Vedlegg F – Fagnotat SOC

Security Operations Center i kommunal sektor

Innhold

Innledning

Norske kommuner har stort fokus på digitalisering. Digitalisering av kommunale tjenester og etablering av nye tjenester i sektoren gir store muligheter for den enkelte kommune, innbyggerne og næringslivet. Økende bruk av digitale tjenester kan føre til enklere drift, bedre mobilitet og økt produktivitet i kommunene. Det kan samtidig medføre økende kompleksitet, lange og uoversiktlige verdikjeder og med det også øke risiko.

Nasjonal sikkerhetsmyndighet (NSM) skriver i Risiko 2022 at cyberaktivitet mot Norge skjerper det digitale trusselbildet og at fra 2019 til 2021 har NSM sett en tredobling i antall alvorlige hendelser og cyberoperasjoner. Fremmede etterretningstjenester står bak flere alvorlige hendelser i denne perioden. Risiko for alvorlige cyberoperasjoner er høy og øker. I tillegg ser NSM en kraftig økning i digital utpressing og sabotasje, såkalte løsepengevirus eller ransomware. Både her hjemme og i andre land har slike hendelser fått omfattende konsekvenser ved at systemer lammes og viktige tjenester stopper. Bare i desember 2021 ble matvareprodusenten Nortura, mediekonsernet Amedia og Nordland fylkeskommune rammet av slike cyberhendelser.

Et av de mest sentrale tiltakene mot denne typer hendelser er å etablere en evne til å oppdage og håndtere sårbarheter. Alle kjente rammeverk som dekker informasjonssikkerhetsområdet omhandler evne til å oppdage og håndtere sårbarheter i egen infrastruktur. NSMs grunnprinsipper for IKT-sikkerhet, NIST-rammeverket, CIS Critical Security Controls og ENISA-anbefalinger omtaler alle denne sentrale evnen.

I sektoren er det store variasjoner i størrelsen til kommunene i form av ansatte og innbyggere. Situasjonen for de aller fleste små og mellomstore kommuner er at de har faglige og økonomiske utfordringer med å ivareta ansvaret for å identifisere, forebygge og håndtere digitale trusler alene.

Selv om det er stor variasjon i størrelse, kapasitet og kompetanse i kommunene, er det store likheter i angrepsflater og angrepsvektorer, samt forebyggings- og håndteringsmetodikk. Av den grunn er det også sannsynlig å oppnå betydelige effekter med tanke på forebygging og håndtering av digitale angrep dersom det etableres strukturer for samarbeid og felles tjenester. Dette vil også være i tråd med KS' digitaliseringsstrategi der visjonen er at gode og tilgjengelige digitale tjenester styrker dialogen med innbyggere og næringslivet, og gir gode lokalsamfunn.

En viktig del av arbeidet med identifisering og forebygging vil handle om SOC-relaterte tjenester. I kommunal sektor har SOC stor oppmerksomhet det siste året. KS er kjent med at et stort antall kommuner er i prosess med å enten etablere et SOC eller tilknytte seg en ekstern leverandør av SOC. Hva SOC-tjenester innebærer, og hvordan det kan organiseres for å få best mulig effekt for kommunal sektor drøftes i dette fagnotatet.

Alternativene som drøftes er:

- Etablering lokalt (i den enkelte kommune)
- Kjøp av SOC-tjenester/funksjoner av kommersiell aktør (av den enkelte kommune)
- Regionalt, eksempelvis i foreslåtte operative sikkerhetsmiljø i diginettverkene.
- Etablering av SOC på nasjonalt nivå, eksempelvis i eller i tilknytning til en CERT.

Det vil være muligheter for hybride løsninger der prefererte egenskaper fra de forskjellige alternativene kombineres for å gi en bedre løsning.

Avgrensning

Dette notatet beskriver:

1. Hva et security operations center (SOC) er
2. Hva som kreves av ressurser innen kompetanse, kapasitet, økonomi og teknologi for å etablere et SOC tilpasset et kommunalt behov
3. Hvilke fordeler og ulemper kommunal sektor vil stå overfor ved etablering av SOC lokalt, regionalt, nasjonalt og kommersielt (kjøp som tjeneste fra leverandør)

Som beskrevet i innledningen er notatet utviklet for å drøfte hvilke muligheter som finnes i kommunal sektor for å samarbeide om SOC-tjenester, enten som tjenester i regi av kommunene selv eller som en del av et tjenestekjøp fra leverandører.

Notatet drøfter ikke andre sentrale sikkerhetsfunksjoner annet enn SOC-tjenestene, og vil derfor utelukkende omtale forholdet mellom et SOC og andre sikkerhetstjenester med grensesnitt mot SOC på en generisk måte. De nærmeste samarbeidspartnerne med et SOC vil normalt være en CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) og IRT (Incident Response Team). En CERT/CSIRT er en koordinerende enhet for informasjonssikkerhet, mens et IRT er et team som responderer på og håndterer hendelser («kriseledelse» innen IKT). Selv om disse tjenestene og funksjonene er ofte integrert eller i samarbeid med en SOC, fokuserer dette notatet utelukkende på basisfunksjon i SOC.

Hva er et Security Operations Center?

Et sikkerhetsoperasjonssenter, også kjent som et SOC, er en administrert sikkerhetstjeneste som overvåker og analyserer virksomhetens infrastruktur med hensikt om å forebygge, oppdage og hindre uønskede informasjonssikkerhetshendelser. Et SOC defineres av ENISA som et senter som «leverer deteksjonstjenester ved å observere tekniske hendelser i nettverk og systemer, og kan også være ansvarlig for hendelsesrespons- og håndtering. I store virksomheter kan SOC kun fokusere på overvåknings- og deteksjonstjenester, og overlater deretter hendelseshåndteringen til CSIRT "[1]

Et SOC kan være organisert internt i virksomheten, eller tilknyttes eksternt. Et SOC er avhengig av verktøy, tilgang på kompetanse, god dataflyt i tjenestene og oversikt og innsikt i infrastruktur. En slik funksjon er normalt døgnbemannet, noe avhengig av størrelsen og hvilke andre tjenester som krever døgnbemanning i virksomheten. Sikkerhetsoperasjonssenteret bør rapportere til organisasjonens informasjonssikkerhetsansvarlig og/eller til virksomhetens responsenhet, og være i løpende dialog med IKT-driftsorganisasjonen i virksomheten.

Forholdet mellom IKT-driftsorganisasjonen og et SOC kan være alt fra at SOC er totalintegrert til helt frittstående. I mindre virksomheter er det naturlig at et SOC deltar i driftsoppgaver i stille perioder.

Funksjon

Et SOC skal overvåke nettverkstrafikk, endepunkt og IKT-infrastrukturen. Funksjonen skal oppdage og forhindre, bidra til å håndtere hendelser raskere, og kan ha mulighet for å gjennomføre rotårsaksundersøkelser og iverksette tiltak. I et slikt senter vil det typisk foregå en kontinuerlig overvåkning av intern- og internettrafikk, intern nettverksinfrastruktur, servere, endepunkt, databaser, applikasjoner, IoT-enheter og fagsystemer. Avhengig av modenhet på infrastruktur,

[1] ENISA report – how to set up CSIRT and SOC, 2020. Tilgjengelig fra https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

integrasjoner og kompetanse vil et etablert og operativ SOC kunne gjennomføre automatiserte risikomitigerende tiltak parallelt med at virksomhetens egne eller innleide IRT-ressurser alarmeres.

Med riktige forutsetninger, tilgang på kompetanse, verktøy og datakvalitet, skal SOC kunne sette opp varsler på unormal oppførsel i infrastruktur. Det er vanlig at det etableres regler for vanlig og akseptabel aktivitet, og hva som ikke er. Disse reglene finjusteres løpende, avhengig av kjennskap og kompetanse om oppførsel i infrastrukturen.

Ved unormal aktivitet undersøkes aktiviteten av personell i SOC. Dersom det indikeres at aktiviteten er ondsinnet kan flere involveres, og håndtering iverksettes. Dersom det oppdages behov for å mobilisere virksomhetens øvrige beredskapsorganisasjon og involvere annen kompetanse, eksempelvis informasjonssikkerhetsleder, IRT, beredskapsrådgivere o.l, er det funksjonens ansvar å varsle.

Et SOC skal rapportere ved definerte intervaller til IKT-organisasjonen og relevante ledere. Det skal sikre at ledelsens er oppdatert på antall hendelser, og gi en situasjonsoversikt og innblikk i trusselbildet for virksomheten.

Tjenesteleveranser

Et SOC har normalt definerte tjenester og leveranser. Avhengig av virksomhetens størrelse og behov kan primære tjenester være:

- Overvåking av løsninger
- Sårbarhetsanalyser
- Logg-analyser, herunder konsolidering av logg og analyse
- Inntrengningsdeteksjon på nettverk og maskiner
- Endepunktsovervåkning
- Overvåkning av sky- og skytjenester
- Rapportering og oppfølging
- Sikkerhetsorkestrering og automasjon
- Etablering av regler og malverk for hva som skal monitoreres og logges
- Agere og iverksette tiltak basert på informasjon fra CERT-strukturen
- Overvåke det generelle situasjons- og trusselbildet
- DNS-sikkerhet, e-post sikkerhet, malware, virus
- Vulnerability Management, undersøkelse etter utnyttede sårbarheter

ENISA lister opp følgende tjenester i en SOC-funksjon, der uthevet skrift er minimumstjenester:

Figure 3: First service framework – Typical SOC services

Sekundære tjenester:

- Utvide repertoaret for hva som alarmeres på
- Kartlegge organisasjonenes sårbarheter, eksponering og fotavtrykk på nett proaktivt
- Deteksjon av misbruk (domene, e-post, navn)

Struktur og kompetanse

Et SOC skal være en sentralisert organisering i virksomheten, enten etablert internt eller tilknyttet eksternt. I et slikt senter vil det være behov for spesialisert sikkerhetskompetanse, men også kompetanse innen IKT-drift, juridisk kompetanse og beredskapskompetanse. I et SOC vil det generelt være behov for følgende kompetanse:

- Leder med ansvar for drift, oppfølging av aktivitet og rapportering til virksomhetens ledelse
- Sikkerhetsanalytikere (security analysts, security investigator eller incidents responders) med oppgave i å oppdage, undersøke og være de første respondenter på varsler. Disse omtales gjerne som førstelinjen.
- IT-sikkerhetspersonell med ansvar for å utarbeide og vedlikeholde deteksjonsregler og malverk.

Verktøy

Et SOC er avhengig av ulike verktøy og god datakvalitet. Manglende visibilitet og evne til logging i digital infrastruktur kan medføre begrensninger for evnen til monitorering, analyse og håndtering. Relevante verktøy for et SOC er blant annet, men ikke avgrenset, til:

- Loggserver(e), for eksempel Splunk, Senitel, Log Analytics, Elastic e.l
- Security Information and Event Management (SIEM). For eksempel Splunk, Senitel, Elastic/Kibana, Qradar.
- MISP, Malware Information Sharing Platform. Trussel- og etterretningssamarbeid som henter trusselbildeinformasjon fra åpne kilder.

- MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)
- Nettverksmonitoreringsverktøy, eksempelvis Defender for Cloud og Microsoft Sentinel.
- Endpoint detection and response verktøy (EDR), eksempelvis Carbon Black og Cisco AMP.
- Håndtering av varslinger og funn fra CERT-strukturen.

Kommunenes rammevilkår og behov

KS har gjennom høsten 2021 og 2022 gjennomført et innsiktsarbeid for å identifisere behov på informasjonssikkerhetsområdet i kommunal sektor. En av de sentrale funnene er at store deler av sektoren har behov for å etablere eller videreutvikle evne til å oppdage potensielle eller faktiske hendelser i sin infrastruktur. Mange kommuner vurderer det slik at kravene som stilles til den enkelte kommune med hensyn til kompetanse og kapasitet for etablering og drift av et SOC ikke er mulig å imøtekomme alene. Dette gjenspeiles blant annet i arbeidet med anskaffelsesprosesser for SOC-tjenester som pågår i en rekke kommuner og IKSer. Samtidig vil økonomiske krav til etablering og drift av et SOC være langt større enn det mange små og mellomstore kommuner kan klare alene.

I løpet av 2022 har KS fått melding om et titalls kommuner som alle arbeider med å anskaffe SOC eller SOC-relaterte tjenester. Anskaffelsesprosessene begrunnes med behovet for å få etablert tjenesten så snart som mulig, samt at det for de aller fleste kommunene ikke er mulig å etablere et SOC på egenhånd.

Vurderingskriterier

Kommunenes samlede behov er å etablere en egenevne til beredskap, forebygging, avdekking og hendelseshåndtering. For å imøtekomme de delene av dette behovet som omhandler overvåking og håndtering, har KS vurdert ulike alternative modeller for etablering av SOC i sektoren. For å vurdere ulike modellers egnethet for kommunal sektor, settes det opp vurderingskriterier de forskjellige modellene kan vurderes opp mot.

A: Kompetanse

Ved etablering, drift eller tilknytning til SOC-funksjon/tjeneste er det vesentlig for tjenestens kvalitet at det er tilgang på tilstrekkelig og tilpasset kompetanse i SOC-funksjonen.

Ressursbehovet til et SOC for å kunne levere døgnbemannet på de områdene som beskrevet under «Tjenesteleveranser» er betydelig. Det kreves spisskompetanse på hvert av områdene sin utgjør tjenesten, og behovet er ofte svært tidssensitivt.

Det er behov for spesialisert kompetanse i en SOC-funksjon, og dette er nå en kompetanse som er svært ettertraktet i arbeidsmarkedet. Etterspørselen etter kompetanse er vesentlig større enn tilbudet og utdanningstakten, noe som tilsier at etterspørselen vil være vedvarende høy i en lengre periode. Det eksisterer ingen utdanningsretning som gir en entydig «SOC-utdanning», noe som gjør at alle ressurser som skal arbeide i et SOC i praksis er utdannet gjennom en kombinasjon av utdanning, interesse og erfaring. Det er derfor sannsynlig at et SOC også må ta høyde for å utdanne egne ressurser over tid.

En SOC-tjeneste krever i utgangspunktet ingen lokal tilstedeværelse, men det vil være en betydelig fordel for et SOC å kjenne til lokale og spesifikke forhold som gjelder en enkelt virksomhet. Særlig gjelder dette i situasjoner der virksomhetene som skal støttes er lite homogene i sin infrastruktur, se kapitel «C: Kunnskap og lokale forhold» for utdyping.

B: Økonomi

SOC-funksjonen er den desidert mest ressurskrevende i en fullfunksjons sikkerhetsorganisasjon. I mange tilfeller må det i større organisasjoner være mer enn 20 heltidsansatte for å kunne dekke alle fagfelt og samtidig ha døgnbemannet drift. Dette er avhengig av størrelsen på infrastrukturen, men 4 årsverk pr skift (16 årsverk) er et minimum for å dekke sikkerhetsfunksjonene i døgndrift. Kostnader og drift av et SOC består i all hovedsak av lønn og lisenser til verktøy.

Siden et SOC kan skalere og dekke flere virksomheter uten å øke ressursbruket tilsvarende, vil det være gode muligheter for å hente ut stordriftsfordeler på lisenser og personell. Dette er også forretningsmodellen for de virksomhetene som selger SOC-tjenester i dag, selv om dette bildet korrigeres noe av at pris også avhenger av datamengde.

Etablering og drift av et SOC vil potensielt også utløse kostnader i andre deler av virksomhetene som benytter tjenestene. Det vil over tid avdekkes nye behov som vil utløse nye kostnader, for eksempel deler av infrastrukturen som ikke er dekket initialt, behov for tilpasninger og økte krav til logging, analyse og respons.

I utgangspunktet vil valg av teknologi og verktøy være mest avhengig av virksomhetens økonomi, ønsket tjenestespekter og kompetansesammensetningen i SOC. Når det gjelder teknologi og verktøy bør derfor mulighet for skalering og potensielle kostnader på grunn av kompleksitet belyses. Kapasitet til å oppdage, analysere og agere på hendelser vil også påvirke kostnadsbildet gjennom økte krav til verktøy, kompetanseprofiler og antall personer som må inngå i SOC.

C: Kunnskap om lokale forhold

Erfaring fra kommuner viser at kjennskap til lokale forhold er sentralt for å kunne levere gode SOC-tjenester. Et SOC som ikke har kjennskap til infrastrukturen, hva den benyttes til eller hvilke deler som påvirker hverandre vil ikke være i stand til å levere tidsriktige og gode tjenester. Kommunene kan sees på som sammensatt av flere sektorer, og tilhørende infrastruktur gjenspeiler dette. Kunnskap om hvordan en kommune fungerer ut over teknologien vil kunne være kritisk i forbindelse med oppdagelse av en hendelse. Det har også en stor betydning for oppsett av regler, malverk og etablering/tilknytning til tjenesten.

Dersom ikke kunnskapen om lokale forhold er til stede, må det påberegnes en lengre implementeringsfase og større ressursbruk fra mottakskommunen.

D: Respons/reaksjonstid

Som en forlengelse av kunnskap om lokale forhold er den tiden som benyttes til å reagere på trusseletterretning fra CERT/CSIRT og veilede kommuner i risikomitigering viktig. Kunnskap om kommunenes situasjon, kompetansenivå og dermed evne til å motta og fordøye anbefalinger om tiltak vil innvirke direkte på den tiden det tar fra en ny risiko blir kommunisert på nasjonalt nivå til den blir mitigert i den enkelte kommune.

Et SOC vil i utgangspunktet være døgnbemannet og dermed ha kort respons/reaksjonstid for hendelser uansett hvor i infrastrukturen en hendelse oppstå, men oppfølging/mottak hos kommunene vil være avhengig av gjensidig kunnskap og forståelse. Geografisk plassering har liten betydning for arbeidet i en SOC i dette perspektivet, i motsetning til for eksempel en IRT.

E: Volum

Et SOC kan potensielt overvåke et svært stort antall enheter i en infrastruktur, men evne til håndtering både falske positive og faktiske hendelser i parallell er krevende og øker med antall enheter i infrastrukturen. Dette kan kompenseres noe ved bruk av verktøy og deling av malverk,

funn og tiltaksbeskrivelser, men mulighetene til dette vil være størst der infrastrukturen og tilhørende systemportefølje er relativt samsvarende. En heterogen infrastruktur vil være krevende å hente ut stordriftsfordeler. Det er derfor en nødvendig forutsetning ved alle alternativer at funksjonen kan håndtere volumet.

Muligheter og utfordringer for kommunal sektor og SOC-funksjoner

De aller fleste SOC-tjenestene kan som nevnt leveres fra et annet fysisk sted enn tjenestene skal konsumeres. Dette muliggjør sentralisering av tjenestene, og derigjennom oppnå stordriftsfordeler. Hvorvidt man bør etablere et SOC lokalt, sammen med andre i en større kontekst, for eksempel regionalt eller nasjonalt, må derfor vurderes ut fra andre kriterier enn bare tjenesteleveransenes beskaffenhet.

Som beskrevet under «Hva er et Security Operations Center» inngår en rekke funksjoner og tjenester i et SOC. Selv om tjenestene ikke er bundet fysisk til et sted vil det være begrensninger i andre deler av tjenesteproduksjonen som kan begrense hvor mye tjenestene kan skaleres og sentraliseres.

Lokal SOC – SOC i kommunen

Med lokalt etablert SOC menes at hver enkelt kommune etablerer et eget SOC for egen kommune og leverer funksjonen til seg selv. Ved etablering av intern SOC i den enkelte kommune, må kommunen selv bære kostnaden med etablering, implementering, personell og drift. Det er teknisk mulig å etablere og drifte et SOC lokalt i den enkelte kommune, men dette alternativet er vanskelig å se for seg mulig å gjennomføre med tilstrekkelig både med tanke på tilgang på kompetanse og økonomisk forsvarlighet. Dette kommer av at kommunen må ha evne til å rekruttere, vedlikeholde, utvikle og beholde spisskompetanse i funksjonen, en spisskompetanse som er svært ettertraktet i arbeidsmarkedet.

De færreste kommunene har mulighet til å påta seg en ny driftsutgift på flere millioner kroner i året. En utfordring er derfor det økonomiske aspektet, og at en slik funksjon er ikke synlig for innbyggere samt at driftsutgiften medfører ikke mulige inntekter. De største kommunene vil sannsynligvis kunne etablere et SOC, men det er og vil også her sannsynligvis bli utfordringer med rekruttering av relevant kompetanse. Dette gjelder særlig i områder der flere aktører etterspør den samme kompetansen. Etableringen fordrer også at det tilkjennes nok økonomiske midler til etablering og varig drift i kommunen.

Lokal SOC vil ikke gi stordriftsfordeler der flere deler på utgiftene og kompetansen, og i liten grad gi mulighet til bistand mellom kommunene. Kommunene vil måtte rekruttere og konkurrere om den samme spisskompetansen, og det er grunn til å tro at særlig distriktene vil oppleve utfordringer med rekrutteringen.

Regional SOC – SOC-samarbeid

Med regional SOC menes en felles funksjon som etableres for å betjene flere kommuner i en region. Organisatorisk plassering kan eksempelvis være i digitaliseringsnettverkene. Det er nærliggende å tenke at det er én vertskommune for fysisk- og organisatorisk plassering, men at tjenesten er tilgjengeliggjort til flere kommuner. Et regionalt SOC må levere de samme tjenestene som andre alternativer. Etableringen av regional SOC kan løses ulikt i de ulike regionene, avhengig av mulighetene og utfordringene i den enkelte region. For å oppnå stordriftsfordeler er det likevel ønskelig at, dersom det landes på regionalt alternativ, det utformes mest mulig likt på tvers av regionene.

Et regionalt SOC må ha evnen til å rekruttere, vedlikeholde, utvikle og beholde spisskompetanse. Ved en slik organisering, må det av hensyn til antall kommuner tilknyttet, være et større fagmiljø og mer operativ kapasitet. Det er derfor nærliggende å tenke at et regionalt SOC vil ha muligheten til å tilby en attraktiv arbeidshverdag- og plass. I det videre vil det også være en fordel ved at kommunene selv ikke må konkurrere om den samme spisskompetansen, men heller samarbeide og nyttiggjøre seg av samme kompetanse- og personell. I dagens samfunn er ikke arbeidsplass- og tilhørighet like avhengig av fysisk lokasjon som tidligere. Dette gjelder også for personell i en regional organisasjon. Det kan dermed være mulig å ha personell fysisk beboende på andre geografiske lokasjoner enn der tjenesten leveres.

Økonomisk vil det kunne oppnås stordriftsfordeler ved behov av anskaffelse av system, verktøy- og lisenskostnader. Fremfor at hver kommune må gå til anskaffelse av de samme verktøy, kan dette anskaffes i fellesskap.

Dersom det etableres flere regionale SOC kan de samarbeide og bidra til å skape et oversiktsbilde for kommunal sektor. Dette fordrer at det etableres rammer for etablering og drift av strukturen. Disse funksjonene kan også bidra til at de kommunene som i dag ikke evner å respondere og konsumere de tjenester som leveres fra CERT-strukturen får mer operativ bistand til gjennomføring av nødvendige sikkerhetstiltak.

En mulighet og utfordring med regional etablering er modenheten i den enkelte kommune. En etablering av tjenester på regionalt nivå må adressere mottakskommunenes kompetanse og kapasitet. Erfaringer fra CERT-strukturen tilsier at flere kommuner har store utfordringer med konsumering og respons på tjenestene som leveres, ofte omtalt som manglende konsumeringsevne. Dersom regionale SOC etableres må det ta høyde for at kommunene vil ha, særlig i oppstartsfasen, betydelig bistandsbehov. Dersom det etableres nok kapasitet på regionalt nivå, vil det trolig medføre at kommunene får mer operativ bistand og blir i større grad satt i stand til å konsumere SOC-tjenester. Det kan også få positive konsekvenser for konsumeringsevnen av CERT-tjenester.

En mulig utfordring med etablering av et regionalt SOC kan være finansiering. Det er behov for finansiering til etablering, drift og vedlikehold. En regional plassering av SOC vil medføre kostnader for den enkelte kommune, og finansieringsmodell for tjenesten må vurderes. Finansiering av et SOC er dermed avhengig av at kommunene som tilknyttes har budsjettmidler og prioriterer å benytte disse på en slik tjeneste.

En annen utfordring med regional SOC er modenheten i regionen, og evnen digitaliseringsnettverkene har til å opprette en ny tjeneste og funksjon som SOC. Det må derfor påberegnes en oppstartsfase ved valg om etablering av regionale SOC, og det kan være regionale forskjeller og muligheter avhengig av kapasitet og modenhet i regionen. Dette henger også tett sammen med finansiering og økonomisk mulighet til etablering og drift.

Nasjonal SOC for kommunal sektor

Med nasjonal SOC for kommunal sektor, menes det at det etableres én SOC som skal betjene hele kommunal sektor. Siden det er betydelige muligheter for stordriftsfordeler ved å sentralisere SOC vil det være naturlig å vurdere om et sentralt SOC for alle norske kommuner kan være hensiktsmessig.

Det er nærliggende at en slik nasjonal SOC etableres i tilknytning til en CERT, og kan etablere tett samarbeid med CERT-funksjonen. Det kan også være et alternativ at en slik nasjonal SOC etableres i forbindelse med opprettelsen av en virksomhet for digitale fellestjenester i regi av KS. I utredningen for KS's digitale fellestjenester (DIF) skrives det blant annet det kan vurderes om DIF kan tilrettelegge

for å ivareta felles kommunale sikkerhetsfunksjoner.[2] Dersom nasjonal etablering av SOC tilknyttes DIF, vil også medlemskommunene være deleiere i selskapet og kan og skal ha påvirkning på tjenestene som leveres fra selskapet.

En SOC-tjeneste krever som beskrevet tidligere ikke lokal og/eller fysisk tilstedeværelse, noe som åpner for en sentral plassering og etablering av et større fagmiljø. Et sterkt og uniformt kompetansesenter vil trolig være en attraktiv arbeidsgiver, og har flere av de samme mulighetene som beskrevet under regional etablering. Også her vil kommunene samarbeide og nyttiggjøre seg av attraktiv kompetanse, fremfor å konkurrere om ressursene.

En utfordring med etablering av et nasjonalt SOC, er tilsvarende som for regionalt nivå – modenheten og konsumeringsevnen til mottakskommunen. Tilsvarende som ved etablering av regionalt nivå, må det tas høyde for at nasjonalt SOC må ha kapasitet til å følge opp mottakskommunene. Avstanden fra den enkelte kommune til nasjonalt nivå må adresseres, og det kan være utfordrende for den enkelte kommune å nyttiggjøre seg av en nasjonal tjeneste dersom ikke nødvendig operativ bistand er tilstrekkelig og tilgjengelig. Denne utfordringen rapporteres det om fra CERT-strukturen i dag, og må adresseres ved eventuelt valg om etablering av SOC-tjenester på nasjonalt nivå.

Finansielt vil også en nasjonal SOC være avhengig av økonomiske midler, og være avhengig av at kommunene prioriterer kostnaden en slik tjeneste vil påføre dem. Kostnaden vil likevel være mye mindre enn ved særlig lokal etablering eller kommersiell tilknytning. Dersom nasjonal SOC etableres i forbindelse med selskap for digitale fellestjenester, kan finansiering ses på i forbindelse med dette og dermed være en del av sentral finansiering.

En annen utfordring med nasjonal SOC er innsikt og kompetanse om lokale forhold, som henger tett sammen med utfordringen om konsumeringsevne og avstand. Det er også et spørsmål om kapasitet og volum, og om det er mulig å etablere et SOC som kan håndtere volumet til samtlige kommuner i Norge. For hele sektoren vil det være millioner av enheter i heterogene infrastrukturer der trusler i en lokal infrastruktur vanskelig kan aggregeres og dermed ageres på sentralt. Ved etablering nasjonalt, kan denne situasjonen dermed medføre et behov for å dele opp i regionale enheter og/eller mindre enheter for bistand til mottakskommunene.

De største fordelene med nasjonal etablering er et større, sentralt fagmiljø som kan etablere felles malverk- og deteksjonsregler for kommunal sektor. De samme fordelene vil også gjelde for finansiering, og det kan oppnås betydelige stordriftsfordeler ved nasjonal etablering.

Kommersiell SOC – kjøp av SOC fra kommersielle aktører

Med kommersiell SOC menes private og kommersielle aktører som leverer SOC-tjenester til betalende kunder. De private aktørene har de samme rammevilkårene som beskrevet over når det gjelder behov for kompetanse og tilhørende driftskostnader, men har som hele eller deler av sin inntjeningsmodell å dele kostnaden på flest mulig aktører.

Fordelen med å gå inn på SOC-tjenester som rent tjenestekjøp er flere. Først om fremst muligheten til å unngå en initial investeringskostnad og fra første dag dele driftskostnaden med flere andre. Kommersielle aktører har allerede etablert tjenestekataloger med beskrevet tjenestekvalitet, noe

[2] KS digitale fellestjenester – konseptutredning. Tilgjengelig fra: https://www.ks.no/globalassets/fagomrader/digitalisering/digitaliseringsstrategien/KS-digitale-fellestjenester-Konseptutredning-versjon-1-0-11-05-2022-2-.PDF, s. 24.

som kan være en fordel for å kunne vurdere om kostnadene kommunene pådrar seg står i forhold til de tjenestene som blir levert.

Kvalitet på tjenesteleveransen kan likevel være vanskelig å bedømme utelukkende ut fra kvantitative vurderinger - åpningstider, responstid vil for eksempel ikke nødvendigvis reflektere behovet til kommunal sektor. Som ved alle andre kommersielle anskaffelser med flere kjøpere utenfor sektor vil det være varierende grad og mulighet til påvirkning av tjenesteleveransen.

En eventuell del- eller fullverdig tjenesteutsettelse av SOC for kommunal sektor må risikovurderes. Det kan blant annet være avhengighet til kommersielle aktører, kapasitet ved hendelser hos samtlige kommuner, kommersielle interesser- og utfordringer, e.g lønnsomhet.

Utfordringene ved kjøp av SOC-tjenester fra kommersiell leverandør er flere. En av disse observeres allerede konturene av blant kommunene: Kommunal sektor bygger opp egen kompetanse innen SOC-relaterte tjenester som deretter blir rekruttert til kommersielle leverandører for at disse skal kunne levere tjenester til kommunen. Denne problemstillingen er ikke ukjent på andre kompetanseområder, men kommer særlig til uttrykk på dette området siden det allerede er et betydelig underskudd på kompetanse. Lokalkunnskap vil i liten grad være til stede innledningsvis ved et tjenestekjøp fra en kommersiell aktør, og i den grad de opparbeides er det ikke garanti for at kommunen får tilgang til den.

En annen utfordring som vil kunne føre til unødige forsinkelser i deteksjon og mindre mulighet for uttak av stordriftsfordeler er at samarbeid mellom kommersielle SOC'er naturlig nok bare vil finne sted dersom det er kommersielt begrunnet. Dette er trolig også noe av forklaringen i observasjonen Ponemon Insititute gjorde i 2020: «From a financial point of view, a 2020 Ponemon Institute study, conducted on 637 professionals, revealed that the average maintenance cost of an internal SOC for a company with between 1,000 and 5,000 employees is as high as $1.68 million. Interestingly, the ROI of an outsourced SOC decreases as the company grows, with a higher average cost for the outsourced one than for the internal one, if we take into account all the companies surveyed ($2.86 million versus $4.44 million) »[3].

[3] https://www.ponemon.org/research/ponemon-library/security/the-state-of-soc-effectiveness-signs-of-progress-but-more-work-needs-to-be-done.html

Drøfting av alternativene

Som beskrevet i dette dokumentet, er det flere alternativer for kommunal sektor for etablering og/eller tilknytning til en SOC-funksjon. Basert på vurderingskriteriene kompetanse og økonomi, kan det oppsummert fremstilles i følgende tabell:

	Kompetanse	**Økonomi**	**Kunnskap om lokale forhold**	**Respons/reaksjonstid**	**Volum**
Lokal	Ingen gjenbruk eller overlapp. Liten mulighet til å etablere større kompetansemiljø. Kompetanse internt nødvendig.	Høye kostnader for kommunen, ingen å dele kostnaden med.	God kunnskap om lokale forhold. Full gjenbruk av kompetanse.	Svært rask responstid ved tilstrekkelig bemanning.	Mulighet til å håndtere internt volum.
Regional	Mulighet for etablering av større kompetansemiljø. Et stort fagmiljø samlet i et kompetansesenter vil høyst sannsynlig være en attraktiv arbeidsgiver. Noe kompetanse om lokale forhold. Samarbeid mellom regionene mulig.	Stordriftsfordeler.	Stor grad av kunnskap om lokale forhold, kjennskap til nøkkelpersonell og til kommunal sektor. Gjenbruk av kompetanse mulig. Mottakskommunen må ha konsumeringsevne av tjenesten.	Rask responstid ved tilstrekkelig bemanning, mulighet for døgnbemannet tjeneste.	Mulighet til å håndtere regionalt volum.
Nasjonal/sentral	Mulighet for etablering av et betydelig kompetansemiljø. Et stort fagmiljø samlet i et kompetansesenter vil høyst sannsynlig være en attraktiv arbeidsgiver. Svak kompetanse om lokale forhold.	Betydelige stordriftsfordeler.	Kunnskap om kommunal sektor, mindre kjennskap til lokale forhold, eks. infrastruktur i den enkelte kommune. Lav gjenbruk av kompetanse. Mottakskommunen må ha konsumeringsevne av tjenesten.	Rask responstid ved tilstrekkelig bemanning, mulighet for døgnbemannet tjeneste.	Utfordringer med å håndtere nasjonalt kommunalt volum.
Kommersiell	Mulighet for etablering av større kompetansemiljø. Lite eller mangelfull kompetanse blir værende i kommunal sektor.	Stordriftsfordeler mulig, men prismodell ofte volumbasert. Store individuelle kostnader per kommune.	Innledningsvis liten grad av kunnskap om lokale forhold, må påberegnes en etableringsperiode for opparbeidelse av kunnskap om lokale forhold. Lav gjenbruk av kompetanse Mottakskommunen må ha konsumeringsevne av tjenesten.	Rask responstid ved tilstrekkelig bemanning, mulighet for døgnbemannet tjeneste.	Mulighet til å håndtere volum med avtalepart.

Som tabellen viser, er det fordeler og utfordringer ved samtlige skisserte alternativer. Felles for alle alternativene er at det kreves investeringer (noe mindre for det kommersielle alternativet enn for de andre) og sikring av fremtidige driftskostnader. Disse midlene må nødvendigvis prioriteres i de kommunale budsjettene. Avhengig av prioritering i budsjettene vil det naturligvis være en begrensning og/eller mulighet til hva den enkelte kommune har anledning til å etablere selv eller hente tjenester fra.

Det generelle utfordringsbildet til sektoren er tilgang på nok og riktig kompetanse på området, og denne utfordringen deles i hele det norske samfunn, inkludert hos kommersielle aktører. Det er derfor også en fellesnevner som vil kunne være en begrensning og/eller mulighet for alle alternativene.

Det som er økonomisk mest belastende for den enkelte kommune er etablering av en lokal SOC-funksjon. Særlig de små og middelsstore kommunene vil ha store økonomiske og faglige utfordringer med en lokal etablering. Det er også erfaringsvis økonomisk belastende med anskaffelser av SOC-tjenester fra en kommersiell aktør, og det vil uansett være en periode med merbelastning for kommunen ved implementering og oppstart. Det er også viktig å påpeke at ved full tjenesteutsettelse vil det være behov for lokal kompetanse, og kommunen må fremdeles dekke et minimums behov for beredskaps- og hendelseshåndtering, samt kjennskap til lokale organisatoriske og tekniske forhold.

Behovet og tilgangen for kompetanse i kommunal sektor vil vedvare, og ved omfattende bruk av kommersielle aktører, vil det medføre en risiko for at kompetansen ikke kan rekrutteres eller beholdes i kommunal sektor. Ved etablering av lokale, regionale eller nasjonale SOC-funksjoner i regi av kommunene selv, kan dette sees på som egeninvestering i kompetanse.

Ved etablering av regionale kommunale SOC-funksjoner kan økonomiske midler være en gjeldende utfordring. Ved et slikt alternativ vil det også være behov for finansiering til etablering og drift av funksjonen. Det kan derimot oppnås stordriftsfordeler i forbindelse med anskaffelse av verktøy, lønnskostnader og lokasjonskostnader. Ved regional etablering kan det bidra til å styrke kommunal sektors attraktivitet som arbeidsgiver, og kunne tilby et større fagmiljø med et viktig samfunnsoppdrag. Det kan også bidra til at kommunal sektor ikke konkurrerer om samme kompetanse, men kan dele og nyttiggjøres av kompetansen. Det er også ved dette alternativet avhengig av at den enkelte kommune kan dekke et minimums behov for beredskap- og hendelseshåndtering.

Alternativet med nasjonal SOC vil gi betydelige stordriftsfordeler, og ha mange av de samme muligheter som ved etablering regionalt. Et nasjonalt SOC gir mulighet for utvikling av felles deteksjonsregler og malverk for hele kommune-Norge, som kan medføre et mer uniformt sikkerhetsarbeid i kommunal sektor. En slik etablering vil kunne medføre utfordringer med tanke på den enkelte kommunes konsumeringsevne, og en slik funksjon må dermed etablere tilstrekkelig kapasitet og operativ bistandsevne. Det er også mulige utfordringer med volum, omfang og lokal kjennskap.

Anbefaling

Faggruppen anbefaler at kommunal sektor omforenes om en modell for etablering av og/eller tilknytning til SOC initialt med den viktigste funksjonaliteten knyttet til deteksjonsregler og

alarmering på disse. Dette er også viktig med tanke på oversikt over hvilke kommuner som har hvilke samarbeid, og informasjonsbehovet for andre aktører som KS, NSM, Datatilsynet og CERT-strukturen måtte ha i forbindelse med forebygging, oppdaging og håndtering av hendelser. Det er viktig med tydelige ansvarsforhold og definerte tjenesteleveranser, og at modellen forankres hos relevante aktører. Finansieringsmodell må også avklares i en tidlig fase.

Ved alle alternativene må det påberegnes at tjenesten som skal etableres eller tilknyttes ikke kan etableres som en fullverdig tjeneste umiddelbart. Dettes skyldes blant annet behovet for å rekruttere og etablere et kompetansemiljø, onboarding av mottakskommunene, avklaringer av tjenestene som skal leveres og finansieringsmodell. Det er derfor hensiktsmessig at ved en kommunal etablering regionalt eller nasjonalt, må slik etablering først fokusere på minimumstjenester, og kan bygge ut tjenestespekteret over tid. Det må trolig også påberegnes noe tid før alle mottakskommunene er tilknyttet en slik tjeneste. Målet må likevel være at hele kommunal sektor er tilknyttet en sikkerhetsovervåkningsfunksjon, som øker modenheten for hele sektoren.

Basert på skisserte utfordringer i kommunal sektor, er det ikke hensiktsmessig at den enkelte kommune etablerer SOC lokalt og individuelt. Basert på skisserte utfordringer er det heller ikke hensiktsmessig at den enkelte kommune kjøper SOC-funksjoner av kommersielle aktører.

For å kunne i imøtekomme sektorens utfordringer i fremtiden, både med tanke på økonomi og tilgang på kompetanse, er det mest nærliggende at enten regional eller nasjonal SOC etableres for kommunal sektor. Ved begge alternativene er det muligheter, og i stor grad like utfordringer. Det er særlig den enkeltes kommunes konsumeringsevne som er en utfordring ved sentralisering av tjenester, og som må adresseres ved etableringen. Arbeidsgruppen anbefaler en to-delt løsning som kan imøtekomme utfordringene med kompetanse og konsumeringsevne:

- *det etableres en nasjonal alarmsentral, SOC,* fortrinnsvis tilknyttet til DIF eller en CERT, med den viktigste funksjonaliteten tilknyttet deteksjonsregler og alarmering på disse.
- *det etableres en regional operativ bistand tilknyttet nasjonal alarmfunksjon* for lokal bistand til mottakskommunene. Faggruppen anbefaler videre at den regionale bistanden etableres i digitaliseringsnettverkene, og sees i sammenheng med foreslått opprettelse av regionale sikkerhets- og kompetansesenter i kommunal sektor.