |
| KraftCERT | Analysere og varsling<br>Rådgivning og utarbei-delse av "best practice"<br>Kurs | Råd og bistand<br>Utrykning ved større hendelser | Rammeavtale med mnemonic |

*IRT reiser ikke ut, men gir råd og bistår

## ISAC- Information Sharing and Analysis Centre.

Vanlige oppgaver for et ISAC er å innhente informasjon fra flere instanser, analysere denne og dele med medlemmer og samarbeidende organisasjoner. Et ISAC må ha god kjennskap til medlemmenes organisasjoner, hvilke konsekvenser som kan oppstå ved sårbarheter eller ved angrep. Dette betyr i praksis at for å forstå virksomhetene må de ha tilgang til ledelsen, kommunikasjonsavdelinger og teknisk personell. Analyse av innhentet informasjon vil være reaktive tjenester, men informasjonsdeling slik at man kan ta sine forholdsregler vil være proaktivt. Et ISAC behøver ikke være bemannet 24/7.

Et ISAC må ha god kjennskap til medlemmenes organisasjoner.

Følgende arbeidsoppgaver er vanligvis tilknyttet et ISAC;

- Samarbeid med andre CERT
- Samarbeid med utenlandske CERT
- Inngå avtaler for tidlig varsling av hendelser og sårbarheter
- Holde seg generelt oppdatert om trusler, sårbarheter og utnyttelse av disse.
- Varsle medlemmer hvis relevant.

## IRT - Incident Response Team

Vanlige oppgaver for et hendelseshåndteringsteam er å bistå i håndtering av hendelser. Et IRT vil også bistå i håndtering av hendelser som ikke nødvendigvis er kriser. De vil derfor kunne avlaste et krise-/beredskapsteam. IRT vil også kunne bistå ved kriser, men krisehåndtering vil vanligvis bli håndtert av et beredskap-/kriseteam. Eksisterer ikke kriseteam er det IRT som må håndtere hendelsen. IRT bør ha vaktordninger slik at de kan reise ut eller være tilgjengelig hvis hendelser inntreffer.

Et IRT vil også bistå i håndtering av hendelser som ikke nødvendigvis er kriser.

Følgende arbeidsoppgaver er vanligvis tilknyttet IRT;

- Støtte i håndtering av hendelser
- Kompetanse
- Tiltak
- Koordinering om det rammer flere medlemmer
- Pressekontakt hvis ønskelig
- ”On-site” hos medlemmene eller bistand til lokal håndtering

## SOC - Security Operations Centre

Oppgaver knyttet til SOC er tekniske tjenester, ofte tilknyttet infrastrukturen. Overvåking av nett-trafikk og varsle ved mistanke om uønsket trafikk er basisoppgaver. Dette gjelder også ved bruk av sårbare systemer i nettverket. HelseCSIRT overvåker Norsk Helsenett. Store driftsleverandører som EVRY og Telenor har egne over-

våkingsteam. Det er også vanlig å utkontraktere slike tjenester. Bankene har som regel egne team eller har utkontraktert tjenesten til en driftsleverandører.

Basisoppgavene til et SOC vil være overvåking av nett-trafikk og varsle ved mistanke om uønsket trafikk.

Disse oppgavene er vanlige for et overvåkingssenter;

- Overvåke infrastruktur, systemer, logger
- Analysere mottatte data
- Detektere sårbarheter og forsøk på innbrudd
- Varsle medlemmene
- Erfaringsutveksling med anonymiserte data ut til medlemmene

Det er mye begrepsforvirring når det gjelder beskrivelse av tjenester knyttet til CERT-funksjoner. Ofte har organisasjoner sine egne navn og forkortelser. Vi har i de følgende kapitler valgt å benytte begrepene som de norske sektor-CERTene benytter; ISAC, SOC og IRT.

*En kommunes*

# INFORMASJONSBEHOV

Det er viktig å forstå hvilket behov kommunene har for informasjon og hjelp ved hendelser for å kunne gi anbefaling om etablering av en CSIRT-funksjon. Norges kommuner er veldig ulike i antall innbyggere, geografisk plassering og topografi. Dette påvirker samarbeidsforhold, ressurser og kompetanse. Videre i utredningen vil begrepet kommune også omhandle fylkeskommuner.

Det har i utredningen vært gjennomført dialog med flere kommuner som til sammen gjenspeiler mangfoldet. Dette gjelder i forhold til antall innbyggere og geografisk plassering. Kommunenes utsagn er anonymisert og fordelt i tre kategorier. For å sikre anonymitet har vi valgt å ikke nevne geografisk plassering, men fordele kommunene mellom liten (under 5.000 innbyggere), middels (mellom 5.000 og 100.000 innbyggere) og stor (over 100.000 innbyggere). Det har vært gjennomført dialog med IKT-personell, sikkerhetsansvarlige og kvalitetsansvarlige. Det har også vært gjennomført intervjuer med interkommunale selskaper som ivaretar kommunenes IKT-drift.

”Litt er mye mer enn ingenting” - Per Arne Enstad, Uninett CERT

Intervjuene er gjennomført for bedre å kunne forstå en kommunes struktur, prosesser og hvilke systemer som kan være aktuelle for informasjonsdeling internt i organisasjonen. Det viktigste formålet med intervjuene har imidlertid vært å ta rede for hvilke behov en kommune har knyttet til informasjon om trusselbildet og bistand ved hendelser. Det har også vært fokus på hvilke anbefalinger kommunene selv gir for en eventuell etablering av et CSIRT Flere av aktørene har god kjennskap til CSIRT og har gjennomtenkte og konstruktive vurderinger knyttet til en etablering.

Intervjuobjektene poengterer viktigheten av å få en sentralisert enhet som kommer med entydige og klare anbefalinger.

Et gjennomgangstema fra alle intervjuobjektene har vært 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 HelseCSIRT, men disse er generelle. I dag er informasjonsdeling basert på nettverk, tilfeldigheter og ildsjeler.

I dag er informasjonsdeling basert på nettverk, tilfeldigheter og ildsjeler.

Det har også vært et tema at det er vanskelig for mindre kommuner å stille krav til leverandører. Forholdet mellom leverandør og kommune er basert på tillit og manglende kompetanse gjør det vanskelig å vite hvilke krav man bør stille. Et CSIRT bør kunne lage veiledninger slik at det er enklere for kommuner å kunne stille krav til leverandører. Leverandører har ikke nødvendigvis tilstrekkelig kjennskap til å kunne levere gode løsninger uten en kravspesifikasjon fra bestiller.

Manglende kompetanse gjør det vanskelig å vite hvilke krav man bør stille.

Kompetanse er et gjennomgående tema for hvorfor et CSIRT bør etableres. De mindre kommunene har ikke ressurser og kompetanse som de større kommunene. De store kommunene som har blitt intervjuet har vist vilje til å hjelpe mindre kommuner med kompetanse også ved hendelser. Det er blitt lagt vekt på at et CSIRT bør være "navet" som knytter dette sammen. En oversikt over ressurspersoner som kan kontaktes på tvers av kommunene har også vært et forslag. Dette vil sikre et CSIRTmed begrenset bemanning en mulighet til å ivareta kompetanse på mange nivåer og systemer ved hendelser.

Kompetanse er et gjennomgående tema for hvorfor et CSIRT bør etableres.

Vi har av intervjuene og kontakt med kommunene forståelse for at begrepet CERT eller CSIRT ikke er allment kjent blant de mindre kommunene. Behovet er imidlertid der og kommunene gir uttrykk for at det er vanskelig å vite hva som er "godt nok". Mindre kommuner kan også ha utfordringer med å vite hva som skal overvåkes for eksempel ved logging. Det oppfattes også som at de interkommunale selskapene har fått ansvar for drift av IT-systemer og informasjonssikkerhet.

Kommunene gir uttrykk for at det er vanskelig å vite hva som er "godt nok".

De interkommunale selskapene trekker frem samarbeidet med Helse CSIRT som veldig godt. Dette gjelder forhold knyttet til helsesektoren i kommunene. Det trekkes imidlertid også frem behovet for overvåking og varsling av øvrig infrastruktur som det er få kommuner i dag som har ressurser og kompetanse til å utføre selv. Det er behov for tilgang til informasjon raskt for å håndtere hendelser effektivt. Det er særlig behov for informasjon tilrettelagt for sektoren om trusler, oppdateringer og spesielle typer angrep.

Kommunal Informasjonssikkerhet (Kins) er en frivilling medlemsforening for hovedsakelig kommuner. Kins har godt over 100 kommuner som medlemmer og tilbyr årlige arrangement. Styret i Kins og ildsjeler blant medlemmene har igangsatt et uformelt forum hvor medlemmene kan stille spørsmål og få svar. Det kreves innlogging på Kins sin hjemmeside og innlogging på forum for å få tilgang til innlegg. Det har vært litt blandete tilbakemeldinger i intervjuene blant kommunene på opprettelsen av dette forumet. Det positive har vært at man på et enkelt vis har fått til et sted hvor man kan diskutere mulige løsninger og dele kunnskap knyttet informasjonssikkerhet. Manglende kvalitetssikring av innhold og krav til innlogging har vært nevnt som negative elementer.

KINS har gitt eget innspill til denne utredningen hvor de bekrefter og beskriver informasjonsbehovet til kommunene;

*Kins ser et stort behov for en felles døgnåpen Kommune CERT, som kan holde seg raskt oppdatert og raskt varsle kommunene om svakheter/sårbarheter/trusler i så vel fagsystemer som standard programvare og teknologi.*

Kins foreslår også å opprette et Norsk Kommune Nett (NKN) på samme måte som Norsk Helse Nett. I tillegg anser de det som en nødvendig oppgave for Kommune CERT å kunne detektere og motvirke angrep mot det lukkede kommune-nettet.

Deres anbefaling er at det skaffes midler til å videreutvikle KinsFORUM til å bli et fungerende "varslings-CERT" for alle kommuner og fylkeskommuner. Dette kan ifølge Kins gradvis videreutvikles til å omfatte etablering av et lukket Kommune Nett og fullt ut fungerende CERT-funksjon. Bærum kommune har vært pågangsdriver for forumet og det er ildsjeler fra denne kommunen som drifter forumet.

E-kommunekartleggingen[14] til KS viser at kommuner med færre enn 5000 innbyggere har i mindre grad utarbeidet strategi for informasjonssikkerhet. Dette gjelder også for utarbeidelse av egne retningslinjer for informasjonssikkerhet.

Av undersøkelsen fremkommer det at de kommuner med god kjennskap til egne retningslinjer for informasjonssikkerhet gjelder i stor grad kommuner med flere enn 50.000 innbyggere. Dette gjelder også i hvilken grad kommunens internkontroll- og styringssystem er forankret i øverste administrative ledelse.

Undersøkelsen har også forespurt kommunene om de har tatt i bruk skytjenester og om det er gjennomført grundige sikkerhets- og sårbarhetsanalyser for de tjenestene som er tatt i bruk. Over 40% av kommunene sier nei til dette spørsmålet. Det er kun 29% som i sin egenevaluering har svart ja på dette spørsmålet. Her går det også et markant skille ved de store kommunene. Over halvparten av kommunene med flere enn 50.000 innbyggere har svart ja, mens for kommuner med færre enn 20.000 innbyggere, har under 30% av kommunene svart ja.

Kun 29% av kommunene har gjennomført sikkerhets- og sårbarhetsanalyser viser e-kommuneunder-søkelsen 2014.

Eforvaltningsforskriften[15] stiller krav til at alle underlagte virksomheter skal ha et styringssystem som beskriver mål og strategi for informasjonssikkerhet. Ut fra sin egenvurdering kan det synes at store kommuner har bedre oversikt og innarbeidet rutiner og prosesser for informasjonssikkerhet. Dette bekreftes også av intervjurunden som er foretatt ute hos kommunene og erfaring fra sektoren. Det er kun 36% av kommunene som har svart på e-kommunekartleggingen i 2014.

Store kommuner har bedre oversikt og innarbeidede rutiner og prosesser for informasjonssikkerhet.

Program for IKT-samordning i kommunesektoren (KommIT) har i sitt mandat hatt informasjonssikkerhet som en del av sin agenda. Programmet var av 3- årig varighet og er nå avviklet. Et av KommITs strategiske mål var å øke den kommunale IKTkompetansen.

14 E-kommunekartlegging 2014, KS; Personvern og informasjonssikkerhet

15 Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

På oppdrag fra KS gjennomførte Rambøll Management Consulting AS i november 2014 en vurdering av fremtidig organisering av samordnet IKT-utvikling etter at KommIT programmet var avsluttet[16]. I rapporten redegjør Rambøll for hvorledes KommIT har dekket området informasjonssikkerhet. Programstyret i KommIT har prioritert informasjonssikkerhet som et satsningsområde. KommIT har i samarbeid med Helse Sør Øst og Norsk Helsenett gjenbrukt og videreutviklet opplæringsmateriale som skal utvikle de ansattes bevissthet rundt informasjonssikkerhet. Det er usikkert hvilken effekt dette har hatt på kompetansenivået, men e-kommunekartleggingen viser at man ikke har kommet helt i mål. Bevisstgjøring er også bare en del av informasjonssikkerhetsarbeidet.

KommIT fortsetter som en fast del av KS sin organisering. KS planlegger å styrke arbeidet ved å tilføre flere ressurser fra sin linjeorganisasjon. KommIT har vært organisert som et program og har delvis vært finansiert av prosjektskjønnsmidler og av kommunene selv. Informasjonssikkerhet skal fortsatt være en del av oppgavene i linjen.

16 Rambøll; Modeller for samordnet IKT-utvikling i kommunesektoren, 26. november 2014

Administrerende direktør i KS, Lasse Hansen, uttrykte i sin innledning på e-kommunekonferansen 2015 at kommunesektoren er inne i en utfordrende tid. -"I tillegg til kommunereformen, vil regjeringen legge fram en stortingsmelding om digitalisering i vårsesjonen. Her vil regjeringen ganske sikkert klarlegge en del forventninger til oss i kommunesektoren. Det blir en utfordring å samordne eller koble statlig og kommunal sektor på en god måte. Dere er godt kjent med at statens alle løse tråder, de må vi hver dag forsøke å tråkle sammen ute i kommunen vår".

Det legges opp til betydelige endringer av rammebetingelsene for kommunene og deres digitaliseringsarbeid, ifølge KS. KS sitt arbeid har utspring i to hovedakser; den første som utviklingspartner ved å se på løsninger for kommunene og bidra med kompetanse. Den andre aksen er arbeidet med rammebetingelsene for kommunene, hvilket betyr arbeid mot regjering, departementer, direktorater og storting, det interessepolitiske arbeidet [17].

KS har bidratt med fagkompetanse i utredningen og trekker frem at det ikke er et eget direktorat for kommunene. I flere av intervjuene har kommunene nevnt KS som mulig eier av Kommune CSIRT. KS har ingen formell myndighet ovenfor kommunene. KS er derimot positive til en eventuell etablering og stiller seg til rådighet for å eventuelt se på mulige organisasjonsformer og mulige finansieringskanaler. Det er KS sitt syn at Kommune CSIRT bør finansieres av det offentlige. Til sammenligning ble HelseCSIRT i sin tid av opprettet av Helsedirektoratet. HelseCSIRT er fullt ut finansiert fra det offentlige.

KS er positive til en eventuell etablering av et kommune CERT.

17 http://ks.no/fagomrader/utvikling/digitalisering/kommit/fremtidens-ekommune/

DIFI er også blitt nevnt av kommunene som en mulig eier av Kommune CSIRT. Kommunal- og moderniseringsdepartementet (KMD) la tidligere i høst frem en handlingsplan for arbeidet med informasjonssikkerhet i statsforvaltningen[18]. Handlingsplanen skal bidra til å styrke sikkerheten og gi digitaliseringsarbeidet i offentlig sektor økt kvalitet. Kompetansemiljøet i Difi er KMDs utøvende organ for å nå målsetningen om en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen, og har dermed en viktig rolle i gjennomføringen av tiltakene i handlingsplanen. DIFIs har ovenfor NorSIS uttalt at deres rolle i handlingsplanen ikke gir mandat til å etablere CSIRT for kommunene. DIFI er ansvarlig for statsforvaltningen og det er derfor ikke aktuelt å se på mulig eierskap til en slik funksjon på dette tidspunktet.

18 https://www.difi.no/artikkel/2015/09/ny-handlingsplan-informasjonssikkerhet-i-statsforvaltningen

*Mulig sektor-CERT*

# FOR KOMMUNEN

Informasjon hentet fra kommuner, interesseorganisasjoner og undersøkelser rettet mot kommunene knyttet til informasjonssikkerhet, viser at det er mye arbeid som gjenstår når det gjelder kommunenes kompetansenivå for informasjonssikkerhet. Det synes også uhensiktsmessig at alle landets kommuner skal utvikle og etablere kompetanse og benytte ressurser på nivå med en CSIRT-funksjon.

Kommunenes utfordringer knytter seg både til manglende kompetanse og ressurser, men også vanskelig å vite hvor og fra hvem man skal henvende seg for å få korrekt informasjon. Det har også vært lite samarbeid mellom kommunene når det gjelder informasjonssikkerhet. Interkommunale selskaper knyttet til IT-drift er imidlertid mer vanlig. Leverandøravtaler som sikrer overvåking og support er ofte for kostnadskrevende for de små kommunene.

Flere store kommuner har leverandøravtaler som gir de tilgang til kompetanse eksternt i tillegg til at de også internt har god kompetanse på informasjonssikkerhet. Dette gjelder antageligvis bare et fåtall av de store kommunene som har egne informasjonssikkerhetsavdelinger.

Intervju er gjennomført med både store og små kommuner og det er gjennomgående at man ønsker mer systematisk og strukturert informasjon om sårbarheter og trusler som gjelder kommuner generelt. Dette gjelder særlig de mindre kommunene som er sårbare da man ikke har tilstrekkelige ressurser eller nødvendig kompetanse for å ivareta informasjonssikkerhet på en tilfredsstillende måte. Det er en etterspørsel etter praktiske veiledninger som enkelt kan tas i bruk av kommunene.

Det synes uhensiktsmessig at alle landets kommuner skal utvikle og etablere kompetanse og benytte ressurser på nivå med en CSIRT-funksjon.

Det er etterspørsel etter praktiske veiledninger som enkelt kan tas i bruk av kommunene.

Det synes nødvendig med vesentlig kompetanseheving blant mange kommuner knyttet til informasjonssikkerhet og håndtering av hendelser. 80 % av Norges kommuner har færre enn 5000 innbyggere. Dette forteller også noe om størrelsen på administrasjonen og kompetansemiljøet de er en del av. En sentralisert organisasjon som kan drive kompetansehevende tiltak som rådgivning, utvikle veiledninger og avholde kurs ser ut til å være oppgaver som bør ivaretas av et CSIRT Dette er også i tråd med den informasjon vi har mottatt fra kommunene selv og fra organisasjoner som KINS og KS. KINS og KS har god kjennskap til kommunene og de får henvendelser fra kommunene som tydelig viser manglende kompetanse og forståelse for hvorfor det er nødvendig med tilfredsstillende sikkerhet og god håndtering av hendelser. Hva man overvåker og lagrer av logger har også vært et tema som er uklart for mange kommuner. Et CSIRT vil kunne lage veiledninger og anbefalinger knyttet til felles utfordringer. Kommunene vil dra nytte av et sentralisert sted de kan henvende seg til.

Rådgivning, utvikling av veiledninger og avholdelse av kurs ser ut til å være nødvendige oppgaver som bør ivaretas av et CSIRT.

Kommunene vil også være bedre rustet til å håndtere hendelser. De kan kontakte CSIRT-et og få bistand selv om kapasiteten til et CSIRT ikke er "on-site".

FinansCERT og KraftCERT har begge startet sine organisasjoner med 3 ansatte. En bemanning på kun tre personer krever at man kjøper inn tjenester for å kunne opprettholde nødvendige ISAC, IRT og SOC tjenester.

HelseCSIRT som også ivaretar et sensornettverk har til sammen 9 årsverk, mens Uninett CERT kan dra veksler på Uninett sin kompetanse og utgjør til sammen 3 årsverk.

I følge CMU er det et minstekrav til hva et CERT bør tilby av tjenester. De fremhever[19]:

- analyse av hendelser
- onsite respons ved hendelser
- støtte ved hendelser
- koordinering av respons på hendelser

Ut over disse grunnleggende tjenestene, er det vanlig at CERT-er også tilbyr tilleggstjenester som varsling, support til håndtering av sårbarheter og opplæring og holdningsskapende tiltak, alt avhengig av kundenes behov. Dette bekreftes også av ENISA, som påpeker av tilleggstjenester knyttet til forebygging og opplæring er viktige for redusere risiko og behovet for respons på sårbarheter eller angrep[20].

19 West-Brown et al., 2003: Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University

20 ENISA, 2006: A step-by-step approach on how to set up a CSIRT. Tilgjengelig for nedlasting her: https://www.enisa.europa.eu/activities/cert/support/guide

To forhold framholdes som avgjørende for hva CERT-en skal tilby[21]:

- **Hva trenger medlemmene?**

Hva er nødvendig for at medlemmene skal lykkes i sin virksomhet og oppnå sine mål?

- **Hva kan CERT-en levere?**

Hva kan den levere med eksisterende ressurser, kompetanse og partnernettverk?

Et lite antall pålitelige tjenester er bedre enn mange upålitelige.

Viktigheten av å gjøre grundige vurderinger av tjenestetilbudet understrekes av en rekke aktører: Et lite antall pålitelige tjenester er bedre enn mange upålitelige – og avgjørende for å bygge tillit hos medlemmene.

Mangel på kompetanse og ressurser er et gjennomgangstema hos kommunene. Det vil derfor være nødvendig ved opprettelse av et Kommune CSIRT at de har et tjenestetilbud som på sikt ivaretar mer enn kun varsling av sårbarheter og hendelser. Flere kommuner vil ha problemer med å ivareta varslingene på en tilfredsstillende måte fordi de mangler kompetanse til å forstå tiltakene eller vite hvilke som gjelder dem. I tillegg kreves det kompetanse for å evne å oppdage hendelser når de inntreffer. Flere av disse oppgavene kan utkontrakteres, men kommunene vil fortsatt ha ansvaret for at sikkerheten er tilfredsstillende. Dette betyr at et minimum av kompetanse må beholdes internt og det er viktig med bestillerkompetanse når man skal inngå avtaler med utkontrakteringspartnere.

Flere av CSIRT oppgaver kan utkontrakteres, men kommunene vil fortsatt ha ansvaret for at sikkerheten er tilfredsstillende.

21 http://www.cert.org/incident-management/services.cfm. 16.9.2015

Flere av de små kommunene som NorSIS har vært i dialog med har informasjonssikkerhetsansvarlige og behandlingsansvarlige, som i utgangspunktet har andre fagstillinger. Utfordringen med dette er at ansatte får dette ansvaret nærmest "dyttet" på seg. En økonomiansvarlig er for eksempel ikke automatisk dyktig til å foreta risikovurderinger og iverksette styringssystemer og prosesser knyttet til informasjonssikkerhet hvis man ikke får tilstrekkelig opplæring. Likeledes gjelder dette hendelseshåndtering. Dette er fagfelt som krever spesiell opplæring.

Digitaliseringsarbeidet som foregår i stat og kommune krever at man har tillit til systemene og ivaretar sikkerheten. Det er essensielt at noen oppdager hendelser som oppstår og at man har ressurser og kompetanse til å håndtere dem. Kompetanseheving knyttet til informasjonssikkerhet er nødvendig og det er viktig at kompetansen heves i alle enheter.

Det mangler en struktur og krav til sikkerhet i kommunesystemer i dag. Normen for informasjonssikkerhet trekkes frem av KS som en god rettesnor som kan benyttes til flere formål enn kun Norsk Helsenett. Normen har tilhørende fakta-ark med beskrivelser og henvisninger til bestemmelser og regelverk.

Det mangler en struktur og krav til sikkerhet i kommune-systemer i dag.

KS sitt syn er at det tekniske i kommunene blir godt ivaretatt hos de fleste kommuner. Det som forringer sikkerheten er at det i for stor grad kun blir fokusert på praktiske løsninger. Manglende kompetanse på informasjonssikkerhet vil medføre at risikovurderinger ikke blir tatt til følge, eller at man har mangelfull risikovurdering. Det er viktig å ha bevissthet knyttet til risiko og hvilke konsekvenser man utsetter seg for ved den praksis som blir benyttet.

Et CSIRT for kommunene kan i prinsippet driftes av både offentlige og private aktører.

Et CSIRT for kommunene kan i prinsippet driftes av både offentlige og private aktører. Rådgivning og støtte forutsetter derimot omfattende kompetanse om kommunale tjenester og avviks- og risikohåndtering i kommunene. Tekniske deteksjonsoppgaver vil ikke kreve tilsvarende sektorkompetanse. Håndtering av IKT-hendelser vil derimot i betydelig grad dreie seg om å opprettholde kommunale tjenester. Selv om teknisk deteksjon er viktig, så vil kompetanse om hendelseshåndtering og omfattende kunnskap om kommunal virksomhet være en viktig forutsetninger for et kommune CSIRT.

Håndtering av IKT-hendelser er i praksis å opprettholde kommunale tjenester.

Tillit mellom et CSIRT og kommunene er helt nødvendig. Åpenhet, forståelse for og kunnskap om problemstillinger fremstår dermed som viktige suksesskriterier. Sammenblanding av støtte til hendelseshåndtering og tilsynsoppgaver anbefales derfor ikke. En CSIRT bør ha en rolle i å gi råd og bistå kommunene i å etterkomme offentlige krav og regulatoriske bestemmelser. Vi vil derfor advare mot en eventuell organisering hvor kommune CSIRT er eid eller styrt av en tilsynsmyndighet.

Kunnskap om kommunal virksomhet er en viktig forutsetning for et kommune CSIRT.

# FORSLAG TIL TILTAK

*Trust comes by feet and goes by horse!*
*-govcert.nl*

Utfordringene kommunene står ovenfor som følge av digitaliseringen, viser at et sektor CSIRT vil kunne fylle en viktig rolle. I dette kapittlet drøftes ulike måter å organisere en CSIRT på, hvilke tjenester den bør tilby og hvordan virksomheten kan finansieres.

## Organisering

I valget av organiseringsform går det et skille mellom CSIRT-er som etableres som integrerte deler av en organisasjon og de som etableres som tjenestetilbydere. Førstnevnte kan trekke på spesialister i andre deler av samme organisasjon som for eksempel Uninett CERT. Uavhengige CSIRT-er besitter all nødvendig kompetanse og tjenestetilbud selv eller de kan supplere med innkjøpt kompetanse og tjenestetilbud. Dette kan eksemplifiseres ved at man har en organisasjon som ivaretar ISAC-tjenester, men kjøper overvåkingstjenester fra en ekstern SOC.

Vi vil advare mot en eventuell organisering hvor Kommune CSIRT er eid eller styrt av en tilsynsmyndighet.

ENISA beskriver en tredje mulig organiseringsform – campus-modellen – der en sentral CERT-enhet koordinerer og støtter arbeidet som foregår i lokale CERT-enheter[22]. Campus-modellen brukes for det meste av universiteter og forskningsmiljøer der organisasjonen består av ulike geografisk spredte institusjoner.

En uavhengig organiseringsform – også omtalt som coordinating CERT[23]– synes mest aktuell for et CSIRT for kommunesektoren. Den vil ha ansvar for å koordinere håndteringen av IKT-sikkerhet hos en potensielt stor, mangfoldig og geografisk spredt kundebase. Som tilbyder av sikkerhetstjenester må den kunne stå på egne bein, med sentrale funk-

22 ENISA, 2006: A step-by-step approach on how to set up a CSIRT.

23 Killcrece et al., 2003: Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.

sjoner innenfor egen organisasjon kombinert med innkjøp av mer generelle tjenester. Vår anbefaling vil være en kombinasjon av egen organisasjon supplert med kjøp av tjenester.

ISAC vil utgjøre kjernen i et Kommune CSIRT Analyser er derimot avhengig av kontinuerlig tilgang til relevante data. Sikkerhetsmessig overvåking er en kompetansekrevende aktivitet som også er kommersielt tilgjengelig. Endring i omfang, betydelig opplæringsbehov og det faktum at slike tjenester er tilgjengelig tilsier at innkjøp av SOC tjenester er en interessant mulighet. Et Kommune CERT bør derimot være i stand til å planlegge og lede hendelseshåndtering med egne ressurser. Etablering av en ressursgruppe som bistår ved hendelser, vil ytterligere kunne styrke kapasiteten ved behov.

ISAC vil utgjøre kjernen i et Kommune CSIRT.

## Medlemmenes behov og forventninger

Medlemmenes forventninger til tjenestetilbud og tydelighet omkring tjenestene, trekkes fram som svært viktige elementer av flere aktører. National Cyber Security Centre of the Netherlands (NCSC-NL) har erfart at medlemmene forventer pålitelighet og høy kvalitet i tjenestene fra dag en, og at det er avgjørende å leve opp til dette for å oppnå tillit.

Medlemmer vil forvente pålitelige og høy kvalitet i tjenestene.

Dette er en erfaring som bekreftes av sektor-CERTene i Norge. Uansett finansiering og nærhet til sektoren må det jobbes intenst for å få frem budskapet og bli kjent som CSIRT i sektoren.

Erfaringsrapporten fra opprettelsen av NCSC-NL legger også vekt på at kundene må kartlegges tidlig i prosessen for å gjøre seg kjent med kundenes forutsetninger (organisasjon, roller og behov). Parallelt må CSIRT-en danne seg et klart bilde av hva den kan og vil levere til kundene. I tilfellet med govcert.nl var det direkte dialog med kundene i etableringsfasen for å sikre et likt syn på tilbud og etterspørsel.

## Tjenester fra koordinerende CERT

Vi har valgt å foreslå en organisering av Kommune CSIRT som en koordinerende kapasitet. Dette vil ha betydning for hvilke tjenester CSIRT-kan tilby, særlig i tilknytning til IR. Stor geografisk spredning og stor medlemsgruppe vil gjøre det svært ressurskrevende å tilby direkte respons lokalt (on-site). Den viktigste funksjonen til et koordinerende CSIRT er derfor å samordne, støtte og hjelpe i håndtering av sikkerhetshendelser.

Vi har valgt å foreslå en organisering av Kommune CSIRT som en koordinerende kapasitet.

De vanligste tjenestene fra et koordinerende CSIRT er[24]:

- Varslinger
- Analyse av hendelser
- Støtte til respons på hendelser
- Koordinering av respons på hendelser
- Koordinering av tiltak på sårbarheter og ondsinnet kode
- Kunngjøringer/informasjonsspredning
- Teknologiovervåking
- Holdningsskapende arbeid, opplæring og trening.

Den viktigste funksjonen til et koordinerende CSIRT er å koordinere, støtte og hjelpe i håndtering av sikkerhetshendelser.

Dette samsvarer med tjenestene som finnes i IRT og ISAC-funksjonene.

I tillegg kan en koordinerende CSIRT ( ISAC) tilby:

- Analyse av sårbarheter og ondsinnet kode
- Støtte til respons på sårbarheter og ondsinnet kode
- Utvikling av sikkerhetsverktøy
- Andre betalte tjenester (avhengig av tid og ressurser)

I teorien er det lite vanlig at koordinerende CERT-er yter tjenester knyttet til ledelsessystemer for informasjonssikkerhet. De avgrenses gjerne til å tilby generelle retningslinjer og veiledninger. Vi anbefaler derimot at et Kommune CSIRT bør tilby veiledninger også på ledelsesnivå. Det er viktig at øverste ledelse i kommunen trekkes med i arbeidet.

Følgende tabell viser en stegvis modell for etablering av et kommune CSIRT. Modellen viser hvilke funksjoner som bør drives under offentlig eierskap og hvilke som kan kjøpes inn. Funksjoner som foreslås etablert i samme tidsrom tilhører samme fase. Funksjonene er mer detaljert beskrevet etter tabellen.

24 Killcrece et al., 2003: Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.

Faser i etablering av et Kommune CSIRT;

| | Fase 1 | Fase 2 | Fase 3 |
|---|---|---|---|
| ISAC | • Ledelse- og analyseka-pasitet<br>• Varslingsorosess<br>• Kompetansegruppe på tvers av kommunene<br>•Samarbeid med andre CERT-miljøer | • Internasjonale nettverk<br>•Veiledere for risikovur-dering<br>•Kompetansehevende tiltak | •Utvide kompetanse-gruppe<br>•Øvelser |
| SOC | • Deteksjonsplan<br>• Avtale om innkjøp av overvåking for 1-2 tjenesteområder | • Overvåking av flere tje-nesteområder | • Overvåking av flere tjenesteområder<br>•Øvelser |
| IRT | • Plan og rutiner for hendelseshåndtering | • Ressursgruppe fra kom-munene | • Team som bistår og koordinerer hendelser<br>• Øvelser |

**Fase 1**

Kommunene har et klart ansvar for avviks- og krisehåndtering. Etablering av et CSIRT bør derfor innledes med opprettelse av ledelses- og analyse-kapasitet. Det synes mest hensiktsmessig at etablering av egen organisasjon i Kommune CSIRT starter som et ISAC. Samtidig bør det etableres avtaler med leverandører om overvåking. HelseCSIRT sitt mandat gjelder sensortjenester knyttet til helseorientert trafikk. Dette kan sammen med rapportering fra kommunenes egne IKT-leverandører utgjøre sensornettverket. Samme informasjon som mottas fra flere hold kan vise seg å ha opphav i samme kilde og uriktig forsterke budskapet. Gode rutiner for analyse bør derfor etableres tidlig.

Sammenstilling og analyse av innhentet materiale vil ivaretas av ISAC-funksjonen for kommunene. De sitter med kommunekompetansen og kan tilrettelegge og utarbeide varsling som ivaretar og trygger kommunenes tjenesteområder. Rapporter fra ISAC-funksjonen vil gi kommunene god innsikt i rådende trusselbilde som er relevant for sektoren. Varsling om virusangrep, phishing-forsøk og oppdatering av programvare er noe av basistjenestene til ISAC. Varsel om programvareoppdatering hvor det konkret redegjøres for kriminalitet, det vil si hvilke konsekvenser det gir for kommunene, vil inngå i rutine. Det vil også være nødvendig å etablere gode samarbeidsrelasjoner med øvrige CERT-funksjoner i Norge.

Som en innledende fase i IRT-arbeidet utarbeides planer og rutiner for hendelseshåndtering. Grunnleggende elementer bør prioriteres slik at de aller fleste kommuner kan implementere planverket umiddelbart og uten spisskompetanse. Personer som ansettes i organisasjonen bør ha god kompetanse i hendelseshåndtering og god oversikt over tjenestetilbud og strukturen til kommunene. Det bør også som en del av fase en etableres en kompetansegruppe på tvers av kommunene som CSIRT kan dra veksler på.

Personer som ansettes i organisasjonen bør ha god kompetanse i hendelseshåndtering og god oversikt over tjenestetilbud og strukturen til kommunene.

**Fase 2**

I fase en etableres informasjonsdeling, overvåking og varsling. Plan for fase to bør foreligge umiddelbart etter oppstart. I fase to anbefaler vi at kompetansehevende tiltak prioriteres. Varsling av sårbarheter og pågående angrep vil være nytteløst hvis en kommune ikke har tilstrekkelig kompetanse til å behandle informasjon fra CSIRT og iverksette tiltak internt umiddelbart. Det vil i den forbindelse være stor gevinst ved å etablere en ressursgruppe på tvers av kommunene som til sammen besitter høy faglig kompetanse. Gruppen vil kunne bistå med rådgivning ved hendelser til alle medlemmene i CSIRT-et. I fase to bør man også etablere samarbeid med tilsvarende CSIRT miljø internasjonalt. Et variert nettverk av både nasjonale og internasjonale aktører sikrer at man mottar informasjon fra flere kilder. Informasjon som sammenstilles fra et bredere nettverk vil ha større sannsynlighet for å speile virkeligheten og rådende trusselbilde.

Informasjon som sammenstilles fra et bredere nettverk vil ha større sannsynlighet for å speile virkeligheten og rådende trusselbilde.

Risikovurdering og andre aktuelle veiledere kan utarbeides til bruk for kommunene i denne fasen. Klassifisering og verdivurdering av kommunenes systemer vil god ha nytteverdi.

En slik forståelse vil hjelpe hver enkelt kommune i risikovurderingsarbeidet. I dette arbeidet vil det være naturlig at CSIRT stiller seg til rådighet som en sentral diskusjonspartner for kommunene. Parallelt med utvidelse av tjenestefunksjoner kan det synes hensiktsmessig å utvide med flere av kommunenes tjenesteområder. I fase to kan man også vurdere å utvide innkjøp av overvåkingstjenester for flere tjenesteområder.

**Fase 3**

Ved oppstart av fase tre vil et velfungerende ISAC være etablert. Fasen bør være dedikert utvidelse av tjenestetilbudet til å omfatte flere tjenesteområder i kommunene. Det kan også være behov for å utvide kompetansegruppen til flere områder.

Utvidelse av SOC-kapasiteten bør vurderes parallelt med utvidelse av ISAC. Tjenesteområdene som overvåkes kan utvides til å gjelde flere. I fase tre vil organisasjonen ha etablert god kompetanse og oversikt over hendelser som inntreffer og kundenes behov. En naturlig utvidelse av IRT-kapasiteten kan være å utvide fra å bistå kommunene ved hendelser til å også å opptre som koordinerende organ på tvers av alle medlemskommunene.  I fase tre bør alle CSIRT kapasitetene trenes og øves både individuelt og i samspill med kommunenes beredskapsapparat.

## Kontroll og myndighet

Tjenestetilbudet og effektiviteten til en koordinerende CSIRT påvirkes også av hvilken myndighet den har over sine medlemmer. Det er vanlig å operere med tre nivåer for kontroll[25]:

### Full myndighet:

CSIRT-en kan instruere medlemmer i respons på hendelser og, hvis tillatelse er gitt, handle på vegne av medlemmet.

### Delt myndighet:

CSIRT-en deltar i medlemmenes beslutningsprosess for å avgjøre respons på hendelser, og gir sine anbefalinger om hensiktsmessig håndtering.

### Rådgivende myndighet

CSIRT-en kan bare øve innflytelse på medlemmenes beslutninger gjennom å gi råd og å synliggjøre konsekvenser av ulike handlinger.

En koordinerende CSIRT vil normalt ha lite kontroll over medlemmene. Det innebærer at medlemmene kan ignorere råd og anbefalinger, og la være å dele informasjon om hendelser. Noe som kan hemme CSIRT arbeid med å analysere og koordinere respons på hendelser. CMU understreker derfor viktigheten av å bygge tillit og tette bånd til medlemmene for koordinerende CSIRT[26]. Dette er nærmere beskrevet i avsnittet om kommunikasjon.

"Tillit bygges i millimeter og rives ned i meter" - Per Arne Enstad, Uninett CERT

Anbefalingen fra CMU understrekes også av de norske sektor-CERTene. Kommuneloven åpner for at interkommunale foretak kan tillegges ansvar [27]. Kommunens ansvar for å opprettholde kommunale tjenester og den kommunale beredskapsplikten[28] tilsier derimot at et CSIRTbare kan tillegges begrenset formell myndighet.

Uninett CERT trekker frem at man kan bruke lang tid på å bygge tillit. Tillit i sektoren bør derfor være et viktig element ved fastsettelse av eierskap til CSIRT og ansettelse av personell.

25 West-Brown et al., 2003: Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University

26 Killcrece et al., 2003: Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.

27 Lov om kommuner og fylkeskommuner

28 Lov om kommunal beredskapsplikt

## Organisasjon og stillingsfunksjoner

En CSIRT organisasjon med flat struktur er mer fleksibel og endringsdyktig i forhold til sine omgivelser. Praksis og erfaringsrapport fra etablering av govcert.nl viser dette[29].

Oppfatningen deles av CMU. Dynamikken i den digitale verden krever fleksibilitet i håndteringen av cybersikkerhet. Rigide retningslinjer og strukturer kan være til hinder for effektiv håndtering av cybersikkerhetshendelser[30].

Rigide retningslinjer og strukturer kan være til hinder for effektiv håndtering av cybersikkerhetshendelser.

### Kompetanse og ferdigheter

Det er mer enn bare tekniske kvalifikasjoner hos medarbeiderne som er avgjørende for å lykkes. Erfaringen fra etableringen av govcert.nl viste til at man i betydelig grad er avhengig av medarbeidernes ferdigheter. Erfaringsrapporten trekker frem følgende ferdigheter som viktige:

- Fleksibilitet, kreativitet og evne til å reagere selvstendig på uventede situasjoner, både som del av et team og på egenhånd
- Gode analytiske evner for å få overblikk over situasjoner og kunne dykke raskt ned til kjernen i problemet
- Evne til å sortere og distribuere informasjon som er relevant for målgruppene
- Evne til å gjøre teknisk informasjon tilgjengelig for personer uten samme innsikt
- Integritet og evne til å skjerme konfidensielle og sensitive opplysninger
- Forståelse for administrative forhold i egen organisasjon

Det siste punktet synes spesielt relevant for etableringen av en Kommune CSIRT. govcert.nl ble opprettet som en statlig organisasjon og medarbeiderne måtte forholde seg statlig administrasjon og forvaltning. På samme måte må medarbeidere i en Kommune CSIRT forholde seg til kommunal administrasjon og forvaltning, ulike organisasjonsmodeller og styringssystemer. Innsikt i hvordan kommunen styres og fungerer vil være viktig for å forstå medlemmene situasjon og betjene dem effektivt.

Innsikt hvordan kommunen styres og fungerer vil være viktig for å forstå kundenes situasjon og betjene dem effektivt.

Erfaring fra Forsvaret viser at et CSIRT må bemannes av personell med høyere utdanning innen alle funksjonsområder. I tillegg må senior medarbeidere ha stor virksomhetskompetanse og evne til å forstå og samarbeide med virksomhetene som skal støttes. CSIRTets rutiner og prosedyrer bør tilpasses de avviks- og krisehåndteringsprosedyrer som anvendes for øvrig i virksomhetene. Personellet må trenes og øves jevn-

29 NCSC-NL, 2006: CERT-in-a-box. Tilgjengelig for nedlasting på https://www.first.org/resources/guides#bp21

30 West-Brown et al., 2003: Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University

lig for å kunne håndtere så vel rutinehendelser som mer krevende situasjoner. Et Kommune CSIRT bør derfor på et tidlig tidspunkt etablere et samarbeid med høyskole- og universitetssektoren.

Inngående kompetanse om leveranser og medlemmer er viktig. Uninett CERT har få faste ansatte. Derimot henter de inn fagkompetanse fra linjeorganisasjonen i Uninett. Rett kompetanse anses derfor som avgjørende for etablering av Kommune CSIRT. Kommunene som i intervjufasen har sagt seg villige til å hjelpe mindre omkringliggende kommuner bør med fordel kunne inngå i en ressurspool til Kommune CSIRT. Det er derfor viktig å kartlegge kompetanse blant medlemmene, slik at denne kan hentes raskt inn ved større og kompliserte hendelser.

### Partnere og nettverk

Samarbeid og informasjonsutveksling med nasjonale og internasjonale partnere er viktig for at et CSIRT til en hver tid skal være oppdatert på trender og trusler. Internasjonalt samarbeid vil dessuten bidra til at et Kommune CSIRT bidrar til å styrke cybersikkerheten generelt.

Viktig med samarbeid på tvers av sektorer. Angrep følger ikke sektorvise næringskjeder. -Uninett CERT

I likhet med overvåkingen av kundenes systemer, må også informasjonsinnhentingen fra partnere og andre eksterne kilder settes i system. Informasjonstilfanget er stort. Informasjonen må derfor samles inn og behandles effektivt gjennom en strukturert prosess. Både ENISA[31] og NCSC-NL[32] presenterer modeller for hvordan disseCERT-ene henter inn og håndterer informasjon fra kunder, partnere og offentligheten. Det er samtidig viktig å vite hvor og fra hvem man får informasjon fra.

I Norge framstår NorCERT og sektor-Certene for helse og kraft, som de potensielt viktigste partnerne for et kommune CSIRT. Det er også viktig med internasjonale nettverk. Trusted-Intruder.com og FIRST International er begge organisasjoner man kan akkrediteres som medlem av.

## Finansiering

Finansieringsmodellene for CERT-er avhenger mye av organisasjonsform og kundebase, og spenner fra rene interntjenester finansiert av virksomheten selv til de som i hovedsak baseres på medlemsavgift fra tilknyttede virksomheter.

NNCSC-NL ble under etableringen av govcert.nl finansiert og mottok driftsmidler av nederlandske myndigheter. Det tilbød sine basistjenester gratis til virksomheter i sentralforvaltningen, mens andre offentlige virksomheter (etater, fylker, kommuner mv) betaler en medlemsavgift for tjenestene. Avgiftsnivået var basert på selvkostprinsippet. I tillegg tilbød govcert.nl tilleggstjenester til selvkost. Disse tjenestene krevde ofte innkjøp av ekstern kompetanse. Ved å tilby dem som tillegg til basistjenestene kunne CERT-en holde sin egen stab liten, men likevel gi et bredere tilbud til kunder som ønsket det[31].

Finansiering basert på medlemsavgift kan by på utfordringer i etableringsfasen. Ansatte, utstyr, lokaler og markedsføring må finansieres før CSIRT har etablert en normal inntektsstrøm. Videre kan det være svært vanskelig å beregne riktig nivå på medlemsavgiften før CSIRT-en er i normal drift . Offentlig støtte, eksterne investorer eller låneopptak vil være nødvendig for å få et CSIRT i operativ drift.

31 ENISA, 2006: A step-by-step approach on how to set up a CSIRT. Tilgjengelig for nedlasting her: https://www.enisa.europa.eu/activities/cert/support/guide

32 NCSC-NL, 2006: CERT-in-a-box. Tilgjengelig for nedlasting på https://www.first.org/resources/guides#bp21

Tilstrekkelig grunnfinansiering trekkes fram som en viktig suksessfaktor i erfaringsrapporten fra etableringen av govcert.nl. Penger og oppslutning fra nederlandske myndigheter medførte at denne tjenesten ble fullt operativ raskt. Til sammenligning har sektor-CERTene i Norge budsjetter i størrelsesorden 7-10 millioner kroner pr. år.

CSIRT kan finansieres på flere måter;

- Helfinansiert av myndigheter
- Delfinansiert av myndigheter og kommunene selv (medlemsavgift)
- Helfinansiert av kommunene via medlemsavgift
- Delfinansiert av myndigheter, kommuner og sponsorer (arbeidskraft eller penger).

Tilstrekkelig grunnfinansiering trekkes fram som en viktig suksessfaktor i erfaringsrapporten fra etableringen av govcert.nl.

KS har sagt seg villig til å bistå i arbeidet med å se på mulige organisasjonsformer og finansieringskanaler.

*Vi anbefaler at et Kommune CSIRT etableres som et interkommunalt selskap. Selskapet bør bemannes og organiseres for å ivareta CSIRT ledelse og ISAC funksjonen. SOC oppgavene, herunder teknisk sikkerhetsovervåking, bør anskaffes fra anerkjente leverandører.*

Vi anbefaler at et Kommune CSIRT etableres som et interkommunalt selskap.

En slik kontrahering må selvfølgelig organiseres slik at hensynet til personvern og annen sensitiv informasjon ivaretas. Et offentlig privat samarbeid vil dessuten redusere kommunenes risiko. Leverandører vil få ansvaret for SOC kompetanse, kvalitet og skalerbarhet. Selskapets oppgaver kan dermed avgrenses til ledelse, analyse, rådgivning og informasjon.

Et kommune CSIRT vil bidra til å opprettholde viktige samfunnsfunksjoner. Driften av de sentrale delene av et CSIRT bør derfor finansieres over statsbudsjettet. Tilpassede tjenester og rådgivning til kommunene kan derimot finansieres gjennom en medlemsavgift.

## Service og bemanning

I tillegg til tjenestetilbudet er det særlig service- og bemanningsnivået som er avgjørende for kostnadsbildet til et CERT. Full oversikt over kostnadsbildet avhenger blant annet av at følgende avklares[33]:

- Er det behov for døgnåpen vakt?
- Skal CERT-en tilby alle tjenester døgnet gjennom eller begrense tjenestetilbud utenfor normal arbeidstid?
- Kan en døgnåpen tjeneste baseres på bakvakt eller løses med turnusordning?

33 ENISA, 2006: A step-by-step approach on how to set up a CSIRT. Tilgjengelig for nedlasting her: https://www.enisa.europa.eu/activities/cert/support/guide

ENISA understreker at det er viktig å gjøre en grundig vurdering av medlemmenes behov for døgnvakt, og at det er stor forskjell på å ønske og å trenge en tjeneste. Varslinger og annen oppfølging utenfor normal arbeidstid vil bare ha verdi om medlemmene har et apparat som kan utnytte dem.

Det er viktig å gjøre en grundig vurdering av behov for døgnvakt, det er stor forskjell på ønske og trenge.

Et ISAC som grunntjeneste for Kommune CSIRT vil trolig ikke kreve døgnbemanning. SOC-tjenestene som er anbefalt kjøpt inn bør derimot bemannes i større deler av døgnet.

### Kompetanseutvikling

I følge CMU er det en vanlig utfordring at CERT-er ikke sikrer tilstrekkelig finansiering til faglig oppdatering og kompetanseutvikling blant medarbeiderne. Dette kan redusere CERT-ens evne til å håndtere nye trusler, angrep og risikofaktorer[34]. Et offentlig privat samarbeid om et CSIRT vil redusere kommunenes ansvar for kompetanseutvikling.

## Informasjonsarbeid

### Kanaler

Under følger en kortfattet gjennomgang av kanaler for spredning av varsler og sikkerhetsrelatert informasjon. I tillegg til disse kommer sekundære kanaler, som seminar, konferanser og informasjonsmateriell som er mindre egnet til å distribuere tidskritisk informasjon, men som derimot er svært viktig med tanke på et Kommune CSIRT.

Et offentlig privat samarbeid om et CSIRT vil redusere kommunens ansvar for kompetanseutvikling.

#### Nettsted

CCSIRT sitt nettsted framheves av flere aktører som hovedkanalen for å distribuere varsler og bakgrunnsinformasjon. Andre kanaler viser normalt til nettstedet for utdypende informasjon. Nettstedet til HelseCSIRT inneholder derimot kun basisinformasjon om tjenesten, mens varslinger og andre oppdateringer presenteres via Helsenetts nettsider.

#### E-post

E-post er en vanlig kanal for å sende ut kritiske varsler. Dette blir også benyttet som den vanligste varslingskanalen for flere av sektor-Certene i Norge.

#### Twitter

NorCERT bruker Twitter aktivt til å spre informasjon om hendelser, trusler og sårbarheter. Twitter-feeden har nærmere 1200 følgere (per september 2015). I tillegg til mer kritisk informasjon, viser også feeden til relevant bakgrunnsinformasjon om cybersikkerhet.

34 http://www.cert.org/incident-management/csirt-development/action-list.cfm#a7 Hentet 17.9.2015

### Blogg

Både NorCERT[35] og cert.se[36] skriver om cybersikkerhet på nettsidene og bloggene til sine respektive moderorganisasjoner. Bloggene brukes til å dele mer generell, ikke-kritisk informasjon om utviklingstrekk og forebygging.

### Media

Erfaringsrapporten etter etableringen av govcert.nl nevner også radio som kanal for spredning av varsler: En nasjonal radiokanal ønsket å formidle korte nyhetsbulletiner om morgenen dagen etter at varslene var sendt ut av govcert.nl.

## Rapporteringsmekanisme

CERT-er som NorCERT og HelseCSIRT har etablert rapporteringsmekanismer med døgnåpen telefonvakt og bemanning av e-post. Ved sending av sensitiv informasjon benytter CERT-ene PGP-nøkler for kryptering.

35 http://www.nsm.stat.no/blogg

36 https://blogg.msb.se/

## Integrasjon med kvalitetssikringssystem

De aller fleste norske kommuner har implementert digitale systemer for kvalitetssikring, avvikshåndtering og internkontroll. Integrasjon med disse systemene kan være en vei for å sikre effektiv varsling av trusler og hendelser. Det er sannsynlig at varslingene kan distribueres til ulike nivåer gjennom disse systemene, enten det er kritiske meldinger til IT-ansvarlige i kommunene eller generelle meldinger til flere eller alle ansatte. Det er likevel en utfordring at enkelte kommuneansatte ikke bruker pc eller andre digitale verktøy i løpet av arbeidsdagen.

Gjøvik og Lillehammer kommune har redegjort for sine systemer som benyttes til avvikshåndtering. Det er særskilt trukket frem behovet for opplæring knyttet til håndtering av avvik. Gjøvik kommune har integrert informasjonssikkerhet som en del av sitt avvikshåndteringssystem. Dette kan med fordel benyttes til varsling ut til fagenheter om digitale trusler som for eksempel phishing-forsøk. Dette vil medføre at man raskt når mange ansatte og det via et system som er i daglig bruk.

Compilo (tidligere KvalitetsLosen) er en av de største tilbyderne av slike løsninger, med rundt 220 norske kommuner på kundelisten[37].

## Dialog med medlemmene

Personlig kontakt og åpen dialog med medlemmene trekkes fram som viktige suksessfaktorer i flere av veilederne om etablering av CERT-er. Énveis informasjon fra CERT-en er ikke tilstrekkelig. Toveis kommunikasjon og samarbeid må på plass for å informere om tjenester, tiltrekke nye kunder, og bygge tillit og samarbeid blant eksisterende medlemmer. Det forenkler samarbeidet og kan styrke åpenheten i forholdet mellom medlemmene og CERTet[38].

Personlig kontakt og åpen dialog med medlemmene trekkes fram som viktige suksessfaktorer.

govcert.nl strukturerte deler av medlemskontakten ved å gjennomføre seks samlinger i året for sine medlemmer. Under disse samlingene fikk teknisk personell og sikkerhetsansvarlige hos medlemmene drøfte overordnede utfordringer knyttet til cybersikkerhet. Samme aktør brukte også betydelig ressurser til å selge inn tjenesten overfor nye medlemmer ved å overbevise dem om verdien av tjenesten. Dette gjaldt primært betalende medlemmer, men også deler av sentralforvaltningen som kunne benytte tjenesten gratis, men som ikke var pålagt å bruke den. NorCERT gjennomfører månedlige samlinger for sektor-Certene i Norge.

37 http://www.vest24.no/denne-mannen-treng-5-6-nye-medarbeidarar/s/5-82-15381

38 ENISA, 2006: A step-by-step approach on how to set up a CSIRT. Tilgjengelig for nedlasting her: https://www.enisa.europa.eu/activities/cert/support/guide

## Dokumentasjon av resultater

God statistikk over leveranser og resultater trekkes fram som viktig for å dokumentere verdien av CERT-en overfor medlemmer og andre interesser. Sammenstillingen av statistikk bør automatiseres helt fra oppstarten. NCSC-NL anbefaler også å bruke dokumentasjonen overfor medlemmer og eiere for å styrke deres eierskap til CERT-en[39].

Eksempler på slik statistikk er:
- Medlemmer: antall, omfang
- Varslinger: antall sendt ut, fordelt på kategorier og viktighet
- Rapporter: antall varslinger mottatt

Start i det små og bygg sten på sten.

## Oppsummering av de viktigste suksessfaktorer

- Starte i det små og bygge sten på sten
- Sikre grunnfinansiering som gjør at CERT-en blir fullt operativ raskt
- Holde det man lover – helt fra dag en
- Kommunisere enkelt og tydelig selv om vanskelige, tekniske tema
- Skape et godt samarbeidsklima med medlemmer og partnere
- Bevare fleksibilitet og entreprenørånd i organisasjonen
- Kjenne sin sektor og ha godt samarbeid på tvers.

Kommuniser enkelt og tydelig selv om tema er teknisk vanskelig.

## Viktigste fallgruver

- Manglende kunnskap om medlemmene og deres situasjon
- Tilby tjenester uten å kunne leve opp til tilbudet
- Tilby tjenester basert på ønsker, ikke faktiske behov
- Starte opp uten forankring i sektoren
- Manglende innflytelse over medlemmene – de følger ikke råd og feiler.

Ha kjennskap til sin sektor og ha godt samarbeid på tvers.

39 NCSC-NL, 2006: CERT-in-a-box. Tilgjengelig for nedlasting på https://www.first.org/resources/guides#bp21

**Vi vil anbefale at det arbeides videre med planer om å etablere en CSIRT-funksjon for kommunene. Dette for å ivareta og bygge tillit til digitaliseringsarbeidet og sikre leveranser av kommunale tjenester.**

## Gode tips til videre arbeid

Det finnes mye materiell som en prosjektgruppe ved etablering kan sette seg inn i. ENISA har utarbeidet en guide for de som skal etablere CERT-funksjoner. I tillegg finnes det mye informasjon hos organisasjoner som SANS Institute, ISACA og erfaringsmateriell på nettet. Et eksempel som er benyttet i utredningen er evaluering av opprettelsen av nederlandske GovCert. Det finnes også organisasjoner man kan tegne medlemsskap i. En internasjonal organisasjon er Forum of Incident Response and Security Teams (FIRST). FIRST etablerer både kurs og konferanser hvor man kan møte likesinnede og utveksle informasjon og erfaringer. Trusted-Intruder er et annet nettverk som også tilbyr kurs.

Vi har under arbeidet med utredningen fått tips om eller vært i kontakt med flere internasjonale institusjoner som er aktuelle for eventuelle besøk. En organisasjon er CERT-IST i Frankrike og en annen er innen WARP-konseptet i Storbritannia hvilket ENISA anbefalte kunne

være aktuelt. CERT-IST er en privat organisasjon i Frankrike som har stor bredde og kundeportefølje på tvers av sektorer. De har en ISAC-funksjon og kan bidra med verdifull erfaring i det å serve mange ulike fagenheter.

WARP-konseptet er et verktøy for deling av informasjon mellom medlemmene i mindre lokalsamfunn. De er enkle å sette opp og vedlikeholde, og er et rimelig alternativ til et fullvoksent CERT. WARP er utbredt i Storbritannia, og konseptet kan benyttes i andre land. Brukere nåes via internett og man vil kunne nå også de som normalt ikke er med i et samarbeid om informasjonsutveksling. Ved samarbeid mellom CERTer og WARPs knyttet til informasjonsdeling vil begge parter få nytteverdi og sikkerhetsmiljøet kan i større grad fjerne "white spots" i sikkerhetslandskapet. Til sammenligning kan et WARP muligens være et avviksystem i en kommune.

MS-ISAC i USA kan også være et sted å besøke for å se på organisering på tvers. MS-ISAC sine kunder er på tvers av statene i USA. De har både statlige, lokale og territoriale myndigheter som sine kunder.


www.norsis.no