2023

Foto: Shutterstock

Styrking av digital robusthet i kommunal sektor

RAPPORT

Sammendrag

Denne rapporten fastslår at trygg digitalisering er en forutsetning for at kommunene skal kunne levere tjenester til alle innbyggere i Norge, nå og i fremtiden. Med trygg digitalisering menes alle de grep som må tas for å oppnå en digital robusthet der utvikling, innføring, drift og forvaltning, og utfasing av digitale løsninger gjøres på en måte som sikrer motstandsdyktighet mot hendelser og digitale angrep, og dermed sikrer tjenestenes kontinuitet og kvalitet. Tiltak for å oppnå trygg digitalisering må alltid vurderes opp mot tiltakenes kostnad og den risikoreduksjon tiltaket gir.

Målbildet for sikker digitalisering i kommunal sektor kan derfor beskrives som at:

- Kommunene er robuste nok til å kunne operere i det digitale rom uten alvorlige hendelser i krisespennet fred, krise og konflikt.
- Kommunene evner å forebygge, oppdage og håndtere digitale angrep.
- Tilgjengelig kompetanse og ressurser innen digitalisering, informasjonssikkerhet og personvern utnyttes effektivt på tvers av kommunal sektor.

Nåsituasjonen innen informasjonssikkerhet og personvern i kommunal sektor sett under ett kan beskrives som varierende grad av:

- styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet.
- nødvendig sikring av teknisk infrastruktur.
- nødvendig evne til å forbygge, oppdage og håndtere hendelser.

Rapporten fokuserer på hvordan forebygge, oppdage og håndtere digitale angrep og hendelser. Altså «grunnplanken» for å kunne oppnå en trygg digitalisering. Fokuset i rapporten er derfor ikke rettet mot personvern i klassisk forstand. Anbefalingene som er gitt i denne rapporten peker ut en retning som vil gjøre kommunene og fylkeskommunene mer robust mot digitale angrep, samtidig som ansvaret og mulighet til lokale tilpasninger ivaretas.

Gitt kompleksiteten i det digitale rom og digitalisering, antas det at man må argere sammen som en sektor for å oppnå nødvendig robusthet i kommunal sektor. Dette er også viktig i forhold til at kommunene som minimum også skal kunne operere krisespennet fred, krise, og konflikt. Oppsummert beskriver tiltakene en retning fremover på mer samarbeid på regionalt eller nasjonalt plan om oppgaver som er for store, kompliserte eller på annen måte koster for mye å gjøre hver kommune enkeltvis.

I tillegg anbefales den enkelte kommune å gjennomføre grep som:

- Gir den enkelte kommune oversikt over egen situasjon/status innen digital robusthet.
- Ivaretar ansvaret og overholder relevant regelverk i egen virksomhet.
- Legger til rette for bedre utnyttelse av de ressursene som allerede eksisterer i sektoren.
- Legger til rette for regionale og nasjonale løsninger der lokal tilnærming vil være uhensiktsmessig.

Foreslåtte tiltak er utdypet med vurdering av kostander og effekter i vedlegg A.

Målgruppen for rapporten er beslutningstakerne, digitalisertingsledere, sikkerhetsledere i kommunal sektor, relevant personell i embetsverket og samarbeidende statelig etater med kommunal sektor.

Bakgrunn for rapporten

Med utgangspunkt i dataangrepet mot Østre Toten kommune og et økende antall dataangrep mot norske virksomheter generelt, startet KS høsten 2021 arbeidet med å analysere kommunenes robusthet og deres evne til å forebygge, oppdage og håndtere dataangrep. Angrepet mot Nordland fylkeskommune 22. desember 2021 aktualiserte behovet ytterligere.

Risiko 2023[1] beskriver at denne type angrep blir vanligere og at dette også får konsekvenser i Norge og det norske samfunnet. Det nasjonale og internasjonale mediebildet gir det samme inntrykket. I Norge er det flere eksempler på dataangrep som har lammet både lokalsamfunn, virksomheter og verdikjeder.

På et seminar 7. februar 2022 med justis- og kommunal- og distriktsministeren, kommunedirektører og ordførere ble behovet for mer operativ bistand til kommunene synliggjort. Et samlet budskap fra kommunene pekte på behov for økt innsats og støtte fra statlig nivå for å kunne håndtere digitale angrep, behov for samordning av veiledningsaktørene, og ytterligere operativ støtte innen digital beredskap og hendelseshåndtering. Behovene har i ettertid blitt tatt opp i konsultasjonsmøter med regjeringen.

Proposisjon 78 S (2021-2022) påpeker også at risikoen for at land som Russland benytter ikke-militære virkemidler som digitale angrep, og etterretnings- og påvirkningsaktiviteten øker, også i Norge. Dette bekreftes videre av PSTs trusselvurdering for 2023.

Vinteren 2022 økte sikkerhetstruslene mot norsk offentlig sektor som følge av Norges involvering i forbindelse med Russlands invasjon Ukraina. 18. mars 2022 kunngjorde regjeringen at de har besluttet å styrke den sivile beredskapen og bevilget 50 millioner til å styrke sikkerheten i kommunal sektor[2]. KS ga den 30. september 2022 innspill til Kommunal- og distriktsdepartementet (KDD) på hvordan midlene bør benyttes. KS har imidlertid per 29. mars 2023 ikke mottatt noen tilbakemelding fra KDD om bruk av midlene.

Med bakgrunn i risikobildet for kommunal sektor besluttet KS vinteren 2022 å utarbeide et kunnskapsgrunnlag[3] for få bedre innsikt i kommunenes status og situasjon, øke robustheten og forsterke evnen til å forebygge, oppdage og håndtere dataangrep i kommunal sektor. Det skal skje ved å konkretisere og forankre sektorens behov for tjenester for å understøtte informasjonssikkerhets- og beredskapsarbeidet. KDD har støttet utredningen med 500.000 NOK.

Resultatet av dette arbeidet er denne rapporten som beskriver:

- Kommunenes utfordringer på overordnet nivå innen digital robusthet.
- Kommunens behov for tjenester innen digital sikkerhet og beredskap.
- Hvilke aktører som leverer tjenester innen digital sikkerhet og beredskap til kommunal sektor. Se vedlegg C, *Dagens aktørbilde for kommunal sektor innen digital sikkerhet*.
- Tiltak som kan iverksettes for å øke robustheten og evnen til å forbygge, oppdage og håndtere digitale angrep både på kort og lang sikt.

Rapporten skal behandles administrativt i KS, etter en behandling i samstyringsmodellen.

[1] https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

[2] Prop. 78 S (2021–2022), Kap. 541 IT- og ekompolitikk, post 22 og 61, https://www.regjeringen.no/no/dokumenter/prop.-78-s-20212022/id2906697/?ch=2

[3] Se vedlegg E for detaljer

Styrking av digital robusthet i kommunal sektor

Innhold

Robusthet – en forutsetning for digitalisering

Digitalisering som begrep benyttes til å forklare hvordan teknologi kan brukes til å forbedre, forenkle og fornye tjenester, eller skape helt nye tjenester. Teknologien og hvordan den settes sammen eller anvendes, i tillegg til tilsiktede eller utilsiktede sårbarheter i teknologien eller bruk av denne, utgjør ofte en sårbarhet for de digitale tjenestene. Dermed er det helt vesentlig at sårbarheten reduseres til et minimum for å kunne opprettholde kommunal funksjons- og tjenesteevne.

Digital robusthet innebærer å redusere sårbarhet og følgene av eventuelle uønskede konsekvenser i alle deler av tjenesteproduksjonen hvor teknologi er involvert, slik at kommunen er tilstrekkelig robust til å opprettholde sin funksjonsevne selv under, og etter digitale angrep eller hendelser. Det betyr at sikkerhetstiltak ikke kan iverksettes i etterkant eller som et ekstra lag, men må gjøres om en integrert del av alt som utgjør en tjeneste og kvaliteten på denne. Dette inkluderer også sikkerhetstiltak som understøtter personvern (personopplysningssikkerhet). I rapporten er dette benevnt som trygg og sikker digitalisering. «Informasjonssikkerhet og personvern» vil benyttes som et samlebegrep for tiltak eller emner som omhandler sikring av informasjon, inkludert personopplysninger.

Digitaliseringsstrategien for offentlig sektor (2019-2025) – *Én digital offentlig sektor*[4] er felles for kommunesektoren og staten. I strategien er det et uttalt mål at alle innbyggere, uansett bosted, skal ha et godt tjenestetilbud i sitt nærmiljø hvor digitalisering skal bidra til en mer effektiv offentlig sektor, mer verdiskaping i næringslivet og ikke minst en enklere hverdag for folk flest.

Digitaliseringsstrategien fastslår at informasjonssikkerhet og personvern er *grunnleggende i digitaliseringsarbeidet og må være et innebygd element fra starten av*. Det understrekes også at digitaliseringen skal ivareta innbyggernes rettssikkerhet og personvern, og sikre at offentlig sektor fortsatt har høy tillit. Digitaliseringsstrategien sier imidlertid lite om *hvordan* dette skal gjøres.

Kommunal sektor står overfor en rekke utfordringer både på kort og lang sikt. Dette gjelder for eksempel alderssammensetning og demografiutviklingen, økonomiske rammevilkår, behov for bærekraftige velferdstjenester, tjenesteutvikling og demokratiutvikling. For å kunne møte disse utfordringene både på kort og lang sikt effektivt, er teknologi og digitalisering en av nøkkelfaktorene.

Alt vi omgir oss med i det daglige og som sørger for at samfunnet fungerer, er i stor grad avhengig av at digitale systemer og nettverk fungerer. Vårt samfunn, vår funksjonsevne og vår velstand hviler på digitale fundament. Samtidig må det erkjennes at det å ta i bruk teknologi medfører sårbarhet hvis det ikke håndteres på rett måte. Ulike hensyn må derfor balanseres mot hverandre for å kunne oppnå ønsket effekt.

Denne rapporten legger til grunn det faktum at teknologi og digitalisering er viktige og nødvendige faktorer for å løse de korte og langsiktige utfordringene som kommunal sektor står overfor[5]. Med utgangspunkt i den geopolitiske sikkerhetssituasjonen og konsekvensene av digitale angrep og påvirkningsoperasjoner, blir beskyttelse av teknologien og trygg digitalisering en nødvendig forutsetning for å ivareta funksjonsevnen til offentlige og private virksomheter.

Utfordringsbildet består ikke bare av utenforliggende faktorer som trusselaktører og komplekse verdikjeder. Vi er erkjenner også at det innad i kommunal sektor er ulik grad av modenhet i teknologiutnyttelse, digitalisering og beskyttelse av tjenester, prosesser og teknologi. For å ivareta

[4] Én digital offentlig sektor, https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2685559/
[5] Tid for handling Personellet i en bærekraftig helse- og omsorgstjeneste, NOU 2023:4

demokratiet, rettssikkerheten, og nasjonens funksjonsevne blir det derfor avgjørende at man evner å løfte samtlige kommuner for å gjøre dem mer robust mot digitale angrep og påvirkning.

Med det ovennevnte som bakgrunnsteppe fokuserer denne rapporten på hvordan man kan øke kommunenes robusthet mot digitale angrep ved å ha tilstrekkelig evne til å forebygge, oppdage og håndtere digitale angrep.

Målbildet for trygg digitalisering av kommunal sektor

Det er et uttalt mål at alle kommuner i Norge skal levere gode og sikre tjenester til alle innbyggere i Norge. Med dagens digitaliseringstakt og samfunnsutvikling står sektoren ovenfor både store muligheter og betydelige utfordringer. Norsk offentlig forvaltning skal oppleves sammenhengende og helhetlige av innbyggere, frivillig sektor og offentlige og private virksomheter, uavhengig av hvilke offentlige virksomheter som tilbyr dem. Kommunene må derfor være i stand til å gjennomføre digitaliseringen på en trygg måte som en integrert del av virksomhets- og styringsstrukturen, uten å miste tilstrekkelig styringsevne.

Trygg digitalisering blir dermed en forutsetning for at kommunene i fremtiden kan levere tjenester til alle innbyggere i Norge, og samtidig ivareta sine lovpålagte tjenester og oppgaver. Med dette som bakgrunn kan målbildet for sikker digitalisering i kommunal sektor formuleres som at:

- Kommunene er robuste nok til å kunne operere i det digitale rom[6] uten alvorlige hendelser.
- Kommunene evner å forebygge, oppdage og håndtere digitale angrep.
- Tilgjengelig kompetanse og ressurser innen digitalisering, informasjonssikkerhet og personvern utnyttes effektivt på tvers av kommunal sektor.

Føringer for trygg digitalisering i kommunal sektor

Ansvaret for ivaretakelse av informasjonssikkerhet og personvern påhviler den enkelte kommune. Lov om kommuner og fylkeskommuner (kommuneloven) gir nærmere regler om fylkeskommuners og kommuners organisering. Etter kommuneloven § 5-3 er all utøving av fylkeskommunal eller kommunal kompetanse lagt til fylkestinget og kommunestyret som øverste organ. Det er disse politisk valgte organene som innehar den reelle avgjørelsesmyndigheten om hvordan det administrative nivået skal innrettes. Kommunelovens § 25-1 stiller krav om at «kommuner og fylkeskommuner skal ha internkontroll», og peker på kommunedirektøren som ansvarlig for denne. Selve organiseringen, inkludert organisering av informasjonssikkerhetsarbeidet er dermed kommunedirektørens ansvar.

Det stilles også krav til styring og internkontroll innen informasjonssikkerhet gjennom eForvaltningsforskriften. Internkontrollen på informasjonssikkerhetsområdet skal i henhold til eForvaltningsforskriften § 15 annet ledd være basert på anerkjente standarder for styringssystem for informasjonssikkerhet.[7] Videre gir lov om nasjonal sikkerhet (sikkerhetsloven) en rekke vesentlig føringer innen digital sikkerhet som treffer kommunal sektor i ulik grad.

Kommunen skal i henhold til forskrift om kommunal beredskapsplikt jobbe systematisk og helhetlig med samfunnssikkerhetsarbeidet på tvers av sektorer i kommunen. I henhold til forskrift om kommunal beredskapsplikt § 4 skal kommunen være forberedt på å håndtere uønskede hendelser,

[6] The cyber domain (digitale rom) is defined as the physical and logical interconnection of information systems, including network devices, communications infrastructure, media, and data (Windvik and Diesen 2013).
[7] Digitaliseringsdirektoratet «Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner», 2020

og skal med utgangspunkt i en helhetlig risiko- og sårbarhetsanalyse utarbeide en beredskapsplan. I henhold til § 7 skal beredskapsplanen øves på hvert annet år.

Personopplysningslovens prinsipp om ansvarlighet går ut på at virksomheten, i dette tilfellet kommunen eller fylkeskommunen, skal ha oversikt over sin behandling av personopplysninger og iverksette tekniske og organisatoriske tiltak som gjør at loven følges. Kommunen har også ansvar for å dokumentere at loven følges.

For kommuner og fylkeskommuner innebærer ansvaret dermed rent konkret at kommunen skal håndtere sikkerhet og personvern i egen virksomhet, herunder etablering av styringssystem (internkontroll) for informasjonssikkerhet og personvern, sikker drift av IKT-tjenester og underliggende IKT-infrastruktur, samt ivareta informasjonssikkerhet og personvern i prosjekt og anskaffelser. Ansvaret innebærer også tilhørende beredskapsrutiner- og planverk, samt etablering av tilstrekkelig operativ og strategisk kompetanse, også til å ivareta relasjoner til og leveranser fra myndigheter og leverandører.

Ansvaret som er beskrevet over endres ikke selv om kommunen eller fylkeskommunen inngår et samarbeid med andre kommuner, eksempelvis IKS, vertskommune eller en annen form for digitaliseringssamarbeid, eller om kommunen inngår avtaler med leverandører om oppgave- eller tjenesteutførelse. Alle disse ulike formene for samarbeid er utelukkende sentrert rundt *oppgavefordelingen*, og gjelder ikke ansvar for ivaretakelse av informasjonssikkerhet og personvern i egen kommune eller fylkeskommune.

Utfordringsbildet for kommunal sektor

Når vi ser på landskaps- og aktørbildet som omgir kommunene og fylkeskommunene fremstår det som komplekst og fragmentert. IKT-sikkerhetsutvalget (NOU 2018:14 – sikkerhet i alle ledd) omtaler en rekke etater som har rådgivning og veiledning om IKT-sikkerhetsområdet som en tversektoriell oppgave. I tillegg veileder ulike sektoraktører på spesifikke fagfelt, eksempelvis helse, e-kom og undervisningssektoren. Ifølge IKT-sikkerhetsutvalget fremstår veiledningen som fragmentert og lite koordinert. Dette påpeker også Personvernkommisjonen (NOU 2022:11)[8]:

«Fra et overordnet perspektiv er det en utfordring for den generelle informasjonssikkerheten at virksomheter primært har fokus på, og vurderer, sikkerheten i egen virksomhet eller sektor. Dette kan medføre at mindre sårbarheter hos de enkelte virksomhetene samlet kan utgjøre større sårbarheter i et samfunnsperspektiv.»

I Riksrevisjonens rapport «Undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor» (2023) uttales det «arbeidet med digital sikkerhet berører hele samfunnet, og krever derfor samordning av aktører og virkemidler på tvers av sektorene»[9]. I rapporten fremkommer det at Justis- og beredskapsdepartementet etter Riksrevisjonens vurdering ikke i tilstrekkelig grad ivaretar sitt ansvar for digital sikkerhet i sivil sektor, som igjen kan få alvorlige konsekvenser for kritiske samfunnsfunksjoner og nasjonale sikkerhetsinteresser.

Rapporten påpeker også at arbeidet med forebyggende digital sikkerhet er vanskelig for den enkelte virksomhet. Det begrunnes i at det er krevende å holde oversikt over hvilke regelverk som gjelder, hvordan regelverkene står i forhold til hverandre, og hvilke myndighetsaktører og veiledere

[8] https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/
[9] https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor/

virksomhetene skal forholde seg til. Riksrevisjonen påpeker også at viktige tverrsektorielle tiltak for å håndtere digitale angrep er forsinket.

Digitaliseringsdirektoratet undersøkte i 2020 hvordan fylkeskommuner og kommuner arbeider med informasjonssikkerhet og fremla sine funn i rapporten «Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner» [10], hvor det finnes en utdypende beskrivelse av en del av utfordringene i kommunal sektor innen informasjonssikkerhet.

De fant at fylkeskommuner og kommuner, og spesielt små og mellomstore kommuner, ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet. Digitaliseringsdirektoratet trakk særlig frem ivaretakelsen av internkontroll, beredskap, øvelser og hendelseshåndtering og sikkerhetskultur- og kompetanse innen informasjonssikkerhetsfeltet som store utfordringer for kommunal sektor. Digdir også har vurdert utfordringsbildet, og ser det samme som beskrives i denne rapporten.

Kommuner og fylkeskommuner synes det er vanskelig å få oversikt over og etterleve regelverk for digital sikkerhet. Riksrevisjonens rapport om digital sikkerhet i sivil sektor bekrefter dette. Det bekreftes også av Digitaliseringsdirektoratet gjennom arbeidet deres med informasjonssikkerhet i forvaltningen[11].

Den enkelte kommune og fylkeskommune har behov for å se digital sikkerhet inn i en helhetlig kommunal virksomhetsstyring, hvor muligheter, utfordringer og risiko kan sees i sammenheng. Kommunene må også ha evne og kompetanse til å digitalisere trygt i hele sin forvaltning og tjenesteyting, og kunne motta bistand og veiledning for å forebygge, oppdage og håndtere digitale angrep. Denne evnen og kompetansen må være integrert i virksomhetsstyringen og internkontroll. Dette har vist seg å bli en utfordring når ulike aktører gir sektorspesifikk veiledning, rådgivning og tolkning.

Både gjennom hendelser og informasjonsinnhentingen KS har gjennomført i samarbeid med kommunene over tid og kunnskapsinnhenting i forbindelse med denne rapporten[12], har det tegnet seg et tydelig utfordringsbilde. Analyser og undersøkelser av bakgrunnsmaterialet tyder så langt at det er svært ulik modenhet innen informasjonssikkerhet, digital beredskap og personvern i kommunal sektor. Dette kan på et overordnet nivå sammenfattes i:

- Har varierende grad av styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet.
- Har varierende grad av nødvendig sikring av teknisk infrastruktur.
- Har varierende grad av nødvendig evne til å forbygge, oppdage og håndtere hendelser.

For ytterligere beskrivelse av utfordringsbildet henvises det til vedlegg B.

Behov for økt digital robusthet i kommunal sektor

De behovene som beskrives i denne rapporten vurderes å være de viktigste for kommunal sektor ut fra rapporter og utredninger som allerede foreligger, samt kunnskapsinnhenting i forbindelse med denne rapporten. Sektoren rapporterer selv om manglende kompetanse, kapasitet og prioritering av økonomiske midler til og innenfor fagfeltene som omhandles i rapporten.

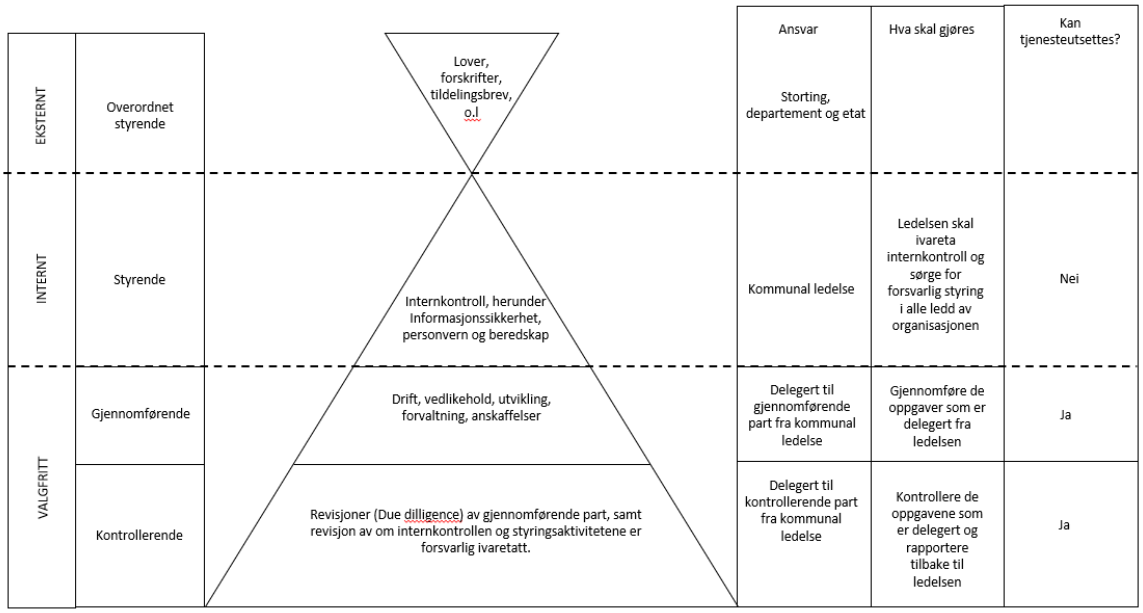
[10] https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102
[11] https://www.digdir.no/informasjonssikkerhet/felles-sikkerhet-i-forvaltningen/4115
[12] Se vedlegg E

For å sikre nødvendig robusthet er det påkrevet å bygge en struktur som vil sørge for at samtlige kommuner og fylkeskommuner, uavhengig av størrelse, evner å gjennomføre både digital transformasjon og tilstrekkelig sikring av informasjonen som forvaltes. For at kommunal funksjonsevne skal kunne opprettholdes uavhengig av trusselnivå og geopolitisk sikkerhetssituasjon, må anbefalte tiltak må adressere denne situasjonen.

Dimensjoner i behovsbeskrivelsen

Den enkelte kommunen har som nevnt ansvar for å etablere tilstrekkelig internkontroll og påse etterlevelse av denne. Det er flere måter å ivareta oppgavene som følger av ansvaret på, f.eks. fra å ivareta både ansvar og oppgaver i egen kommune til å sette ut oppgaver helt eller delvis (tjenesteutsetting).

Ansvaret med tilhørende oppgaver i den enkelte kommune kan kategoriseres inn i de tre dimensjonene som er styrende, gjennomførende og kontrollerende, se figur 1 nedenfor. Modellen nedenfor (figur 1) tar utgangspunkt i de gjeldende anbefalingene som ligger i allerede eksisterende veiledningsmateriell fra ulike statlige aktører.



Figur 1 Visualisering av ansvar og oppgaver[13]

De ytre lovmessige rammene (her kalt overordnet styrende) innen sikkerhets-, beredskaps-, og personvernarbeidet fastsettes av Stortinget, departement eller eventuelt en statlig etat.

Den styrende dimensjonen omhandler fastsettelse av hva som skal gjøres av hvem, i tråd med de ytre rammene definert i lov. Den gjennomførende dimensjonen omhandler hvordan og når oppgave(r) skal utføres i tråd med føringene fra den styrende dimensjonen. I den kontrollerende dimensjonen skal det dokumenteres om det som er utført i gjennomførende dimensjonen er i samsvar med føringer fra den styrende dimensjonen.

I den styrende dimensjonen er ansvaret definert, og en kommune eller fylkeskommune kan ikke delegere bort ansvaret for forsvarlig styring av kommunen. Oppgavene som følger av ansvaret ligger i

[13] Figuren er utformet med inspirasjon fra DigDirs' dokumentrammeverk, tilpasset kommunal sektor.

den gjennomførende og kontrollerende dimensjonen, og kan i større grad gjennomføres av valgfri part, avhengig av hva som er besluttet i den enkelte kommune eller fylkeskommune.

Ansvar og oppgaver i den styrende dimensjonen

Kommune- og fylkeskommuneledelsen er avhengig av tilstrekkelig styring på sikkerhets, beredskaps- og personvernområdet for å kunne lede den kommunale virksomheten på en god måte. Denne styringen kan oppnås gjennom etablering og oppfølging av et systematisk arbeid med sikkerhet, beredskap og personvern. Basis for det systematiske arbeidet må være en tilstrekkelig situasjonsforståelse om behovet og nåsituasjonen på området.

Som et utgangspunkt for å kunne forstå egen sikkerhets- og risikosituasjon bør det etableres et sett av kapabiliteter på informasjonssikkerhetsområdet:

- Situasjons- og risikoforståelse i kommunen for politisk og administrativ ledelse.
- Strategisk sikkerhets-, beredskaps- og personvernkompetanse i kommunen.
- Strategisk digitaliserings- og forvaltningskompetanse i kommunen.

Situasjons- og risikoforståelse i kommunens ledelse

Situasjons- og risikoforståelse er helt sentralt for prioritering innen hele leddet av kommunal tjenesteleveranse. Behovet for verktøy, kompetanse og situasjonsoversikt kan variere avhengig av om det rettes fokus mot den politiske ledelsen eller den administrative ledelsen.

Kunnskapsgrunnlaget gir en indikasjon på at både den administrative og politiske ledelsen opplever et behov for verktøy som gir, på en enkel måte, tilstrekkelig situasjons- og risikobeskrivelse i egen kommune. Det er viktig å understreke at flere kommuner har gode verktøy og metode for situasjons- og risikobeskrivelse til ledelsen, men at det er behov for tilgjengeliggjøring av et slikt verktøy til hele kommunal sektor. Det er dermed et behov for et enkelt standardisert styrings- og tiltaksverktøy innrettet mot kommunal ledelse, i tillegg til å styrke kompetansen både på politisk og administrativt nivå.

Strategisk sikkerhets-, beredskaps- og personvernkompetanse i kommunen

I tjenesteutviklingen er det viktig å ha en strategisk tilnærming for å kunne balansere mellom teknologisk mulighetsrom på den ene siden og teknologisk og prosessuell risiko på den andre siden. Et av de viktigste elementene med strategisk sikkerhetskompetanse er å gjøre den administrative og politiske ledelsen i kommunen i stand til å nå sine mål ved å utnytte teknologi og samtidig håndtere risiko på en god måte.

Kunnskapsgrunnlaget[14] indikerer ulik modenhetsgrad i kommunal sektor innenfor dette området. Tilbakemeldingen fra kommunal sektor har vært at det er behov for å styrke og utvikle kompetansenivå innen fagfeltene omhandlet i denne rapporten. Behovet innretter seg mot spesifikt kompetansehevning og strategisk styringskompetanse for samspill og rapportering til ledelsen.

Strategisk digitaliserings- og forvaltningskompetanse i kommunen.

Digitaliseringsområdet er dynamisk og i kontinuerlig utvikling. Manglende kompetanse om sammenhenger (integrasjoner, arkitektur og prosessavhengigheter) på et overordnet nivå øker risikoen for å introdusere sårbarheter i eksisterende digitale løsninger. I tillegg vil kommunen kunne introdusere nye løsninger som ikke teknologisk eller prosessuelt passer inn med eksisterende

[14] Se vedlegg E

løsninger og strukturer i kommunen. Kunnskapsgrunnlaget[15] gir indikasjon på teknisk gjeld[16] i kommunal sektor. Kombinert med behov for rekruttering av fagpersonell, kan dette også gi økt sårbarhet for den enkelte kommune.

For å imøtekomme utfordringene med forvaltning av digitalisering og digital infrastruktur, er det derfor et behov for å utvikle strategisk digitaliserings- og forvaltningskompetanse, med hensikt om å ta de riktige beslutningene for trygg digitalisering.

Ansvar og oppgaver i den gjennomførende dimensjonen

Denne dimensjonen beskriver de oppgavene som forventes utført på grunnlag av det som er besluttet i den styrende dimensjonen. Oppgavene må innebære aktiviteter som sikrer at kommuneledelsen får tilstrekkelig situasjonsforståelse, i tillegg til å forebygge, oppdage og håndtere hendelser som har sitt utspring i eller konsekvenser for informasjonsteknologi. Mer konkret vil det si aktiviteter som fører til at digital infrastruktur og de digitale tjenestene- og systemene utvikles, driftes og forvaltes i tråd med de krav som er satt til oppgaveutførelsen.

Utførelsen av oppgavene kan både være intern og ekstern sett fra kommunens perspektiv. Denne rapporten skiller ikke på ulike former for oppgaveutførelse, men fastslår at det finnes flere muligheter for å gjennomføre oppgavene, eksempelvis IKS, drifts- og digitaliseringssamarbeid, fullstendig tjenesteutsettelse til privat aktør, hybride konstellasjoner, og lignende. Ansvaret for at oppgavene utføres innenfor de rammene som er lagt ligger likevel fast forankret i kommunens ledelse.

Det følger av både kunnskapsgrunnlaget[17] og ansvaret for tilstrekkelig internkontroll at flere overordnede behov hører til den gjennomførende dimensjonen:

- Oversikt over sammenheng mellom tjenester, systemer og IT-infrastruktur.
- Løpende sikring av all IT-infrastruktur, inkludert skytjenester.
- Overvåking, analyse- og hendelseshåndtering.
- Beredskaps- og gjenopprettingsevne.
- Løpende kompetanseheving på området.

Oversikt over sammenheng mellom tjenester, systemer og IT-infrastruktur

IT-infrastrukturen, systemporteføljen og tjenestetilbudet i kommunene er i stadig endring og utvidelse. Samtidig blir stadig mer av de digitale tjenestene understøttet av skytjenester, og inngår dermed i en enda mer kompleks verdikjede enn tidligere.

Sårbarheter kan utnyttes eller ved uhell føre til uønskede hendelser. Siden sårbarheter ofte oppdages i ettertid av at et system eller applikasjon er tatt i bruk, er det avgjørende for digital robusthet at kritiske detaljer i IT-infrastruktur og arkitektur til enhver tid er kjent.

Situasjonsforståelse er som nevnt sentralt for å kunne prioritere riktig på sikkerhets- og personvernområdet. Et grunnleggende element i situasjonsforståelsen er at kommunene har en enkel og oversiktlig beskrivelse av status for styringssystem, rutiner og teknologi, gjerne i henhold til etablerte rammeverk som Nasjonal Sikkerhetsmyndighets (NSM) Grunnprinsipper for IT-sikkerhet. En

[15] Se vedlegg E
[16] I denne kontekst benyttes «teknisk gjeld» som begrep for å beskrive underinvestering og dermed foreldelse av teknologiske løsninger, herunder maskinvare og programvare
[17] Se vedlegg E

slik vurdering vil være et meget godt utgangspunkt for å gjøre videre prioritering av tiltak i den enkelte kommune.

I Norge har NSMs Grunnprinsipper for IT-sikkerhet oppnådd status som de facto standard på området. Grunnprinsippene er ikke en oppskrift på teknologiske løsninger eller definerte rutiner, men beskriver krav til IT-løsningene og -tjenestene som bør oppfylles av den enkelte virksomhet for å at virksomheten skal kunne forvente å ha tilstrekkelig digital robusthet.

For å kunne prioritere mellom tiltak som er nødvendige for å redusere risiko må det gjennomføres risiko- og sårbarhetsvurdering (ROS). Ved at alle systemer er vurdert, vil også kommuneledelsen få oversikt over kommunens totale risikobilde på IT-området. ROS er derfor en av kjernekomponentene i risikostyring, og det er svært viktig at arbeidet prioriteres ved alle sentrale IT-systemer og endringsprosesser.

Dersom det er sannsynlig at en behandling vil medføre en høy risiko for personers rettigheter og friheter, skal kommunen før behandlingen starter foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet, jf. GDPR artikkel 35 nr.1. Dette gjelder særlig ved bruk av ny teknologi og det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i. En personvernkonsekvensvurdering (DPIA) skal gjennomføres før behandlingen av personopplysninger starter.

Gjennomføring og dokumentasjon av vurderinger som ROS og DPIA er helt elementære grunnsteiner i den enkelte kommunes risikostyring, og skal være en del ut av kommunens styringsverktøy, og krever begge at det eksisterer en oppdatert oversikt over sammenheng mellom tjenester, systemer og IT-infrastruktur.

Mange kommuner og fylkeskommuner gjennomfører ROS og DPIA. Dette kan, dersom mekanismene er tilrettelagt for det, gi god oversikt til kommunens ledelse om situasjonen. Likevel skriver Digitaliseringsdirektoratet (Digdir) i 2020 at

> *Observasjonene viser at 68,8 % av fylkeskommunene gjennomfører risikovurderinger systematisk og periodisk. Tall for kommunene viser at 58,9 % av de store kommunene, 47,7 % av de mellomstore kommunene og 33 % av de små kommunene gjør det samme*[18].

Dette tilsier at kommuner og fylkeskommuner fortsatt har et betydelig behov for å øke aktiviteten på dette området. Status på oversikt over sammenhenger i IT-infrastrukturen er ikke godt kartlagt, men over 15%[19] av kommunene vurderte i 2022 det slik at de ikke visste om IKT-utstyr har kommet på avveie, noe som gir en indikasjon på manglende oversikt.

Løpende sikring av IT-infrastruktur, inkludert skytjenester

Forebygging av digitale angrep i og mot teknisk infrastruktur gjøres mest effektivt ved å redusere sårbarhetsflaten. Evne til å oppdage og fjerne eksterne og interne kjente sårbarheter bidrar til å verifisere etablerte sikkerhetstiltak samtidig som sårbarhetsflaten reduseres.

En vesentlig komponent av digital robusthet er sikker IT-drift. Det er stor konsensus i IT-bransjen om hva som gir sikker IT-drift, og det finnes flere standarder som underbygger denne. I NSM sine Grunnprinsipper for IT-sikkerhet og andre sikkerhetsstandarder, eksempelvis ISO 27001, pekes det på at grunnsikringen og god forvaltning av IT-infrastruktur er helt sentral for å oppnå tilstrekkelig beskyttelse mot dataangrep og digitale hendelser. De aller fleste kommunene og fylkeskommunene

[18] Digdir: «Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner» (2020), s. 16

[19] Vedlegg E, tabell 12617

har et forhold til NSMs Grunnprinsipper for IT-sikkerhet. Status for den enkelte kommune varierer betydelig ift. om grunnprinsippene er omsatt til konkrete tiltak, og gjennom erfaring fra hendelser og innsiktsarbeidet[20] har det blitt kjent at en rekke kommuner f.eks. ikke har gjennomført det NSM kaller «Fem effektive tiltak mot dataangrep». Disse fem tiltakene kan alene betraktelig redusere sannsynligheten for å bli rammet av et digitalt angrep.

Som tidligere nevnt er leverandørmarkedet en vesentlig bidragsyter ved digitalisering av kommunal sektor. Kommunene opplever det som krevende å følge opp leverandører, spesielt store, på sikkerhet, digital beredskap og personvern. Det kan skyldes intern kompetanse, ressurssituasjon, eller kommunen i seg selv er for små til å få gjennomslag i møte med store selskap. Det er også rapportert om utfordringer i anskaffelsesprosesser og tilgjengelig kompetanse om hvilke sikkerhetskrav som bør stilles.

Overvåking, analyse og hendelseshåndtering

Begrenset kompetanse og kapasitet til å ivareta nødvendig deteksjons- og responsevne, øker sannsynligheten for at uønskede hendelser ikke oppdages eller håndteres på (tids)riktig måte. Det kan medføre at konsekvensen av hendelsen øker. Hurtig deteksjon og respons på eventuelle uønskede hendelser er kritisk for å sikre gjenopprettelse av systemer og drift, sikre data og derigjennom tjenestetilbudet i kommunen.

Innsiktsarbeidet KS har gjennomført i samarbeid med kommunene viste at bare 1/3 av kommunene har etablert sårbarhetsscanning som en løpende tjeneste[21]. Nesten alle kommuner har en eller annen form for sårbarhetsscanning av tjenester som er eksponert mot internett, men det er vesentlige mangler på scanning av interne tjenester og underliggende IKT-infrastruktur. Dette medfører at et betydelig flertall av kommunene ikke er klar over sikkerhetstilstanden i egen IT-infrastruktur.

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[22] som et senter som «leverer deteksjonstjenester ved å observere tekniske hendelser i nettverk og systemer», og kan også være ansvarlig for hendelsesrespons i virksomheten.

Et IRT (Incident Response Team), et beredskapsteam som kan gripe inn ved hendelser, er avgjørende for at den enkelte kommune eller fylkeskommune raskt kan håndtere en pågående hendelse og kan dermed bidra til å redusere konsekvensen av hendelsen. SOC (overvåke, oppdage) og IRT-tjenester (respons) sees derfor gjerne i sammenheng. Innsiktsarbeidet har vist at det i dag er få kommuner eller fylkeskommuner som faktisk har etablert eller tilknyttet seg SOC og/eller IRT med tilstrekkelig kapasitet og kompetanse, selv om mange sonderer markedet.

Ved etablering av eller tilknytning til SOC og IRT vil en kommune eller fylkeskommune ha økt sin evne til å oppdage og respondere på hendelser betydelig. Dette vil redusere sannsynligheten for en uønsket digital hendelse som utpressing, sabotasje eller innbrudd, og kan redusere skadeomfanget dersom hendelsen skulle oppstå.

[20] Se vedlegg E

[21] Vedlegg E, dialog med kommuner og SSB tabell 12618

[22] https://www.enisa.europa.eu/

En CERT[23]-tilknytning kan også være et skritt på veien til bedre responsevne for en kommune. De aller fleste kommunene og fylkeskommunene er allerede tilknyttet HelseCERT eller andre CERT-er, selv om ikke alle har muligheten til å utnytte denne tilkoblingen på grunn av kompetanse- eller kapasitetsmangel i egen virksomhet.

Beredskap og gjenopprettingsevne

Selv om en kommune eller fylkeskommune har etablert grunnsikring (NSMs Grunnprinsipper for IT-sikkerhet) og har knyttet seg til eller etablert tjenester for varsling, forebygging, oppdagelse og håndtering (CERT, SOC og IRT), gir det ingen sikkerhet for at kommunen unngår å bli rammet av et digitalt angrep, bare lavere risiko for at det skal inntreffe.

I verste fall må kommunen gjennom en full gjenoppretting til normal drift etter en alvorlig hendelse, noe som har vist seg å kunne være en prosess som tar mange måneder, eksempelvis sett ved hendelsen i Østre Toten og Nordland fylkeskommune. For å være mest mulig forberedt på et digitalt angrep med verste utfall må kommunen ha beredskapsplaner både for å håndtere selve hendelsen, men også for følgefeil som oppstår i alle sektorer i kommunen som følge av hendelsen. I tillegg må systemer og data gjenskapes mest mulig smidig og effektivt. Dette krever både planlegging, trening og teknologiske løsninger og ikke minst at kommunene kan stå i en krisesituasjon over lengere tid. Det fordrer at den enkelte kommune og fylkeskommune også må ha gode planer for kontinuitet og gjenoppretting av tjenestene.

80% av kommunene rapporterer om tekniske backupløsninger plassert på annen lokalitet enn driftsmiljøet, og over 60% rapporterer om rutinemessig testing av om backup er korrupt eller manipulert[24]. Det er viktig å presisere at dette ikke forteller noe om kommunens treningsnivå på å håndtere digitale hendelser. Ut fra dialogen med kommunene våren 2022 er det grunn til å tro å nivået her er vesentlig lavere enn på den tekniske løsningssiden.

Løpende kompetanseutvikling

Manglende risikoforståelse i kommuner og fylkeskommuner kan påvirke kultur, holdninger, handlinger og prioriteringer negativt. Det kan føre til ineffektivitet gjennom utilstrekkelig styring, og mulig øke sannsynlighet for uhensiktsmessig ressursallokering og feilprioriteringer, samt at den enkelte handler på en måte som øker risikoen for at digitale angrep blir vellykkede.

Kompetanse er ferskvare og utvikling bør derfor skje kontinuerlig. Etablering av varige strukturer for å sikre at eksisterende og nyansatte i kommunen får riktig og tilstrekkelig kompetanse til å gjennomføre sine arbeidsprosesser trygt og lovlig bør derfor forventes å finnes i den enkelte kommune. Administrativ og politisk ledelse må også få tilstrekkelig kunnskapsgrunnlag til å kunne ta de riktige beslutningene og prioritere mellom flere risikoområder.

Innsiktsarbeidet har vist at det er varierende i hvilken grad det er etablert målrettet opplæring for politisk og administrativ ledelse i kommuner og fylkeskommuner. Den samme situasjonen gjelder for kommunalt ansatte.

Oppsummert om den gjennomførende dimensjonen

Kommuner og fylkeskommuner har som beskrevet under utfordringsbildet[25], vansker med å beskytte teknisk infrastruktur mot både utilsiktede og tilsiktede hendelser. Situasjonen er krevende fordi flere kommuner allerede har et opparbeidet gap mellom nåværende og ønsket situasjon. I tillegg forsetter

[23] CERT står for Computer Emergency Response Team, se https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering

[24] Vedlegg E, SSB tabell 12618

[25] Vedlegg B

dette gapet å øke fordi digitaliseringen øker i tempo, og nye løsninger og tjenester innføres uten at gamle nødvendigvis saneres (teknisk gjeld).

Som tabell 12618[26] viser gjøres det mye god arbeid i kommunal sektor for å sikre IT-infrastruktur. Samtidig melder kommunal sektor at det er behov for tiltak for å oppnå tilfredsstillende sikkerhet.

Den enkelte kommune må innhente og sammenstille, eller utvikle, kompetanseutviklingstiltak som sikrer at den politiske og administrative ledelsen får opplæring i hvilke muligheter og utfordringer kommunen står overfor i digitaliseringen, og hvordan kommunen på best mulig måte kan håndtere den risikoen som følger med. Det er også nødvendig at alle ansatte får tilrettelagt opplæring, i tillegg til at kvalifisert fagpersonell får anledning til kontinuerlig fagpåfyll.

Utarbeidelse av (standardiserte) sikkerhetskrav øker sannsynligheten for at det anskaffes systemer som har tilstrekkelig innebygget sikkerhet, og at det er mulighet til å vedlikeholde sikring av systemene i etterkant. Dette inkluderer skytjenester.

Kontroll på verdikjeden for digitale tjenester er en sentral del av sikringen av IT-infrastruktur. Gjennom en selskapsgjennomgang (såkalt «due diligence») vil kommunen kunne sikre seg at tjeneste- og driftsleverandørene leverer tjenester som har tilstrekkelig sikkerhet og beredskap, samt har evne og kapasitet til å håndtere hendelser.

For å få en effektiv samhandling bør kommunene ha en felles møtearena for å kommunisere og tydeliggjøre hvilke krav som kommunen stiller og kommer å stille til digitale leveranser fra sine leverandører. Det er viktig å lytte til leverandørene på hva de evner og kan levere, særlig med hensyn til hva kommunen vil kravstille i fremtiden. På denne måten vil det skapes en gjensidig felles forståelse og samvirke for gode og sikre tjenester.

Landstinget i KS vedtatt og gitt KS en tydelig rolle og et oppdrag med å sikre samordning og økt gjennomføringskraft i digitaliseringsarbeidet i kommunal sektor[27]. Landstinget uttaler videre at *dette er viktig for å sikre utvikling av helhetlig løsninger for innbygger og næringsliv. En av fordelene ved å gå sammen om en felles virksomhetsarkitektur er at man samler seg om et sett med krav til leverandører og samarbeidsaktører*.

Behovet er kjent og kommunene ønsker at KS skal ta en enda sterkere pådriverrolle innen digitalisering, noe nå KS arbeider aktivt med.

Ansvar og oppgaver i den kontrollerende dimensjonen

Den kontrollerende dimensjonen beskriver oppgaver og aktiviteter som må gjennomføres for å sikre at oppgavene i den gjennomførende dimensjonen blir gjort i tråd med de føringene som er gitt i styringsdimensjonen. Oppgaver og aktiviteter som utføres i den kontrollerende dimensjonen kan i stor grad delegeres til valgfri part, men fordrer gode rapporteringslinjer tilbake til den styrende dimensjonen.

En velfungerende egenkontroll er viktig for å sikre tilliten innbyggerne og for å sikre effektiv og riktig ressursbruk i kommunen. Kommuneloven har regler om kontrollutvalg, revisjon og administrasjonssjefens internkontroll, jf kapittel 22-25 i kommuneloven.

I webinar den 18. november 2022 med NKRF/KS ble det fremmet et behov for økt for kompetanse innen operativ IT-sikkerhet for de som gjennomfører revisjoner. Tradisjonelt gjennomføres det dokumentrevisjon i den enkelte kommune, men det er et behov for kompetanse om hvilke spørsmål

[26] Vedlegg E

[27] https://www.ks.no/om-ks/hva-gjor-vi/ks-toppmoter/landstinget-2020/landstinget-gir-ks-en-tydelig-rolle-i-arbeidet-med-digitalisering/

og kontroller det er viktig å gjennomføre for å etablere et riktig bilde av sikkerhetstilstanden i kommunen, utover det som fremkommer av dokumentkontrollen. Dette behovet bekreftes også av Riksrevisjonen:

> *Riksrevisjonen har gjennom mange år gjennomført revisjoner av digital sikkerhet på viktige samfunnsområder for å undersøke om etatene sikrer informasjonen og beskytter IKT-systemene godt nok. En viktig utvikling i bruk av metoder er nettopp dreiningen bort fra ren dokumentkontroll mot mer dyptgående undersøkelser av om internkontrollen fungerer og analyser av det faktiske sikkerhetsnivået.*[28]

Det er derfor et behov for ytterligere praktisk operativ IT-sikkerhetskompetanse i den kontrollerende dimensjonen, med særlig søkelys på parter som gjennomfører revisjoner på sikkerhets- og personvernområdet i kommunene.

Når det gjelder leverandørkontroll er tilbakemeldingene at mange kommuner, og spesielt de mindre, finner det utfordrende å gjennomføre kontroll av spesielt de store leverandørene til kommunal sektor. Dette kom spesielt frem i forbindelse med Schrems-II dommen[29] hvor flere leverandører ikke var klar over f.eks. hvor dataene lå[30].

For å kunne redusere sårbarhetsflaten i kommunal sektor er det derfor viktig å kunne følge opp og påse at leverandørene gjør nødvendige sikkerhetstiltak, og at tjenestene leveres i henhold til tidsaktuell lovgivning og føringer.

Operasjonalisering og gjennomføring av oppgaver

Ansvaret for forsvarlig styring og internkontroll, ivaretakelse av personvernlovgivningen og beredskapsarbeidet er som nevnt den enkelte kommunes ansvar. Dermed er alle listede oppgaver i overstående kapitler den enkelte kommunes ansvar å iverksette for å oppnå tilstrekkelig sikkerhet. Det medfører også at den enkelte kommune i utgangspunktet må bære samtlige kostnader som følger av aktivitetene.

Uansett årsak til at kommunenes og fylkeskommunenes nåsituasjon innen digital robusthet, vil det være svært uheldig om situasjonen fortsetter slik. Sannsynligheten for uønskede hendelser som rammer de kommunale tjenestene er betydelig, og konsekvensene kan være alvorlige.

Oppgaver som følger av ansvaret og derfor forventes gjennomført av den enkelte kommune:

- Gjennomføre modenhetsvurdering opp mot NSM Grunnprinsipper for IKT, for eksempel som en del av forvaltningsrevisjonsplan for 2023/24 i tråd med risiko- og vesentlighetsvurderingen.
- Etablere metoder og verktøy for å tilgjengeliggjøre situasjons- og risikobeskrivelse innen sikkerhets-, beredskaps- og personvernområdet for administrativ og politisk ledelse, og sikre oppfølging. Ledelsens styring og oppfølging bør baseres på etablerte veiledere og standarder, eksempelvis DigDir's veiledning eller ISO 27001.
- Gjennomføre sårbarhetsreduksjon og etablere «sikkert» oppsett av systemer og infrastruktur, herunder innføre NSMs «Fem effektive tiltak mot dataangrep».
- Sikre at tilstrekkelig strategisk kompetanse innen informasjonssikkerhet, personvern og beredskap er tilgjengelig.

[28] https://www.ks.no/fagomrader/digitalisering/kompetanse-og-verktoy/informasjonssikkerhet-og-personvern/er-en-trygg-digital-hverdag-mulig-i-kommunene/

[29] https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581

[30] https://kins.no/verktoykasse/schrems-ii-og-leverandoroppfolging/

- Vurdere status for gjennomførte ROS/DPIA på sentrale fagsystem, og gjennomføre ROS/DPIA på sentrale fagsystem og behandlinger der dette ikke er utført.
- Etablere og vedlikeholde teknologiske sikkerhetskrav, samt opprette leverandørdialog.
- Revidere sentrale leverandører på informasjonssikkerhetsområdet.
- Etablere tilknytning til CERT, tilknytning eller opprettelse av SOC og IRT, herunder etablere rutiner for håndtering av tilknytningen (varsler, alarmer etc.).
- Etablere og forvalte beredskapsplanverk, gjennomføre øvelser.
- Utvikle og gjennomføre tilpasset kompetansehevingstiltak for politisk og administrativ ledelse, brukere og teknisk/støtte-personell[31].

Disse oppgavene tar utgangspunkt i et minste felles multiplum av hva en kommune eller fylkeskommune bør gjennomføre for å kunne øke sin digitale robusthet til et nivå som reduserer sannsynligheten for at alvorlige IKT-hendelser skal påvirke kommunal tjenesteproduksjon og føre til betydelige gjenopprettingskostnader.

Flere av disse anbefalingen ble også sendt ut til landets kommunedirektører og ordførere i ett felles brev av Kommunal- og distriktsminister og KS styreleder i 9. mars 2022[32] som i tillegg tar spesielt tar for seg;

- Sikkerhetsovervåkning.
- Sikring av kritiske funksjoner og tjenester.
- Beskytte tjenester som er tilgjengelig på Internett.
- Årvåkenhet og teknologi.

Noen kommuner har allerede innført deler av disse tiltakene, men innsiktsarbeidet gjennomført i 2022 viste tydelig at det for mange kommuner gjenstår mye.

Med det kunnskapsgrunnlaget som ligger til grunn for denne rapporten, vil man måtte trekke den konklusjon at det vil være svært utfordrende for den enkelte kommune å alene finansiere og utføre mange av oppgavene kommunen er pålagt å gjøre. Modenhetsnivået varierer selvsagt mellom kommunene, og noen få kommuner utfører alle de oppgavene som ligger i den styrende, gjennomføre og kontrollerende dimensjonen. Basert på kunnskapsgrunnlaget som foreligger og de erfaringene som er gjort i de senere år, er det sannsynlig at de fleste kommunene vil ha behov for bistand i en eller annen form for å komme videre i sikkerhetsarbeidet, og noen kommuner vil ha behov for betydelig grad av bistand.

Gjennomføring av samtlige foreslåtte tiltak vil derfor, for en god del kommuner, bety betydelige investeringskostnader, med tilhørende driftskostnader på flere millioner kroner i året. For hele kommunal sektor under ett vil disse tiltakene, hvis de gjennomføres kommune for kommune, gi investeringskostnader på flere hundre millioner med dertil hørende driftskostnader. Med dagens økonomiske situasjon for kommunene er det lite sannsynlig at den enkelte kommune kan gjennomføre disse tiltakene alene uten tilførsel av midler.

Selv om det er den enkelte kommunes ansvar å sikre at oppgavene blir utført, bør kommunene vurdere om noen av oppgavene kan gjennomføres i fellesskap/samarbeid mellom dem, der kostnadene blir delt mellom de ulike kommunene som deltar i samarbeidet.

[31] Roller innen informasjonssikkerhet, personvern og beredskap

[32] https://www.ks.no/fagomrader/digitalisering/kompetanse-og-verktoy/informasjonssikkerhet-og-personvern/rader-kommunene-til-a-se-pa-it-sikkerhetstiltak/

Behov kan møtes regionalt

Det følger av rammene rundt det kommunale og fylkeskommunale selvstyret at tjenesteyting og samfunnsutvikling vil være ulik fra kommune til kommune. Samtidig skal kommuneloven bidra til at kommuner og fylkeskommuner er effektive, tillitsskapende og bærekraftige.

Etablering, utvikling og drift av digitale tjenester og tilhørende infrastruktur er tjenester som i stor grad lar seg skalere. De fleste kommuner har allerede vurdert effektivitetsfordelene med å drifte digitale tjenester i fellesskap eller kjøpe disse av eksterne aktører som mer fordelaktig enn muligheten til å bestemme alle detaljer rundt tjenestedriften selv. Den samme vurderingen vil sannsynligvis etter hvert skje innen digital sikkerhet, beredskap og personvern ettersom dette er kostnadskrevende tjenester.

Fremveksten av nasjonale løsninger og økende samstyring mellom forvaltningsnivåene forsterker behovet og graden for standardisering av arbeidsprosesser og systemer. Drift av nettverk, servere og systemer blir utfordret i takt med stadig høyere forventinger om kvalitet, effektivitet og produktivitet – og ikke minst sikkerhet.

Økende bruk av sensorer, IoT, dataomfang og kunstig intelligens forsterker både mulighetene og utfordringene. Krav til personvern står sterkere i samfunn og lovgivning, og de digitale truslene øker i omfang. Dette medfører at det er stort behov for kompetanse i de enkelte kommunene, som ofte må konkurrere om de samme ressursene som andre offentlige aktører og private aktører.

Som kunnskapsgrunnlaget viser opplever de fleste kommuner at det er krevende å etablere de nødvendige tjenestene og funksjonene på egenhånd. På toppen av dette kommer utfordringene med at det er knapphet på den kompetansen det er behov for til disse tjenestene. I tillegg har flere kommuner gitt tilbakemelding på behov for kartlegging av mulighet for felles driftsenheter, med formål om å sanere teknisk gjeld, tilgang på kompetanse og redusere sårbarhetsflaten.

Dagens situasjon og utvikling utfordrer de etablerte drifts- og forvaltningskonseptene i kommunal sektor. Kostnadene forbundet med digitalisering og IT/IKT vil trolig fortsette å øke, mens det økonomiske handlingsrommet er forventet å bli vesentlig mindre.

Fremtidig organisering av drift og forvaltning av IKT i kommunal sektor

Etablering av samarbeidsformer mellom kommuner har vist seg å gi betydelige gevinster for kommuner og tjenestemottakere[33]. Den vanligste formen for samarbeid innen digitalisering har vært å etablere felles driftsenheter innenfor samme geografiske område.

Med felles driftsenheter menes det at flere kommuner går sammen om å drifte den digitale infrastrukturen, herunder nettverk, servere, system og systemarkitektur, klient, skyteknologi og brukerstøtte, med mer. Etter hvert har det også vokst frem samarbeidsformer der fokus har vært mer helhetlig på digitalisering, med felles prosesser i samarbeidet rundt digital robusthet, anskaffelser, innføring og lignende.

I 2023 er utredningen «Hvordan kan det samlede utfordringsbildet for fremtidig IKT i kommunal sektor håndteres?» en del av FoU-porteføljen[34] til KS. Det foreslåtte prosjektet har som mål å utrede hvordan det samlede IKT utfordringsbildet i kommunal sektor kan møtes. Arbeidet er delt mellom en kunnskapsoppsummering og utvikling av en strategi for hvordan felles utfordringsbilde kan ivaretas i

[33] https://www.statsforvalteren.no/siteassets/fm-oslo-og-viken/kommunal-styring/kommunereform/nivi-rapport-2021_-3-interkommunalt-samarbeid-i-buskerud.pdf

[34] Forslag til FoU-prosjekter kommer fra KS's fagavdelinger, regioner, styrer, råd og fagnettverk. FoU-ordningen skal understøtte KS som arbeidsgiverorganisasjon, interessepolitisk aktør og utviklingspartner.

fremtiden. Strategien skal utvikle et tydelig målbilde og definere oppgavedeling mellom hva som bør håndteres lokalt, regionalt og nasjonalt.

Ettersom utfordringsbildet på området skal adresseres av FoU 'en reflekterer ikke denne rapporten anbefalinger eller tiltak om fremtidig drift og forvaltning av IKT i kommunal sektor, men det påpekes likevel at organisering av drift og forvaltning av IKT er av stor betydning for arbeidet med informasjonssikkerhet og digital robusthet.

Samarbeid om tjenester og kompetanse innen sikkerhet

KS sine anbefalinger knyttet til Proposisjon 78 S (2021-2022) innebar forslag om et Nasjonalt program for informasjonssikkerhet i kommunal sektor. Forslaget inneholdt etablering av regionale sikkerhets- og kompetansesamarbeid for å bistå den enkelte kommune i sin region med følgende operative tjenester og oppgaver:

- Operasjonalisering av anbefalte tiltak fra CERT-strukturen
- Operasjonalisering av tiltak identifisert i ROS og DPIA
- Bistand til sårbarhetsskanning
- Bistand til utvikling og etablering av beredskapsplaner- og øvelser
- Regionens kompetansesenter med tilbud av kompetansehevende tiltak, eksempelvis kurs, opplæringstiltak og seminarer
- Bindeledd mellom CERT-strukturen og kommunene
- Fasilitere og bistå med anskaffelser
- Koordinere og håndtere hendelser lokalt (Incident response team (IRT))
- Formidle situasjonsbildet til administrativ og politisk ledelse
- Operativt fellesskap og kommunikasjonsnettverk i regionene
- Rådgivning og kontrolltjenester

Disse operative oppgavene er nødvendig å iverksette i den enkelte kommune, og er samtidig gode kandidater for kostnads- og kompetansedeling mellom kommunene. En slik samling tjenester kan med fordel gjøres i geografiske klynger, sannsynligvis opp i regional størrelse. Samlingen av tjenester og kompetanse innen informasjonssikkerhet gjør det nærliggende å kalle et slikt samarbeid for regional cyber sikkerhets- og kompetanseenhet for kommunal sektor (RCSK).

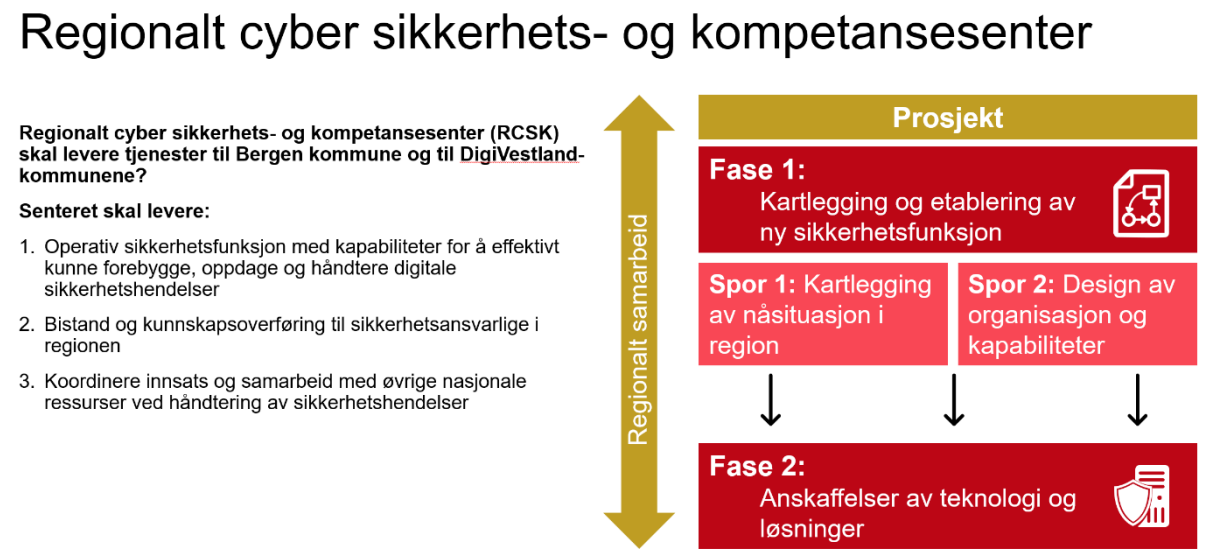
Tjenestene som kan inngå i en RCSK kan variere avhengig av medlemmenes behov og ønsker. RCSK kan bidra til at regionene i større grad kan nyttiggjøre og dele på kompetansen som eksisterer i regionen, og dermed redusere den enkelte kommunes kostander sammenlignet med å hente inn kompetansen selv. RCSK kan også bistå med koordinering mellom øvrige aktører, og bistå de som i dag ikke har forutsetninger til å iverksette tiltak, råd og veiledning gitt fra øvrige sentrale aktører.

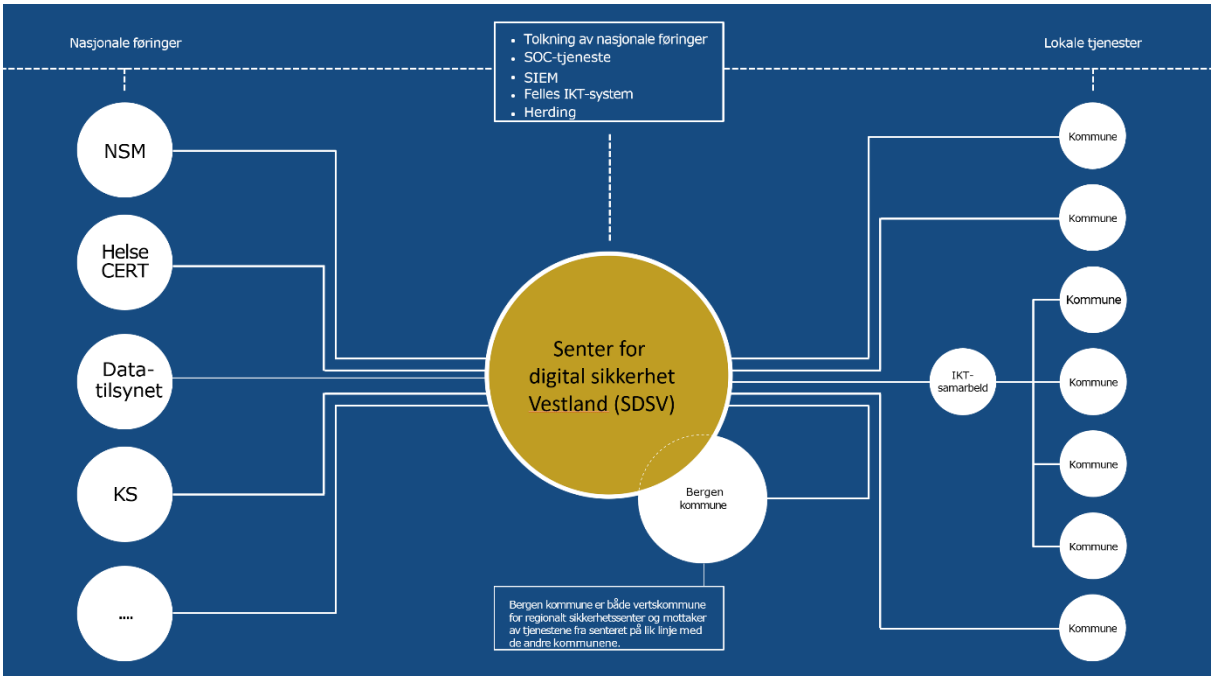
Basert på antall kommuner og fylkeskommuner, kan det være hensiktsmessig at det opprettes flere RCSK som kan samarbeide om å dekke hele sektoren. Kjernekompetansen som er nødvendig for å etablere og drifte tjenestene er svært ettertraktet, så det er ikke sannsynlig at det kan etableres mange slike enheter nasjonalt. Det er trolig også mer kostnadseffektivt å konsolidere større fagmiljøer innen tjenester som IRT, SOC og operativ bistand til kommunene. Basert på tilgangen på kompetanse og størrelsene på regionene, kan 3-4 enheter sannsynligvis etableres i Norge.

Det kan være hensiktsmessig at eksempelvis to- eller flere digitaliseringsnettverk samarbeider om etablering av ett felles RCSK. RCSK kan også opprettes i og mellom større driftssamarbeid eller andre digitaliseringssamarbeid. Med etablering menes ikke nødvendigvis å etablere en ny enhet, men kan være en samarbeidsslutning eller annen form for samarbeid. Vurdering av RCSK kan med fordel sees i

sammenheng med planlagt FoU «Hvordan kan det samlede utfordringsbildet for fremtidig IKT i kommunal sektor håndteres?».

En mulig tilnærming til RCSK, se figurene nedenfor, kan digitaliseringssamarbeidet i Vestland tjene som et eksempel.





Oppsummering og anbefaling av tiltak

Etableringen av et RCSK kan gjøres i samarbeid med digitaliseringsnettverkene, og bør kunne utvikles i tråd med føringer og rammer drøftet i den nasjonale samstyringsstrukturen. Etableringen bør skje på en slik måte at oppgavene er klart definert, og i tråd med behovene til medlemskommunene. Formålet bør være at kommunal sektor har tilgang til et operativt sikkerhetsmiljø regionalt, tettere på kommunene enn det som tilbys i dag, og som utvikles i tråd med de til enhver tid gjeldende behov i både sektoren, regionen og nasjonen ellers.

Anbefaling om tiltak regionalt:

Tiltak	Beskrivelse
1	Kommuner i og utenfor eksisterende diginettverk og IKT-samarbeid, anbefales å etablere en regional cyber sikkerhets- og kompetansesenter i sitt nedslagsfelt (RCSK).

Behov kan møtes nasjonalt

Behovene som kommunene har fremmet kan møtes lokalt og regionalt som beskrevet over. Enkelte funksjoner kan med stor sannsynlighet også etableres nasjonalt, enten ved økt samarbeid og samordning, eller at det etableres og tilgjengeliggjøres tjenester som kommunal sektor kan benytte seg av. Spesielt gjelder dette funksjoner som fortsetter å gi stordriftsfordeler ut over regionalt samarbeid, eller er så kompetansekrevende at det finnes få ressurser nasjonalt som kan utføre tjenesten.

Helhetlig veiledning for og til kommunal sektor

Som beskrevet i vedlegg C oppleves det som utfordrende for kommunal sektor å orientere seg i aktørlandskapet. Selv om det finnes mye veiledningsmateriell innen informasjonssikkerhet, digital beredskap og personvern, er det svært krevende for mange kommuner å operasjonalisere innholdet og dermed kunne utføre de oppgavene og aktivitetene som kreves.

Gjennom kunnskapsgrunnlaget har kommunene beskrevet en situasjon der det er uklart hva som er absolutte minstekrav til den enkelte kommune. Videre er det også flere sektorspesifikke veiledere og aktører som treffer kommunal sektor, som gjør det kapasitetskrevende å tilpasse det egen kommune.

I Meld. St. 9 (2022 –2023), *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* foreslås (punkt 3.5.2):

> «*Flere statlige myndigheter gir råd og veiledning om digital sikkerhet, og myndighetenes arbeid på området kan for omverdenen fremstå fragmentert og lite koordinert. […] Regjeringen vil vurdere ytterligere tiltak for å forsterke samordningen på myndighetsnivå og gjøre det enklere for sluttbrukeren. Regjeringen vil kartlegge brukerbehov og erfaringer med dagens organisering av veiledning innen digital sikkerhet. Dette for å vurdere oppgaver, ansvar og organisering, og om en kraftsamling av veiledningsmiljøer vil kunne gi effektiviseringsgevinster*.»

Tiltaket i stortingsmeldingen imøtekommer behovet beskrevet i denne rapporten.

I tråd med digitaliseringen og samfunnsutviklingen, er det også behov for at statlig forvaltningsnivå ser på hvordan sektorprinsippet påvirker arbeidet med digitalisering, informasjonssikkerhet, beredskap og personvern, som per definisjon er sektorovergripende. Personvernkommisjonen (NOU 2022:11) trekker også frem følgende om sektorvis inndeling av offentlig sektor:

> *«Personvernkommisjonen har inntrykk av at det er bygget opp betydelige kompetansemiljøer på personvern i store deler av forvaltningen de siste årene. Den silo-orienterte oppbygningen av offentlig sektor bidrar imidlertid til små miljøer som sitter adskilt fra hverandre, og kompetansemiljøene drar i liten grad synergieffekter av hverandres kunnskap og innsikt»* (NOU 2022:11, s 76)

Denne refleksjonen stemmer også godt på informasjonssikkerhetsområdet slik kommunene rapporterer det. Som personvernkommisjonen påpeker, er det flere fagmiljøer som ikke i dag evner å skape synergieffekter i den offentlige forvaltningen. Ettersom digitalisering er avhengig av

personvern, informasjonssikkerhet og digital beredskap for å kunne oppnå hensikten, bør det også settes søkelys på hvordan det kan etableres fagmiljøer som ikke bærer preg av silo-orientert oppgavefordeling.

Mange strategier peker på mulighetsrommet ved digitalisering, men beskriver i mindre grad risiko og krav til trygg og effektiv digitalisering. Det er derfor også et behov for å adressere kompetanse- og fagområdene personvern, informasjonssikkerhet og digital beredskap i digitale strategier i sektoren.

Digdirs har tatt initiativ til «Felles sikkerhet i forvaltningen» hvor det startes et arbeid for å utvikle «felles sikkerhet i forvaltningen», inkludert en felles referanseramme (eller norm) for arbeidet med informasjonssikkerhet, for å få en mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning. Formålet er å sørge for gode rammebetingelser som bidrar til at alle offentlige virksomheter har tilstrekkelig styring av risiko for sine oppgaver og tjenester, legge til rette for effektivt arbeid med informasjonssikkerhet, samstyring i sammenhengende tjenestekjeder og god sikkerhet på tvers av hele forvaltningen.

DigDir har invitert aktører som har ansvar for å veilede virksomhetene til å samarbeide for å gi felles retning på arbeidet med informasjonssikkerhet i offentlig forvaltning.

Styringsevne og samstyring

Som beskrevet i kapittel «KS og kommunene» har KS i sitt oppdrag å koordinere, samordne og samle kommunene innen digitaliseringsområdet. Det er etablert et forpliktende samarbeid basert på samstyringsstruktur for digitalisering, og KS har ansvaret for å ivareta og videreutvikle denne strukturen i samarbeid med de regionale digitaliseringsnettverkene. Nasjonale ambisjoner og visjoner på informasjonssikkerhet, digital beredskap og personvern for kommunesektoren bør derfor håndteres gjennom den allerede etablerte samstyringsstrukturen.

Det er den enkelte kommunedirektør som har ansvar for at kommunen imøtekommer kravene i regelverket, men kommunen kan og bør benytte de eksisterende strukturene for samordning for å best mulig utnytte knappe ressurser. En fordeling av oppgaver bør baseres på et prinsipp om gjenbruk av kompetanse, kapasitet og investeringer.

Gjennom 2022 har det blitt gjennomført et arbeid med prinsipper for utbredelse og samstyring innen informasjonssikkerhet, digital beredskap og personvern i kommunal sektor. Hovedmålet med prinsippene er å sikre en enhetlig og gjenkjennbar samordnings- og samstyringsstruktur for kommunesektoren som når helt ut til den enkelte kommune.

De foreslåtte prinsippene er definert som:

I. Informasjonssikkerhet, digital beredskap og personvern må etableres og inngå i den sentrale samstyringsstrukturen.
II. Nasjonale ambisjoner og visjoner i kommunal sektor innen informasjonssikkerhet, digital beredskap og personvern for kommunesektoren, fastsettes gjennom den etablerte samstyringsstrukturen.
III. Kommunikasjon koordineres mellom KS, digitaliseringsnettverkene og andre relevante aktører, slik at den blir enhetlig mot den enkelte kommune.
IV. Hver region har det helhetlige og strategiske ansvar, og utvikler og forvalter egen plan innen informasjonssikkerhet, digital beredskap og personvern med utgangspunkt i det nasjonale føringene tilsluttet i den etablerte samstyringsstrukturen sett hen til digitaliseringsarbeidet i regionen.

V. Der det av ulike hensyn ikke er aktuelt at ansvaret legges til et digitaliseringsnettverk, kan det lokalt midlertidig pekes på en annen ansvarlig aktør som vertskap for koordineringen.

Endring og styrking av fagrådet og sekretariat i samstyringsstrukturen

I dag er det to fagråd: fagrådet for informasjonssikkerhet og personvern og fagråd for arkitektur.

Det er stadig flere prinsipielle saker som skal behandles i samstyringsstrukturen, og sakene som behandles har behov for en mer tverrfaglig tilnærming. Behovet for prinsipielle avklaringer er fremmet av kommunene, begrunnet i behov for felles tilnærming til kompliserte problemstillinger innen arkitektur, sikkerhet, beredskap og personvern. Fagrådene bør derfor ha en langt mer strategisk og fremtredende rolle enn det som er tilfellet i dag, og bidra aktivt både til modning og retning for kommunal sektor innen arkitektur, sikkerhet, beredskap og personvern.

Fagrådene rolle, sammensetning, funksjon, saksflyt og organisering bør derfor vurderes. Når det gjelder organisering bør det vurderes å slå sammen de to fagrådene for å få en mer helhetlig tilnærming. Alternativ vurdere å ha et overordnet strategisk fagråd hvor de nåværende fagråd blir mer «arbeidene» fagråd til det strategiske fagrådet, eller finne andre egne samhandlingsformer som gir effektiv saksbehandling.

Ved vurdering må det hensyntas de ulike fagområdenes behov for kompetanse, tilgjengelighet og gjennomførbarhet i vurderingene i et stort sakskompleks. En naturlig konsekvens av endringene er behov for endring og justering i mandat og sammensetningen. Det gjelder både krav til kompetanse, tilgjengelighet og kapasitet. Videre bør det også hensynta behovet for at fagrådet skal vurdere prinsipielle problemstillinger og avklaringer på vegne av kommunal sektor.

Fagrådet bør bestå av personer med kompetanse fra ulike fagområder, og med ulik erfaring fra kommunal sektor og bør vurderes plassert i sakflyt mellom fag- og prioriteringsutvalgene og DU. Slik kan fagrådet behandle aktuelle saker innen ulike sektorer før de skal besluttes i enten DU og/eller KommIT.

Det er i dag også et behov for å styrke sekretariatsfunksjonen i samstyringsstrukturen. Det begrunnes med at saksmengden innenfor digitalisering, informasjonssikkerhet, digital beredskap og personvern har økt betydelig og har en svært økende saksmengde.

Faglig støtte til nye felles digitaliseringsprosjekter

For at kommunal sektor i fellesskap skal kunne utvikle flere digitale fellesløsninger, er finansieringsordningen Digifin etablert[35]. KS forvalter ordningen. Hensikten med ordningen er å oppnå økt verdi for brukerne, og lavere utviklings- og forvaltningskostnader for kommunal sektor. Det er medlemmene selv som gjennom KommIT gir KS råd om hvilke prosjekter som bør få støtte.

Prosjektene som får støtte, og dermed prioriteres gjennomført i sektoren, har behov for kompetanse og tilgang på kapasitet innen fagområdene informasjonssikkerhet og personvern. For det enkelte prosjekt er det viktig at tilgangen til kompetanse og kapasitet skjer allerede i konsept- og utredningsfasen, for å sikre at prosjektet hensyntar utfordringsbildet. Det kan også ha en positiv effekt for de ulike fag- og prioriteringsutvalg, ved at de kan dra nytte av disse ressursene i en innledningsfase slik at det oppnås en helhetlig tilnærming til digitalisering. Det er derfor et behov for å tilgjengeliggjøre relevant sikkerhets-, beredskaps- og personvernkompetanse inn i prosjektene som støttes via DigiFin.

[35] https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/finansieringsordning-for-digitaliseringsprosjekter/hvordan-soke-stotte/

Øke samordning med KiNS

KiNS har etablert seg som en aktør som store deler av kommunal sektor benytter seg av, og som medlemmene benytter aktivt både i form av medlemskap og som deltakere i styringsgruppen.

KiNS blir også tidvis gitt mulighet til å representere kommunal sektor i ulike fora. Dette kan ha utfordrende sider, for eksempel i situasjoner der KS og/eller samstyringsstrukturen, gir en uttalelse som er forankret i samstyringsstrukturen, og der KiNS gir en annen uttalelse, tilsynelatende på vegne av kommunal sektor. Det kan da fremstå uklart hva kommunal sektor mener ovenfor 3. part, og samtidig uklart hva som er standpunktet internt i sektoren.

Med utgangspunkt i at kommunal sektor bør tilstrebe en helhetlig tilnærming til andre aktører, men også i og mellom kommunene, er det behov for å øke samordning og grenseoppgang med KiNS.

Kompetansehevende tiltak for kommunal sektor

Som beskrevet under kommunens ansvar, er det nødvendig at den enkelte kommune planlegger og gjennomfører kompetansehevende tiltak for ansatte, fagpersonell og politisk og administrativ ledelse. Digdir, KS og KiNS har flere kompetansehevende tiltak for kommunal sektor kan benytte. Andre statlige har også sektorspesifikke kompetansetiltak som kommunal sektor kan benytte.

Kommunal sektor melder likevel tilbake at tiltakene ikke nødvendigvis er koordinerte fra de ulike aktørene. Koordineringsbehovet og at kompetansetiltak er relevant for kommunal sektor kan løses nasjonalt ved at sentrale aktører ytterligere forsterker sin innsats innen koordinering og relevans for kommunal sektor. Det kan svare ut behovet for kompetansetiltak, samtidig som det letter den enkeltes kommune kostnads- og ressursbruk.

Økt tjenestespekter innen forebygging, oppdagelse og håndtering av digitale angrep

Kommuner og fylkeskommuner har som beskrevet under utfordringsbildet vansker med å beskytte teknisk infrastruktur mot både utilsiktede og tilsiktede hendelser. Situasjonen er krevende fordi kommunene allerede har et opparbeidet gap mellom nåværende og ønsket situasjon. I tillegg forsetter dette gapet å øke fordi digitaliseringen øker i tempo, og nye løsninger og tjenester innføres uten at gamle nødvendigvis saneres eller vedlikeholdes (teknisk gjeld).

Samtidig har den enkelte kommune behov for tjenester som bør adresseres regionalt eller nasjonalt på grunn av de høye kostnadene som vil oppstå dersom hver enkelt kommune skal gjennomføre disse alene. Et sektorvis responsmiljø er ansett som en nødvendig funksjon for å redusere sårbarhet og øke evnen til å forebygge, oppdage og håndtere hendelser i kommunal sektor. Dette fremkommer også i Stortingsmelding 9, *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.* I punkt 3.6.2 beskrives det at «*Regjeringen vil bidra til forebygging av uønskede digitale hendelser i kommunesektoren og vil utpeke et sektorvis responsmiljø som kan dekke kommunenes behov.»*

Pr januar 2023 er det ikke utpekt eller etablert et sektorvis responsmiljø (SRM) for kommunal sektor. En SRM vil i utgangspunktet være en CERT som er sektorens responsmiljø. Flere CERTer, både offentlige og private, arbeider inn mot ulike deler av den kommunale tjenesteproduksjonen, men ingen er utpekt som SRM foreløpig. Det er bevilget 50 MNOK kroner[36] til etablering av et sektorvis responsmiljø for kommunal sektor, noe vil være et viktig bidrag i å dekke sektorens behov, men er på langt nær et svar på alle de utfordringene som er skissert.

Tiltakene som er skissert under «Behov kan møtes regionalt» kan avhjelpe situasjonen, men det vil fortsatt være behov for å etablere ytterligere tjenester som kan tilbys den enkelte kommune. Selv

[36] Jf Prop. 78 S (2021-2022) og Riksrevisjonens rapport «Undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor», s. 30 «Statsrådens svar».

om kommunal sektor har behov for CERT-tjenester, er det ikke CERT-tjenestene alene tilstrekkelig for å øke IT-sikkerheten i sektoren. Tjenestebehovet som beskrevet i denne rapporten, fremkommer også av dokumentasjonen overlevert i KS sitt innspill til nasjonalt program for informasjonssikkerhet i kommunal sektor (NPISK).

Kommunalt Cyber sikkerhets- og kompetansesenter (KCSK)

Det er avgjørende at kommunal sektor har et godt responsmiljø for å oppdage, forebygge og håndtere digitale hendelser. I Norge er det etablert et nasjonalt rammeverk for håndtering av IKT-sikkerhetshendelser[37] (rammeverket). Rammeverket gir føringer for virksomheter, responsmiljø og Nasjonal sikkerhetsmyndighet (NSM).

I dag er det flere responsmiljøer som retter seg mot kommunal sektor. Felles for eksisterende CERT-funksjoner er at de er organisert sektorvis, treffer flere eller ulike deler av kommunal sektor, og har et «typisk» tjenestespekter som «oppfyller» en CERT-funksjon. Det er et behov for å etablere en CERT-funksjon for kommunal sektor, som også kan koordinere mellom øvrige eksisterende CERT-funksjoner.

I Stortingsmelding 9 står det som nevnt at «*Regjeringen vil bidra til forebygging av uønskede digitale hendelser i kommunesektoren og vil utpeke et sektorvis responsmiljø som kan dekke kommunenes behov*[38].» I den forbindelse er det viktig for kommunal sektor å understreke følgende behov:

- At CERT-funksjonen er kontakt- og koordineringspunkt for hele kommunal sektor.
- At kommunal sektor har reell innflytelse på utvikling av CERT-funksjonen og tjenestebehov.
- At kommunal CERT-funksjonen er en del av kommunal samstyringsstruktur.
- At tjenestenivåavtale for samlet CERT funksjon avklares og defineres.

Det er viktig for kommunes funksjonsevne og robusthet at kommunal SRM (CERT) pekes ut og etableres så raskt som mulig.

I vedlegg C beskrives CERT-funksjonen ytterligere. Her vektlegges det at sektor-CERT er informasjonsdeler og veileder. Den største delen av arbeidet innen sikkerhet og beredskap faller dermed på virksomheten, noe som også kommer tydelig frem i rammeverket om virksomhetens plikter når det gjelder hendelseshåndtering.

Rammeverket for håndtering av IKT-hendelser definerer håndtering som *defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense.*

I korthet kan de tre viktigste funksjonene for sektor-CERT oppsummeres som:

- Informasjonsdeling på tvers av sektorene. Slik at når en virksomhet blir angrep i en sektor, at man kan dele angrepsvektorene til de andre virksomhetene i andre sektorer for de skal kunne treffe egnede tiltak for å redusere sårbarheten.
- Ved hendelse, gi råd om videre håndtering og hvem som bør involveres i den videre hendelseshåndteringen.
- Gi råd til virksomheter om tiltak for å bedre grunnsikring.

Kommunal sektor har behov for følgende kapabiliteter (ikke uttømmende liste) ut over de «tradisjonelle» CERT-tjenestene:

[37] https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/

[38] https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

- Sårbarhetsskanning (deteksjon): Oppdage kjente sårbarheter og avdekke den totale sårbarhetsflaten for eksponerte tjenester for å muliggjøre sårbarhetsreduksjon og sikkerhetstilstand, samt verifisere etablerte sikkerhetstiltak.
- Varsling: Autoritativ kilde for og distribusjon av informasjon om nye sårbarheter, anbefalte tiltak og kjente hendelser, og mottak av varslinger fra sektoren.
- Sjekkliste og bistand sårbarhetsreduksjon: Oppdatere og distribuere sjekklister, bistand til reduksjon av sårbarheter med metode og kapasitet.
- Bistand til å utarbeide beredskapsplaner innen digital sikkerhet.
- Bistand til hendelseshåndtering: Bidra til ledelse- og teknisk bistand i ulike hendelsesfaser.
- Bistand sikkerhetstesting (både automatisert og manuell): Sikkerhetstesting, testing av konfigurasjon/oppsett mv.
- Overordnet situasjonsoversikt: Bidra til lokal, nasjonal og global situasjonsforståelse for teknisk personell, administrativ og politisk ledelse i kommunene.
- Bistand til anskaffelser, kvalitetssikring av anskaffelser og leverandøroppfølging- og revisjon
- Sentral overvåkningskapabilitet (SOC) og sentral hendelseshåndtering (IRT)
- Rådgivning og kompetanseutveksling: Sparringspartner for digitaliseringsnettverkene og kommuner innenfor informasjonssikkerhetsområdet.

Basert på behovet til kommunal sektor, se også tabellen nedenfor, bør det vurderes og etablere en nasjonal cyber sikkerhets- og kompetansesenter i kommunal sektor (KCSK) hvor kommunens responsmiljø (SRM, kommunenes CERT) er en integrert del av denne.

KCSK bør, i tråd med kommunale behov, ha et bredt tjenestespekter for å øke evnen til å forebygge, oppdage og håndtere hendelser i kommunal sektor:

<table>
<tr><th colspan="3">Tjenestebehov i et kommunalt KCSK[39]</th></tr>
<tr><td colspan="3">Administrativt
- Drift av tjenestene
- Rådgivning
- Sikkerhets- og beredskapsplaner
- Kvalitetssikring anskaffelser
- Felles kTommunale sikkerhetskrav og teknologisk forvaltning
- Felles ROS
- Felles personvernkonsekvensvurderinger</td></tr>
<tr><th>Forebyggende</th><th>Oppdagende</th><th>Håndterende</th></tr>
<tr><td>Operasjonelt
- Overordnet situasjonsoversikt
- Sikkerhetstesting og Red team
- Bistand med sårbarhetsreduksjon
- Gjennomføre Digital Due Dilligence
- Utarbeide og gjennomføre øvelser
- Bistand med sikkert oppsett av sentrale gjennomgående sektor systemer
- Kapasitet til onboarding av kommuner

Drift og forvaltning
- Ansvar felles sikkerhetstjenester
- Ansvar for kommunikasjonsnettverk</td><td>- Nasjonal alarmfunksjon, SOC 24/7
- Varsling
- koordinering med andre nasjonale sikkerhetsmiljøer.</td><td>- Nasjonal kommunal IRT
- Bistand gjenoppretting til normal drift
- Nasjonal virtuell operativ kommunal sikkerhetsorganisasjon</td></tr>
</table>

Basert på skisserte utfordringer i kommunal sektor, se ytterligere beskrivelse i vedlegg F, 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.

[39] Tjenesteaspektet beskrevet her er ikke er uttømmende og beskriver kun de nødvendige kjernetjenestene meldt inn av kommunene gjennom innsiktsarbeidet.

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 som har gjennomgått kommunal SOC-funksjon anbefaler en to-delt løsning som kan imøtekomme utfordringene med kompetanse og konsumeringsevne:

- *det etableres en nasjonal alarmsentral, SOC,* fortrinnsvis tilknyttet til DIF (Digital tjenester i KS) 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.

Som beskrevet i vedlegg B «Utfordringsbildet i kommunal sektor», er det avgjørende at kommunene har et tydelig søkelys på det forebyggende arbeidet. Det er sentralt å ha «orden i eget hus» for å kunne få utbytte av både KCSK, CERT, samt overvåknings- og sikkerhetstjenester.

Kommunal sektor har behov for at kommunal SRM (CERT) utpekes så raskt om mulig, og i en forlengelse av dette, utrede en kommunal KCSK for å imøtekomme det totale utfordringsbildet.

Behov for felles kommunale sikkerhetskrav, både internt og eksternt

I dag finnes det ulike sett med sikkerhetskrav. Disse er gjerne generelle krav og er rettet mot anskaffelse og veiledninger av generell karakter. Kommunal sektor etterlyser i sterk grad spesifikke og operative rettede sikkerhetskrav for anskaffelse, sikker drift, oppfølgning og forvaltning. Videre er det behov for anbefalte sikkerhetskrav til egen drifts- og forvaltningsorganisasjon og prosesser for å ivareta trygg og sikker digitalisering.

Behov for felles tilnærming til personvern

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 henvises her også til personvernkommisjonens utredning, NOU 2022:11[40], *Ditt personvern – vårt felles ansvar — Tid for en personvernpolitikk* for ytterlige informasjon i forbindelse med de utfordringene som teknologien representerer innen personvernområdet.

Kommunal sektor etterlyser en samlet og helhetlig tilnærming til området, ikke bare personvern i forhold til konfidensialitet, men også integritet og tilgjengelighet. Dette er spesielt viktig i forhold til teknologier som kan være avgjørende i forhold liv og helse og andre viktige samfunnsområder, men som ikke nødvendigvis gir den ønskede beskyttelse av personvernet.

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.

[40] https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/

Påvirkning i det digitale rom

Det digitale rom beskrives gjerne som en «verden» av sammenkoblede datasystemer og nettverk og betegnes også ofte som «cyber space».

Proposisjon 78 S (2021-2022) påpeker også at risikoen for at land som Russland benytter ikke-militære virkemidler som digitale angrep, og etterretnings- og påvirkningsaktiviteten øker, også i Norge. Dette bekreftes videre av PSTs trusselvurdering for 2022.

Med utgangspunkt i den geopolitiske sikkerhetssituasjonen og konsekvensene av påvirkningsoperasjoner vil det være avgjørende at kommunal sektor har nødvendig robusthet til å kunne håndtere påvirkningsoperasjoner i det digital rom.

For å ivareta demokratiet, rettssikkerheten, og nasjonens funksjonsevne blir det derfor avgjørende at man evner å løfte samtlige kommuner for å gjøre dem mer robust mot påvirkning i det digitale rom.

Behov for sentrale vurderinger av systemer og behandlinger

Samtlige kommuner er forpliktet til å gjennomføre risiko- og sårbarhetsanalyse (ROS) på de systemene som tas i bruk. Flere kommuner har ikke nødvendig kapasitet eller kunnskap for å gjennomføre vurderinger og implementere tilhørende tiltak, som kan resultere i manglende risikoforståelse og mulig økt angrepsflate. Det er heller ikke hensiktsmessig ressursbruk at samtlige kommuner og fylkeskommuner gjennomfører de samme vurderingene.

KS og Bergen kommune gjennomfører i 2023 et prosjekt for å teste ut en nasjonal vurdering av personvernkonsekvenser (DPIA) for Googles produkter og tjenester i skolen. Dette gjøres i regi av SkoleSec prosjektet[41]. Målet med prosjektet er å samle erfaringer for samstyring og samordning av slike prosesser. I begrunnelsen for sentral gjennomføring av DPIA for Google, fremmes det at det er utfordrende for kommunene å gjennomføre vurderinger knyttet til personvern og informasjonssikkerhet i løsninger som tas i bruk[42].

Kommunal sektor har derfor gitt utrykk for at det gjøres felles vurderinger av sentrale systemer og behandlinger så langt det lar seg gjøre. Det er viktig å bemerke at det fortsatt foreligger et behov i den enkelte kommune for restvurderinger. Det er derfor også behov for at det utarbeides veiledningsmateriell som muliggjør at den enkelte kommune kan gjennomføre de nødvendige vurderinger i egen virksomhet. Behovet for sentrale vurderinger er størst for de største tjenestene- og systemene, eksempelvis M365. Erfaringene fra vurderingene av Google, men også erfaringene fra vurderingene tilgjengeliggjort av FIKS-plattformen, bør benyttes inn i gjennomføringen av nye vurderinger.

Utvikle nasjonal virtuell operativ kommunal sikkerhetsorganisasjon

Noen kommuner ha få sikkerhets-, beredskaps- og personvernressurser, mens andre kommuner har sikkerhetsavdelinger. Det å være «alene» kan ofte være utfordrende, både når det gjelder kompetansehevning ettersom kompetansehevning nødvendigvis ikke betyr å gå kurs, men vel så viktig og være del av et miljø. Det å ha et miljø rundt seg er viktig, både for å kunne sparre og å få tilgang til vurderinger som andre har gjort på sikkerhetsområdet.

[41] https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/personvernkonsekvenser-for-googles-produkter-i-skolen-skal-vurderes/

[42] https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/personvernkonsekvenser-for-googles-produkter-i-skolen-skal-vurderes/

Det er mange dyktige operative kompetente personer som arbeider i kommunene. Disse personene bør settes i forbindelse med hverandre på tvers av Norge slik at tilgjengelig kompetanse kan utnyttes best mulig, f.eks. gjennom en virtuell operativ kommunal sikkerhetsorganisasjon.

En slik type operativ virtuell organisasjon vil gi gevinster på mist tre plan;

- Ved hendelser eller for å gjennomføre øyeblikkelige» tiltak kan kommunene dra veksler på «hele» kommune-Norge (all tilgjengelig kompetanse i sektor nasjonalt).
- Kompetanseutveksling mellom kommunene kan skje raskere.
- Adressering av sikkerhetsproblemer og tiltak kan skje raskere på tvers av hele kommunal sektor, hvor «hele» kommune-Norge vil være løpende informert og involvert.

Det anbefales at det utredes nærmere hvordan en slik virtuell organisasjon kan realiseres.

Oppsummering og anbefaling om tiltak

Anbefalingene som følger av behovsbeskrivelsen søker å imøtekomme behovet for bedre ressursutnyttelse av allerede eksisterende ressurser i sektoren, og lavere kostnader for tjenester som kommunene har behov for, men som de ikke har tilgjengelig i dag.

Anbefaling om tiltak nasjonalt (detaljert tiltaksliste er beskrevet i vedlegg A):

Tiltak	Beskrivelse
2	Vedta prinsipper for informasjonssikkerhet, personvern og i digital beredskap for kommunal sektor i samstyringsstrukturen.
3	Arbeide for å få etablert et kommunalt sektorvis responsmiljø (SRM).
4	Utrede etablering av kommunal cyber sikkerhets- og kompetansesenter (KCSK) med utvidet tjenestespekter tilpasset kommunenes behov.
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.
6	Vurdere forslaget om styrking av sekretariatsfunksjon i samstyringsstrukturen i KS.
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.
8	Delta i Digitaliseringsdirektoratet initiativ «Felles sikkerhet i forvaltningen med ressurser fra kommunal sektor.
9	Øke samordning med KiNS.
10	Gjennomføre sentrale vurderinger av systemer og behandlinger (ROS/DPIA).
11	Utvikle kompetansetiltak for kommunal sektor for ansatte, fagpersonell, politisk ledelse og administrativ ledelse innen digitalisering, sikkerhet, beredskap og personvern.
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.
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.
14	Vurdere å etablere en nasjonal virtuell operativ kommunal sikkerhetsorganisasjon.
15	Vurdere å tilgjengeliggjøre kompetanse inn i felles nasjonale digitaliseringsprosjekter finansiert gjennom DigiFin.
16	Fagområdene personvern, informasjonssikkerhet og digital beredskap innarbeides i ulike digitaliseringsstrategier i kommunal sektor.

Vedlegg A – Detaljert oversikt over foreslåtte tiltak

Vedlegg B – Utfordringsbildet i kommunal sektor

Vedlegg C – Dagens aktørbilde for kommunal sektor innen digital sikkerhet

Vedlegg D – Definisjoner og forkortelser

Vedlegg E – Metode og datagrunnlag

Vedlegg F – Fagnotat SOC

Vedlegg G – Evaluering av sektorvise responsmiljøer

Vedlegg H – Digitaliseringsbrev til kommuner og fylkeskommuner

Vedlegg I – Vedlegg I - RSB - versjon 1.0 - Referansearkitektur sikkerhet beredskap og personvern (Akson-prosjektet)