Vedlegg A – Detaljert oversikt over foreslåtte tiltak

Innhold

Innledning

Anbefalingene i denne utredningen er avgrenset til tiltak for å beskytte og opprettholde funksjonsevnen til kommunal sektor ved digitale angrep og hendelser. Tiltak for å sikre funksjonsevne mot fysiske angrep omhandles derfor ikke. Psykologiske angrep i påvirkningsøyemed, og hvor formålet er å endre demokratiutvikling, samfunnsstyring, samfunnsutviklingen eller rettsikkerhet, omhandles heller ikke.

Det presiseres at anbefalte tiltak ikke løser alle utfordringene med digital robusthet i kommunal sektor, men er de tiltakene som vurderes som de viktigste i nåværende situasjon. Digital transformasjon er dynamisk både i hastighet og retning, og nye tiltak må derfor vurderes kontinuerlig.

Vedlegget er inndelt i 2 hoveddeler:

1. Aktiviteter som bør gjennomføres i den enkelte kommune.
2. Utdyping av tiltak anbefalt i rapporten.

Den første delen omhandler aktiviteter som er eller burde allerede vært innført i alle kommuner. Disse aktivitetene imøtekommer de behovene kommunene har signalisert[1], men rettes tilbake til den enkelte kommune ut fra det ansvaret kommunen har. Flere av aktivitetene sammenfaller i står grad med NSM grunnprinsipper fro IT-sikkerhet og det henvises til disse når det gjelder innbyrdes prioritering[2].

Den andre delen, utdyping av tiltak anbefalt i rapporten, er som navnet tilsier en utdyping av tiltakene i hovedrapporten med:

- Prioritet: Tiltakene er prioritert etter vurdert kritikalitet og nytte for kommunal sektor.
- Beskrivelse av selve tiltaket: Tekst som beskriver selve tiltaket.
- Forventet effekt: Effekt i form av forventet observert endring i situasjon etter at tiltaket er gjennomført.
- Når tiltaket bør gjennomføres: Anbefaling og tidsrom for gjennomføring.
- Kostnadsestimat: Overordnet vurdering av kostander som vil påløpe ved innføring av tiltaket.
- Forslag til finansieringsmodell

Beskrivelsen av de ulike finansieringsmodellene er plassert bakerst i dette vedlegget.

[1] Vedlegg E

[2] https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

Aktiviteter som bør gjennomføres i den enkelte kommune i henhold til ansvar

Aktivitet	**Forventet effekt**	**Kostnadsestimat ut fra vurdering av dagens situasjon**
Vurdere egen modenhet opp mot NSM Grunnprinsipper for IKT-sikkerhet	Gir situasjonsforståelse til kommunens politiske og administrative ledelse. Gir godt grunnlag for prioritering av kommunens tiltak.	Kostnaden for en modenhetsvurdering avhenger av kommunens modenhet på området. Basert på erfaringstall vil det ved bruk av eksterne ressurser koste mellom 300’ og 2.500’ NOK for en modenhetsvurdering avhengig av kommunal størrelse.
Etablere metoder og verktøy for å tilgjengeliggjøre situasjons- og risikobeskrivelse innen sikkerhets-, beredskaps- og personvernområdet for administrativ og politisk ledelse, og sikre oppfølging.	Bedre innsikt og forståelse for kommunens risiko, og bedre oversikt og mulighet for prioritering av tiltak innen informasjonssikkerhet og personvern i kommunen.	De aller fleste kommuner har allerede etablert et minimum av internkontroll med avviks- og hendelsesrapportering, ledelsens gjennomgang osv., og vil dermed kunne inkorporere de omtalte områdene i eksisterende strukturer. Måling og rapportering vil for noen kommuner komme i tillegg, kostnadene for dette er innarbeidet i kompetansepunktet.
Gjennomføre sårbarhetsreduksjon og etablere «sikkert» oppsett av sentrale gjennomgående sektorsystemer, herunder innføre NSMs «Fem effektive tiltak mot dataangrep».	Vesentlig lavere sannsynlighet for å bli rammet av digitale angrep: "*NSM har i flere tiår utviklet tekniske sikkerhetstiltak for beskyttelse av IKT-systemer. Ut fra disse erfaringer ser vi at virksomheter kan stanse de fleste dataangrep med følgende tiltak*"	Den enkelte kommune har ulike status på disse områdene. Kostnaden vil derfor variere betydelig, fra 0 til nærmere 1 MNOK for noen kommuner. I all hovedsak vil kostnadene komme i forbindelse med bistand til etablering av hvitelisting av programvare og fjerning av lokal administrator fra endepunktsutstyr.
Sikre at tilstrekkelig strategisk kompetanse innen informasjonssikkerhet, personvern og beredskap er tilgjengelig.	Alle aktiviteter listet her vil ha økt positiv effekt på kvalitet i gjennomføring med tilstrekkelig strategisk kompetanse involvert innen de nevnte fagfelt.	For kommuner som allerede har denne kompetansen tilgjengelig vil det ikke tilkomme noen kostnader, mens det for en rekke kommuner måtte etableres funksjoner som ivaretar kompetansebehovet. Vurderes til minimum 1 stilling i små kommuner, 2-4 i mellomstore kommuner.

Aktivitet	Forventet effekt	Kostnadsestimat ut fra vurdering av dagens situasjon
Vurdere status for gjennomførte ROS/DPIA på sentrale fagsystem og behandlinger. Gjennomføre ROS/DPIA på sentrale fagsystem og behandlinger der dette ikke er utført.	Økt oversikt over nødvendige tiltak som må gjennomføres for å oppnå et tilstrekkelig sikkerhetsnivå. Vurderingene er en av nøkkelkomponentene i internkontroll, og vil vesentlig forbedre kommunens evne til styring på informasjonssikkerhetsfeltet. Det vil også gi en oversikt over risiko og nødvendige tiltak.	Den enkelte kommune har ulike status på disse områdene. Kostnaden vil derfor variere betydelig.
Etablere og vedlikeholde teknologiske sikkerhetskrav, samt opprette leverandørdialog.	Trygghet for at nødvendige/tilstrekkelige krav stilles til leverandører ved anskaffelse, samt bidra til at leverandører er kjent med hvilke krav og behov som vil bli fremmet over tid.	Første gangs etablering av krav vil ha en kostnadsramme på ca 150.000, deretter mindre kostnader i forbindelse med løpende oppdatering. Den enkelte kommune har ulik status på dette området, og kostnaden vil derfor variere noe.
Revidere sentrale leverandører på informasjonssikkerhetsområdet	Trygget for at leverandører leverer tjenester og produkter i henhold til de kravene kommunen har fremsatt	Den enkelte kommune har ulike status på dette området. Kostnaden vil derfor variere etter status og antall sentrale leverandører.
Etablere tilknytning til CERT, tilknytning eller opprettelse av SOC og IRT, herunder etablere rutiner for håndtering av tilknytningen (varsler, alarmer etc.).	Vesentlig bedret evne til å: 1. Forebygge hendelser gjennom sårbarhetsreduksjon 2. Oppdage hendelser på et tidlig stadium 3. Reagere på en effektiv måte 4. Håndtere en pågående hendelse	Ekstern kost: Løpende kostnad for kjøp av SOC/IRT som tjeneste på 8 MNOK årlig (5 MNOK for SOC, 3 MNOK for IRT) for en gjennomsnittlig kommune. Laveste kostnad for tilknytning til CERT er minimum 0,05 MNOK årlig for en gjennomsnittlig kommune. Intern kost: 1 MNOK for etablering og drift av mottaksapparat for kommunen.
Etablere og forvalte beredskapsplanverk, herunder gjennomføre øvelser.	Trygghet for at kommunen er i stand til å håndtere alvorlige IKT-hendelser.	Første gangs oppdatering av beredskapsplan vil ha en kostnadsramme på ca 150.000, deretter mindre kostnader i forbindelse med løpende oppdatering og øvelser. Den enkelte kommune har ulik status på dette området, og kostnaden vil derfor variere noe.

Aktivitet	Forventet effekt	Kostnadsestimat ut fra vurdering av dagens situasjon
Utvikle og gjennomføre tilpasset kompetansehevingstiltak for politisk og administrativ ledelse, brukere og teknisk/støtte-personell.	Tilstrekkelig kompetanse i kommunen til å vurdere risiko og prioritere tiltak, evne etablert i kommunen til å håndtere alvorlige IKT-hendelser.	Opplæringspakker og gjennomførings av disse til de forskjellige gruppene/rollene vil for en gjennomsnittskommune trolig ha en kostnadsramme på 1MNOK, deretter mindre løpende kostnader ifm med oppdatering. Kostnadene vil variere med kommunens størrelse.

Utdyping av tiltak anbefalt i rapporten

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
1	1	Kommuner i og utenfor eksisterende diginettverk og IKT-samarbeid, anbefales å etablere en regional cyber sikkerhets- og kompetansesenter i sitt nedslagsfelt (RCSK).	Samarbeidsprosjekt mellom deltagende kommuner, i samarbeid med digitaliseringsnettverkene. Må kunne utvikles i tråd med føringer og rammer gitt av den nasjonale samstyringsstrukturen	Behovet for operativ bistand kan svares ut ved at kommunal sektor etablerer egne regionale cyber sikkerhets- og kompetanseenheter (RCSK) som tilbyr operativ bistand og tjenester. Det kan sikre at alle kommuner, gitt de ønsker å tilkoble seg tjenesten(e) som etableres, øker modenheten og robustheten. RCSK kan utføre mange kostnads-, kompetanse-, og kapasitetskrevende oppgaver på vegne av kommunene og fylkeskommunene i regionen. RCSK vil også kunne avlaste sentrale aktørers pågang ved at de fungerer som bindeledd og kan gi bistand til den enkelte kommune. Det vil dermed kunne avlaste og effektivisere den offentlige forvaltningen innen trygg digitalisering. Det vil også gi positive ringeffekter for samstyringsstrukturen da RCSK kan bistå og bidra til å operasjonalisere føringer og prosjekter utviklet og delegert gjennom samstyringsstrukturen.	Påstarte arbeidet i 2023.	Kartlegging estimeres til 2 MNOK	Selvfinansieres

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
1	2	Vedta prinsipper for informasjonssikkerhet, personvern og i digital beredskap for kommunal sektor i samstyringsstrukturen (DU/KommIT)	KS og samstyringsstrukturen	Oppnå helhetlig forankring og samordning med arbeidet med informasjonssikkerhet, personvern og beredskap i kommunal sektor.	2023	0	Ikke relevant
1	3	Arbeide for å få etablere et kommunalt sektorvis responsmiljø.	Regjeringen har ansvaret for å peke ut og etablere. KS og samstyringsstrukturen må bidra til at Regjeringen peker ut.	Etablering av et SRM for kommunal sektor sikrer en økt samlet evne til å oppdage, respondere og håndtere hendelser raskere enn i dag. Dette skal igjen bidra til økt robusthet i hele kommunal sektor uavhengig av modenhetsnivå hos kommunene og øke dere evne til å forebygge, oppdage og håndtere digital angrep og hendelser.	Utpeking av kommunal SRM bør skje i 2023.	50 MNOK (sentralt) årlig. I tillegg vil det påløpe kostnader pr kommune for å håndtere tilkobling til SRM. Dette vil avhengig av kommunens størrelse.	Bør grunn-finansieres gjennom statsbudsjettet.

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
1	4	Utrede etablering av kommunal cyber sikkerhets- og kompetansesenter (KCSK) med utvidet tjenestespekter tilpasset kommunenes behov.	Kommunal sektor	Ved etablering av KCSK, kan det dekke kommunenes behov for bistand til leverandøroppfølging, økt bestillingskompetanse og revisjon av sentrale og store leverandører i og til kommunal sektor. Videre vil det kunne svare ut behovet om etablering/tilknytning SOC og IRT, og en fordeling av kostnader. Etableringen av et kommunalt SRM og KCSK vil bidra til økt motstandsevne, informasjonsflyt og at sektoren har ett fagmiljø som bistår med forebygging, oppdagelse og håndtering av hendelser.	Utredning av KCSK bør påstarte vår 2024.	Utredning av KCSK er beregnet til ca 2.0 MNOK.	Grunnfinansieres
1	5	Vurdere fagrådenes rolle, sammensetning, funksjon, saksflyt og organisering for å få en helthetlig tilnærming til digitalisering og da spesielt områdene arkitektur, sikkerhet, beredskap og personvern.	KS med kommunal sektor.	Tiltaket skal forbedre sektorens evne til å føre og beslutte tverrfaglige problemstillinger, prosjekter og saker. Det vil bidra til å understøtte digitaliseringsstrategiens mål. Og som en forlengelse av dette, kunne spille en avgjørende rolle for god beslutningsstøtte og være med på å utbre digitalisering til kommunal sektor på en trygg måte, slik at kommunal kan digitalisere raskere på en trygg og sikker måte.	Arbeidet bør påstartes høst 2023.	Utredning 1 MNOK	Kostfordeles gjennom KS medlemskontingent

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
1	6	Vurdere forslaget om styrking av sekretariatsfunksjon i samstyringsstrukturen i KS. Tiltak 5 må ses i sammenheng med tiltak 4.	KS	Styrking av sekretariatsfunksjon vil medføre forenklet saksflyt, koordinering i og mellom samstyringsstrukturen, kommunene og KS. Det kan også avlaste fagrådsmedlemmene.	2024	3 MNOK årlig.	Kostfordeles gjennom KS medlemskontingent
1	7	Utarbeide felles kommunale sikkerhetskrav, både til eksterne leverandører og til den enkelte virksomhet, herunder forenkle og ta i bruk markedsplassen for skytjenester for kommunal sektor. Tilgjengeliggjøres for kommunal sektor, og oppdateres årlig av aktører med ansvar for å utarbeide og forvalte sikkerhetskravene. Tiltaket ses i sammenheng med tiltak 8.	KS og DFØ	Lette og forenkle arbeidet med utvikling av sikkerhetskrav til eksterne leverandører og til egen virksomhet. Gi kommunene et bedre og samlet utgangspunkt i forhandlinger med store leverandører. Redusere anskaffelser av sårbare løsninger i kommunal sektor, og øke evnen til å drifte og forvalte løsninger på en sikker måte. I samarbeid med DFØ legge til rette for at kommunal sektor lettere kan ta i bruk markedsplassen for skytjenester.	Oppstart 2024	3 MNOK for å utarbeide første utkast, og deretter 2 mill for å vedlikeholde kravene. Legge til rette for å ta i bruk markedsplassen øver DFØ sitt budsjett.	Grunnfinansieres

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
1	8	Delta i Digitaliseringsdirektoratet initiativ «Felles sikkerhet i forvaltningen med ressurser fra kommunal sektor. KS i samarbeid med samstyringsstrukturen avsetter ressurser for å bidra til dette arbeidet.	Digitaliseringsdirektoratet.	Formålet vil være å samordne og sammenstille tilgjengelige krav, veiledninger og tiltak innenfor fagområdene, med hensikt om å tilby helhetlig veiledning til kommunal sektor. Veiledningen vil bli spisset og bedre innrettet mot kommunal sektor. Samordning og sammenstilling av krav, veiledning og tiltak kan bidra til mer helhetlig tilnærming og veiledning, som kan medføre en bedre situasjonsforståelse. Dette vil også lette den enkeltes kommunes ressursbruk i utarbeidelsen av veiledning og omsetning av eksisterende veiledere.	Påstarte arbeidet i 2023.	2 MNOK årlig.	Grunnfinansieres
1	9	Øke samordning med KiNS.	KS/KiNS	Oppnå en felles enighet om grensegangen mellom ansvars- og oppgavefordelingen mellom KS og KiNS, deriblant hvem som representerer kommunal sektor i ulike fora.	2023 – Løpende	300.000 NOK for å utarbeide felles ansvarslinjer.	Kostfordeles gjennom KS medlemskontingent

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
2	10	Gjennomføre sentrale vurderinger av systemer og behandlinger (ROS/DPIA). Det anbefales at Microsoft M365 og Google og andre sentrale systemer som store deler av kommunal sektor prioriteres først.	KS i samarbeid med kommunene	Det anbefales at M365 og Google prioriteres først som følge av at både Microsoft og Google er en stor leverandør i kommunal sektor. Gjennomføringen av sentrale vurderinger skal bidra til at alle kommuner har nødvendige forutsetninger til å ivareta sitt ansvar og overholde regelverket (GDPR). Videre vil det gi kommunene et bedre utgangspunkt for forhandlinger med store leverandører. Utarbeidelsen og tilgjengeliggjøringen av vurderinger av sentrale system vil også bidra til at kommunene får oversikt over risiko og sårbarheter, som kan benyttes som grunnlag inn i de vurderingene kommunene må gjennomføre i egen virksomhet. Tiltaket skal resultere i et helhetlig rammeverk og veiledning for gjennomføring av ROS og DPIA i kommunal sektor.	Oppstart 2023	2 MNOK for vurdering av M365 og etablering av rammeverk for vurderinger Google – se SkoleSec prosjektet. Det må settes av ca 5 mill årlig for å gjennomføre ROS på sentrale systemer.	Kostfordeles gjennom KS medlemskontingent

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
2	11	Utvikle kompetansetiltak for kommunal sektor for ansatte, fagpersonell, politisk ledelse og administrativ ledelse innen digitalisering, sikkerhet, beredskap og personvern.	Digitaliseringsdirektoratet og KS i samarbeid.	Målrettet opplæring som treffer den ansatte i sine arbeidsoppgaver og virksomhet vil bidra til at ansatte er et ledd ut av det forebyggende arbeidet med informasjonssikkerhet, personvern og digital beredskap. Kompetansetiltak rettet mot fagpersonell vil sikre at kommunene har oppdatert og riktig kompetanse innen fagfeltene, og slik ha personell til å iverksette nødvendige tekniske og organisatoriske tiltak for å møte trusselbildet og utfordringene kommunene står ovenfor i dag. Kompetanseprogram rettet mot politisk og administrativ ledelse vil øke styringskompetansen, både politisk og administrativt. Det vil igjen bedre kommunenes forutsetninger til å utøve sitt ansvar og oppfylle krav om internkontroll i egen virksomhet. Kompetanseprogrammet bør innrettes i to deler, en spesifikt for politisk ledelse og en spesifikt for administrativ ledelse.	Oppstart 2024 - løpende aktivitet	2 MNOK årlig.	Grunnfinansieres

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
2	12	Utrede "Påvirkning i det digitale rom" med hensikt om å tilegne seg nødvendig innsikt i hvordan påvirkningskampanjer i det digitale rom kan påvirke kommunal sektors evne til å ivareta demokratiske prosesser, tillit i samfunnet og tjenesteleveranser.	KS	Utredningen bør sette søkelys på hvordan offentlig sektor generelt, og kommunal sektor spesielt, kan forebygge og forhindre at påvirkningskampanjer skader tilliten til institusjoner og demokratisk styring. Skal skape et kunnskapsgrunnlag for å sikre at kommunal sektor øker sin evne til å ivareta demokratiske prosesser, tillit i samfunnet og til tjenesteleveranser.	2024	Utredning 4 MNOK	Midler søkes gjennom KS's FoU-ordning
2	13	Utrede «personvern i kommunal sektor» for å skaffe innsikt i hvordan kommunal sektor kan tilnærme seg personvern på en god måte i det dynamiske teknologiskiftet.	KS	Nye teknologier, f.eks. maskinlæring (AI), ulike sosiale media, tverrsektorielle systemer (delt behandlingsansvar) mv gir utfordringer innen personvern som må adresseres på en rett måte. Det er derfor avgjørende at kommunal sektor kan tilnærme seg personvern på en god måte i det dynamiske teknologiskiftet. I tillegg er det viktig at man har en god tilnærming til dette området slik at digitalisering kan skje på en god og rask måte. Alternativt er at personvern vil kunne sinke takten på digitalisering i kommunal sektor.	2024	Utredning 4 MNOK	Midler søkes gjennom KS's FoU-ordning

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
3	14	Vurdere å etablere en nasjonal virtuell operativ kommunal sikkerhetsorganisasjon.	KCSK eller RCSK, eventuelt Kommunalt SRM i fravær av RCSK eller KCSK.	Formålet med organisasjonen er å mobilisere riktig og viktig kompetanse til riktig tid på tvers av sektoren for å bistå med håndtering av hendelser. Oppnå mer effektiv ressursbruk på tvers av sektoren, og bidra til at den enkelte kommune kan få faglig bistand av eksisterende ressurser i sektoren til å håndtere hendelser, eller motta tidlig varsling av hendelser i andre kommuner.	2025	2 MNOK	Grunnfinansiering

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
3	15	Vurdere å tilgjengeliggjøre kompetanse inn i felles nasjonale digitaliseringsprosjekter finansiert gjennom DigiFin. Dette for å understøtte nye felles digitaliseringsprosjekter finansiert av DigiFin med fagkompetanse innen arkitektur, informasjonssikkerhet, beredskap og personvern.	KS	Tiltaket skal sikre at arkitektur, informasjonssikkerhet, digital beredskap og personvern innlemmet i digitaliseringsprosjektene finansiert gjennom ordningen DigiFin. Det skal sikre en helhetlig tilnærming til digitalisering ved utviklingen av nye digitaliseringsprosjekter hele sektoren har nytte av. Ressursene skal være tilgjengelig for samstyringsstrukturen, men bør formelt være tilkoblet KS, slik at hele samstyringsstrukturen kan nyttiggjøre seg av dem. Det vil kunne bidra til at nye digitaliseringsinitiativ- og prosjekter bidrar til at sektoren hensyntar behovene for integrert sikkerhetsarbeid, og ikke innfører nye, utilsiktede risikoer i sektoren. Det vil også være en mulighet for å ytterligere dele på utviklings- og forvaltningskostnadene. Videre vil tidlig involvering i konsept- og utviklingsfasene bidra til at digitaliseringsprosjektene står langt bedre rustet i en gjennomføringsfase.	2024	3 MNOK årlig.	Kostfordeles gjennom KS medlemskontingent

Pri	Tiltak	Tiltak	Organisering/ansvar	Forventet effekt	Tid	Kostnads-estimat	Finansierings-modell
4	16	Fagområdene personvern, informasjonssikkerhet og digital beredskap innarbeides i ulike digitaliseringsstrategier i kommunal sektor. Digitale strategier bør adressere digital sikkerhet, beredskap og personvern for å sikre trygg digitalisering i kommunal sektor.	Aktører med ansvar for utarbeidelse av digitaliserings-strategier i og for kommunal sektor. Oppfølgning av KS.	Bidra til at målbildet for digitalisering i den offentlige forvaltningen kan oppnås langt raskere og til en billigere kost. Ved endring i strategien bør det rettes fokus mot mulighetsrom og utfordringsbildet, og hvordan offentlig forvaltning kan lykkes med digitalisering raskere ved å balansere ulike hensyn. En helhetlig og tverrfaglig digitaliseringsstrategi med målsetninger og forankring om informasjonssikkerhet, digital beredskap og personvern som en integrert del av alt digitaliseringsarbeid vil være en god rettesnor på hvordan kommunal sektor kan digitalisere trygt og sikkert. Gi økt forståelse og bedre beslutningsgrunnlag på tvers av kommunal sektor på hvordan digitalisering kan skje trygt, og derigjennom oppnå en raskere digitaliseringstakt.	Itererende	Varierende, avhengig av omfang	Selvfinansieres

Finansieringsmodeller

Tiltakene som anbefales gjennomført vil medføre både investerings- og driftskostnader. Denne utredningen tar ikke for seg hvordan den enkelte kommune eller fylkeskommune skal prioritere nødvendige midler.

Selvfinansiering

Aktivitetene som forventes at kommunene skal gjennomføre for å ivareta sitt ansvar finansieres gjennom «forbruksfinansiering»-modellen. Det vil si at den enkelte kommune eller fylkeskommune dekker alle faktiske påløpte kostnader for tjenestene. Det vil for eksempel innebære drift, vedlikehold, forvaltning, bemanning, tilknytning til sikkerhetskapabiliteter som SOC, IRT og CERT.

Kostfordeling

De foreslåtte tiltakene kan finansieres gjennom kostfordelingsmodellen. Det vil innebære at tjenestene finansieres av den enkelte kommune og fylkeskommune, men at kostnaden fordeles mellom brukere av tjenesten(e) basert på en fordelingsnøkkel. Det vil inkludere de samme behovene som beskrevet under selvfinansiering, men ved bruk av denne finansieringsmodellen vil kommunal sektor i større grad kunne dele på kostnadene.

Grunnfinansiering

Grunnfinansiering vil si at tiltaket finansieres gjennom sentrale midler, eksempelvis at det tildeles midler over statsbudsjettet. Denne rapporten anser det som den mest hensiktsmessige finansieringsmodellen for sentrale tjenester som et kommunalt sektorvis responsmiljø.