Vedlegg C, Dagens aktørbilde for kommunal sektor innen digital sikkerhet

Innhold

Aktørbilde for kommunal sektor innen digital sikkerhet

Kommunal sektor er ikke en tradisjonell fagsektor, men først og fremst et selvstendig forvaltningsnivå som består av mange fagområder- og sektorer. Det tilbys tjenester og veiledning til kommunal sektor innen sikkerhet fra rekke offentlige aktører, men det meste av veiledninger springer ut fra sektorprinsippet og sektormyndigheter. Sektortjenester- og tilbydere treffer med det kommunal sektor i ulike deler av tjenesteleveransen og ulike fagsektorer i forvaltningen. Disse tjenestene og veiledningene kan være delvis eller fullstendig overlappende, og kan være forvirrende å orientere seg i.

I tillegg kommer tjenester og produkter som leveres av eventuelle private leverandører. Hvem og hvor den enkelte kommune mottar tjenester, produkter og veiledning fra er med det også et kostnadsspørsmål.

En slik innretning er lite ressurseffektivt og bidrar til et fragmentert sikkerhetsarbeid i kommunal sektor. Utover kommunene selv og deres operative håndtering, kan aktørbildet systematiseres overordnet inn i tre kategorier:

1) Veiledende
2) Rådgivende og forebyggende
3) Operasjonelle (håndtering av hendelser)

Veiledende aktører

Det er en rekke veiledende aktører for kommunene og fylkeskommunene. Sentrale veiledningsaktører er KS, Datatilsynet, Digitaliseringsdirektoratet (DigDir), Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB), Direktoratet for forvaltning og økonomistyring (DFØ) for å nevne noen. I tillegg kommer andre aktører som gir fagsektorspesifikk veiledning, slik som for eksempel Utdanningsdirektoratet og Direktoratet for e-helse.

Felles for disse aktørene er at de utarbeider nasjonale eller sektorspesifikke veiledninger innen informasjonssikkerhet og personvern. Aktørene gir også generelle råd om hvordan veilederne best kan benyttes i den enkelte virksomhet. Det krever at virksomheten har en egen kapasitet og faglig kompetanse til å omsette veiledning og rådene inn i egen virksomhet og arbeid.

Rådgivende og forebyggende aktører

Rådgivende og forebyggende aktører bistår den enkelte virksomhet ved å gi råd eller gjennomføre tiltak. Disse aktørene bidrar ofte med trusselvurderinger og anbefaling om konkrete tiltak. Aktører er de ulike CERT-miljøer[1], nasjonale aktører som NSM, Nasjonalt Cyber Crime Center (NC3), DSB og en rekke private aktører.

Det er flere kommuner som er medlem i varslingssystem for digital infrastruktur (VDI) og sårbarhetskartleggingstjenesten Allvis NOR i regi av NSM. En stor andel av kommunene er også en del av det nasjonale beskyttelsesprogrammet (NBP) i regi av HelseCERT, hvor andre er tilknyttet andre CERT-miljøer. Videre tilbys det ulike tilbud som sikkerhetsovervåkning, kurs, sertifiseringer og retningslinjer av både kommersielle og offentlige aktører og som kommunal sektor benytter seg av.

[1] CERT står for Computer Emergency Response Team. Se mer om CERT under «Om CERT».

Operasjonelle aktører

Operasjonelle aktører bistår virksomheten med hendelseshåndtering og koordinering ved sikkerhetshendelser. Aktørene kan analysere og bistå med håndtering av hendelsen. Det kan også innebære koordinering mellom ulike aktører. Aktører som bistår med dette er gjerne CERT-miljøer, NSM og private aktører.

I tillegg finnes en rekke kommersielle aktører som tilbyr hjelp til forebygging, bistand og håndtering ved hendelser i ulike nivåer, f.eks. å tilby bistand til å håndtere hele hendelsen og gjenoppretningen.

Det er viktig å understreke at CERT-miljøene ikke tar over hele hendelseshåndteringen lokalt, men bistår på et overordnet nivå. Det innebærer at det er kommunen selv som i all hovedsak må gjøre arbeidet med å håndtere selve hendelsen og gjenoppretningen til normal drift etter hendelsen. Det er derfor avgjørende at kommunal sektor har en egenevne til hendelseshåndtering.

Utfordringen her, i likhet med veiledningsaktørene og rådgivende og forebyggende aktører, er at det er mange aktører som treffer kommunal sektor og dermed kan det være vanskelig for kommunene og orientere seg hvem de skal være tilknyttet og hvilke tjenester de kan mottar.

Om CERT

CERT står for Computer Emergency Response Team og er en koordinerende enhet for informasjonssikkerhet. CERT er et registrert varemerke eid av Carnegie Mellon University. CERT-funksjonen kan grovt sett inndeles i tre kategorier: reaktive tjenester, proaktive tjenester og rådgivningstjenester.

Reaktive tjenester utløses dersom det har skjedd en hendelse, varsel om angrep, ondsinnet programvare, sårbarheter eller forsøk på innbrudd. Det kan være varsling av hendelser, håndtering av hendelser, sårbarhetshåndtering og lignende. Reaktive tjenester er det grunnleggende i enhver CERT.

Proaktive tjenester er informasjon og veiledning med hensikt om å forberede, beskytte og sikre systemer i påvente av angrep og hendelser. Det kan være sikkerhetsrevisjoner, konfigurering og vedlikehold, utvikling av verktøy, overvåkning og formidling. Formålet er å redusere antall hendelser og risikoen for at en hendelse inntreffer.

Formålet med rådgivingstjenester er å gi utvidet forståelse og god informasjon til virksomheten slik at virksomheten er bedre rustet til å håndtere hendelser i fremtiden. Det kan innebære risikovurderinger, beredskapsplanlegging, rådgivning og opplæring.

Tabellen nedenfor gir en oversikt over tjenester man normalt kan forvente (ikke uttømmende liste) i disse tre tjenestekategoriene. En CERT kan levere en eller flere av tjenestene, men samtlige sektor-CERT leverer reaktive tjenester som er opplistet i tabellen under.

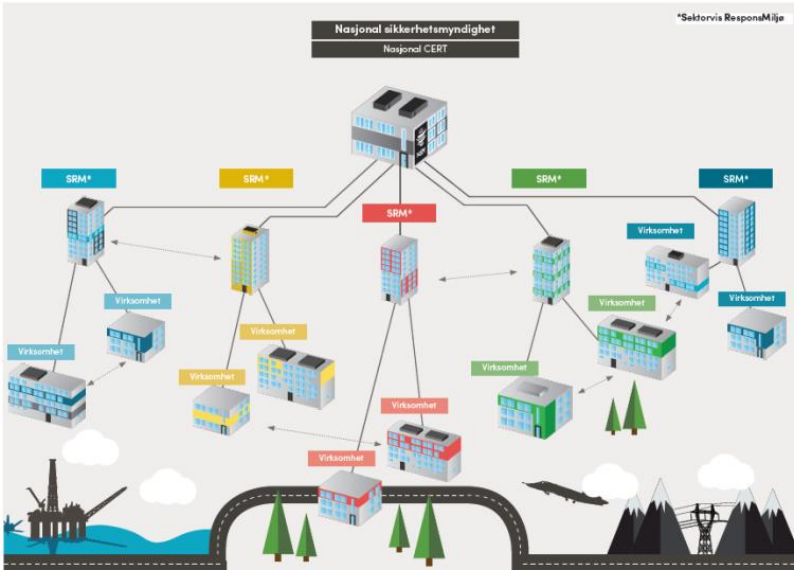
Reaktive tjenester	**Proaktive tjenester**	**Rådgivingstjenester**
Varsling Sårbarhet og hendelseshåndtering - Analyse - Bistand - Koordinering	Formidle sikkerhetsinformasjon og trusselbildet Overvåking av ekstern infrastruktur (typisk ekstern Internettrafikk) Utvikling av sikkerhetsverktøy Sikkerhetstesting	Risikoanalyser Katastrofe- og beredskapsplanlegging Sikkerhetsrådgivning Bevisstgjøring og opplæring

		Øvelser innen hendelseshåndtering og beredskap

The European Agency for Network and information security (ENISA) har også beskrivelser om CERT-funksjoner, men har et ekstra søkelys på den nasjonale CERT-funksjonen.

Rammeverk for håndtering av IKT-sikkerhetshendelser beskriver en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal sektorovergripende håndteringsevne, hvor det enkelte departements konstitusjonelle ansvar også ivaretas[2].

I Norge er det utpekt sektorvis responsmiljø (SRM) innen flere sektorer. Det er blant annet NCSC, HelseCERT, KraftCERT, FinansCERT, eduCSC (tidligere Uninett CERT) og EkomCERT.



Figur 1 - Kommunikasjon mellom NSM, SRM og virksomheter i og mellom sektorer (Rammeverk for håndtering av IKT-hendelser, s. 12)

Ettersom kommuner består av flere sektorer er det flere sektor-CERT som treffer kommunene. Dette er for eksempel HelseCERT, NCSC KraftCERT. I tillegg finnes det CERT/CSIRT-funksjoner som ikke er utpekt SRM, men leverer tilsvarende tjenester til sektoren.

Riksrevisjonen påpeker at SRM skal fungere som et bindeledd mellom NCSC og virksomhetene i sektoren, men viser til at SRM i enkelte sektorer bidrar til forsinkelser i håndtering og informasjonsflyt. En evaluering av ordningen med sektorvise responsmiljøer som ble utført av KPMG i 2022, viser til flere utfordringer med ordningen, blant annet uklar ansvars- og rolleforståelse og mangel på tilgang på relevant kompetanse. Som en forlengelse er det tilbakemeldinger fra de ulike CERT-miljøene om variasjon i hvor mange kommuner som har evne å motta de tjenestene som CERT-miljøene tilbyr.

[2] https://nsm.no/getfile.php/133853-1593022504/NSM/Filer/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Sektorvis responsmiljø som treffer kommunal sektor

HelseCERT

HelseCERT ble etablert av Helse- og omsorgsdepartementet (HOD) i 2011 og er hovedsakelig finansiert gjennom statsbudsjettet. HelseCERT er utpekt av HOD som helse- og omsorgssektorens responsmiljø (SRM). Hovedoppgaven til HelseCERT er å øke helse- og omsorgssektorens evne til å oppdage, forebygge og håndtere alvorlige cyberangrep[3].

CERT-tjenester som HelseCERT leverer er pakket inn i programmet nasjonalt beskyttelsesprogram (NBP). Tjenester i NBP inkluderer blant annet informasjonsdeling, forebygging, rådgivning, hendelseshåndtering, sårbarhetsskanning og inntrengingstesting. HelseCERT leverer gjennom NBP både reaktive og proaktive tjenester.

Alle som tilbyr helsetjenester i Norge, kan bli medlem. Det gjelder også for virksomheter tilknyttet helsenettet, eller driftsleverandører for helsetilbydere. I februar 2023 er 336 av landets 356 kommuner, hele spesialisthelsetjenesten og et par hundretalls små og store virksomheter som leverer tjenester i Helsenettet tilknyttet HelseCERT gjennom NBP.

Det er viktig å understreke at selv om 336 av 356 kommuner er tilknyttet NBP, er ikke HelseCERT SRM for kommunal sektor. Det er først og fremst rettet mot helse- og omsorgssektoren, og ikke den totale virksomheten som kommunal sektor driver og forvalter.

Nasjonalt cybersikkerhetssenter (NCSC)

NCSC er en del av NSM og ble etablert i 2018. NCSC er det nasjonale senteret for forebygging, avdekking og bekjempelse av trusler og kriminalitet i det digitale rom. Det er en arena for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet.

Senteret har også den nasjonale responsfunksjonen av alvorlige digitale angrep i Norge, og drifter varslingssystemet for digital infrastruktur (VDI).

KraftCERT/InfraCERT

KraftCERT/InfraCERT er underlagt Olje- og energidepartementet (OED) og er SRM for kraft og petroleum, men har også målgruppen prosessindustri, vann- og avløpssektor og energigjenvinning.

Tjenester som leveres av KraftCERT/InfraCERT er både reaktive og proaktive tjenester som sårbarhetsovervåkning, trusseletterretning, deteksjon, hendelseshåndtering, kurs, rådgivning og bistand til øvelser. KraftCERT jobber for god, sikker og effektiv hendelseshåndtering og informasjonsdeling mellom relevante selskaper nasjonalt og internasjonalt[4]. Tjenestene som KraftCERT/InfraCERT tilbyr treffer den kommunale forvaltningen, men i begrenset omfang. Det omfatter noen kommunale vannverk og interkommunale vannverk.

Kommune CSIRT

Kommune CSIRT er et interkommunalt selskap (IKS) dannet av Lillehammer og Gjøvik kommune i 2019 og operasjonalisert i 2020. Opprettelsen av Kommune-CSIRT var en anbefaling fra utredning gjennomført av NorSIS i samarbeid med Lillehammer og Gjøvik kommune[5]. Kommune CSIRT har et

[3] https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/om-oss

[4] https://www.kraftcert.no/no/#om

[5] https://norsis.no/content/uploads/2022/06/KommuneCSIRT-print.pdf

mål om å være en nasjonal ressurs for alle landets kommuner og fylkeskommuner[6]. Kommune CSIRT har i februar 2023 i overkant av 50 kunder og finansieres gjennom disse

Kommune CSIRT tilbyr tjenester som informasjonsdeling, rådgivning, skanning, samt støtte og koordinering ved hendelser. Kommune CSIRT er ikke utpekt som sektorvis responsmiljø (SRM) for kommunal sektor av KDD, men er midlertidig medlem av SRM-strukturen.

Særlig om CERT

I Norge har man nasjonalt rammeverket for håndtering av IKT-sikkerhetshendelser[7] (rammeverket). IKT-hendelser er definert i rammeverket 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.*

Rammeverket gir en god innføring og veiledning på hva som forventes av virksomheten, sektor-CERT og den nasjonale CERT-funksjonen. Videre gir den også til en viss grad hvilke tjenester en CERT bør inneha.

Videre beskriver rammeverket:

Departementene er ansvarlige for å oppnevne SRM i sektorene og for å sikre at SRM til enhver tid oppfyller gjeldende krav og forventninger som stilles til denne funksjonen. Det enkelte departementet har stor fleksibilitet knyttet til å vurdere hvorvidt det er hensiktsmessig med ett eller flere SRM i egen sektor, eller om det for noen sektorer kan være hensiktsmessig med tverrsektorielle SRM.

IKT-sikkerhet er først og fremst den enkelte virksomhets ansvar. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet under normale forhold, også har et ansvar i en krisesituasjon. I praksis innebærer dette at ansvaret for å håndtere IKT-sikkerhetshendelser ligger hos eier av virksomheten, uavhengig av om denne befinner seg i privat eller offentlig sektor.

Tar man utgangspunkt i rammeverket gir det en god veiledning på hvilken kapasiteter en sektor-CERT skal inneha og hvilken bistand de skal yte virksomhetene som er tilknyttet Sektor-CERT. Dette kan oppsummeres som;

- Arrangere møter for erfaringsutveksling og samhandling for virksomheter i sektor.
- Ha kompetanse om relevante systemer i sektor og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå.
- Kunne gi råd om videre håndtering og hvem som skal involveres i hendelseshåndteringen.
- Varsle om IKT-sikkerhetshendelser i sektoren til NSM, andre SRM og til relevante virksomheter.
- Ha oversikt over omfang av hendelsen og se hendelser innenfor samme sektor i sammenheng og gi råd om tiltak til virksomheter innenfor sektoren.
- Støtte virksomheter i egen sektor ved evaluering av hendelser.
- Gi råd til virksomheter om tiltak for å bedre grunnsikring.

Som man ser av det ovennevnte legges det i stor grad opp til at sektor-CERT er informasjonsdeler og veileder. Den største del av arbeidet innen sikkerhet og beredskap faller på virksomheten, noe som også kommer tydelig frem i rammeverket om virksomhetens plikter når det gjelder hendelseshåndtering.

[6] https://kommunecsirt.no/om-oss

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

Det innebærer at skjer det en hendelse så er det ikke slik at CERTen kommer og «rydder opp». CERT vil bistå med informasjonsdeling og råd, men selve hendelseshåndtering må kommunen gjøre selv i stor grad.

På oppdrag for Justis- og beredskapsdepartementet (JD) har KPMG gjennomført en evaluering av ordningen med sektorvise responsmiljøer (SRM), se vedlegg G.

Evalueringen har identifisert flere utfordringer i dagens ordning:

- *Ulikheter i organisering og virkemåte kan føre til at det oppstår gap og uklare grensesnitt, og hvor enkelte sektorer og/eller virksomheter ikke dekkes tydelig av et SRM.*
- *Det er ulike tolkninger av hvorvidt føringer gitt i rammeverket er krav eller veiledende.*
- *Det er et gap mellom cybersikkerhetsområdets sektorovergripende natur og sektorprinsippet i staten.*
- *Det fremkommer ikke i rammeverket hvilken rolle private leverandører av IKT-infrastruktur og andre samfunnsviktige tjenester skal ha i den overordnede modellen.*
- *Et utfordrende rekrutteringsmarked og begrenset tilgang på relevant kompetanse*
- *Det er uklarheter knyttet til rolle- og ansvarsfordelingen i hendelseshåndtering.*

Det finnes ingen formell beskrivelse på hvilken kapasitet, kompetanse eller tjenester en CERT skal levere. Dette er helt opp til CERTen. Noen CERT plasserer sensorer ut i virksomhetene for å få bedre oversikt over trusselbildet og tilbyr sikkerhetstester, mens atter andre CERT er «informasjonsbærer» og er rådgivende på et overordnet plan.

I korthet kan man oppsummere tre av de viktigste funksjonene for sektor-CERT:

- 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.

Det er flere sektor-CERT som treffer kommunene, f.eks. HelseCERT og KraftCERT (og til viss grad nasjonale NorCERT[8]), derfor blir det også viktig for kommune og ha «et telefonnummer» og forholde seg til, slik CERT innad kan koordinere seg.

Det å knytte seg til CERT løser ikke «alle» sikkerhetsproblem for kommunen, men er en god «sparringspartner» for kommunen på flere områder.

[8] Norges nasjonale CERT, NorCERT (Norwegian Computer Emergency Response Team), er en funksjon i Nasjonalt cybersikkerhetssenter, se https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering

Offentlige aktører innen digital sikkerhet som treffer kommunal sektor

Det er flere offentlige aktører som treffer kommunal sektor. Nedenfor gjennomgås noen av de viktigste med hensyn til digital sikkerhet i kommunal sektor.

Digitaliseringsdirektoratet

Digitaliseringsdirektoratet (DigDir) skal være Regjeringens fremste verktøy for raskere og mer samordnet digitalisering av samfunnet. DigDir er underlagt kommunal- og moderniseringsdepartementet (KDD). Innenfor området informasjonssikkerhet skal DigDir være samordner og pådriver for forebyggende informasjonssikkerhet i offentlig sektor.

I tråd med sitt mandat har DigDir utarbeidet veiledningsmateriell innen informasjonssikkerhet, og da spesielt veiledning innen internkontroll. Videre administrerer DigDir et nettverk for informasjonssikkerhet for offentlige ansatte. Målsettingen med nettverket er å dele erfaringer om arbeid med informasjonssikkerhet på tvers av offentlige virksomheter.

Selv om DigDir arbeider til viss grad med personvernproblemstillinger er hovedfokuset til DigDir det som tradisjonelt kan karakteriseres som styringssystem for informasjonssikkerhet med tilhørende aktiviteter rundt dette.

Direktoratet for forvaltning og økonomistyring (DFØ)

DFØ er statens fagorgan for økonomistyring og skal bidra til å produsere gode beslutningsgrunnlag for statlige tiltak, god organisering og ledelse i staten, samt anskaffelser i offentlig sektor. Direktoratet leverer i tillegg lønns- og regnskapstjenester til over 90 prosent av statsforvaltningen.

DFØ har også ansvar for markedsplassen for skytjenester. Markedsplassen skal være møteplassen for oppdragsgivere og tilbydere av skytjenester når offentlig sektor skal investere i og anskaffe skyteknologi. Det skal gjøre det enklere for offentlige oppdragsgivere å anskaffe sikre, lovlige og kostnadseffektive skytjenester. Det er tilgjengeliggjort både fellesavtaler og veiledning for kjøp av skytjenester. Det skal også være en plass der tilbydere kan presentere sine tjenester og slik bidra til bedre oversikt over markedet for skytjenester.

DFØ treffer kommunal sektor spesielt med hensyn til markedsplassen for skytjenester og da særlig veiledningsmateriell om sikkerhets- og risikovurdering ved anskaffelse av skytjenester.

Direktoratet for samfunnssikkerhet og beredskap (DSB)

DSB skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og skal sørge for god beredskap og effektiv ulykkes- og krisehåndtering. DSB har ansvar for at viktige samfunnsfunksjoner har tilgang til et trygt, robust og tidsmessig kommunikasjonssystem for ledelse og samhandling i daglig virke og ved større hendelser. Direktoratet eier Nødnett og har ansvar for forvaltning og videreutvikling av det i tråd med brukernes behov.

DSB skal også ifølge instruks for departementenes arbeid med samfunnssikkerhet understøtte departementets koordineringsrolle innenfor samfunnssikkerhet og beredskap, og legge grunnlaget for helhetlig forebyggende arbeid og beredskapsforberedelser innenfor offentlig forvaltning og samfunnskritisk virksomhet.

DSB skal bidra også bidra til god digital sikkerhet i samfunnet. DSM eier derfor plattformen ovelse.no som driftes av Norwegian Cyber Range ved Norges teknisk-naturvitenskapelige universitet (NTNU). Øvelser for bedre digital sikkerhet omfatter alle scenarioene på denne plattformen, og disse er utviklet i et samarbeid mellom DSB, NTNU, NorSIS, Digitaliseringsdirektoratet og Nasjonal sikkerhetsmyndighet (NSM).

Nasjonal sikkerhetsmyndighet (NSM)

NSM er direktorat for forebyggende nasjonal sikkerhet. gir råd og gjennomfører tilsyn på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også et nasjonalt ansvar for å avdekke, varsle og koordinere alvorlige IKT-angrep. NSM har et overordnet ansvar for at sikkerhetstilstanden i alle sektorer blir kontrollert, og skal se til at alle virksomheter oppfyller lovpålagte krav. NSM er utpekt som ansvarlig styresmakt etter sikkerhetsloven til å drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur (VDI).

Direktoratet for e-helse

Direktoratet for e-helse skal sørge for nasjonal styring og koordinering i samarbeid med helseforetak, kommuner, fagmiljø og interesseorganisasjoner. Videre skal direktoratet for e-helse styrke digitaliseringen i helse- og omsorgssektoren for å understøtte effektive og sammenhengende helse- og omsorgstjenester. Direktoratet er også sekretariatet for Normen. Normen er en bransjenorm for informasjonssikkerhet og personvern, og er utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren.

Normen er lagt opp som et kravsett til helsevirksomhetene innen risikostyring, personvern og informasjonssikkerhet. Normen er ikke bindende i seg selv for virksomheter, men man blir forpliktet til å følge Normens krav via avtale med Norsk Helsenett (NHN), som gir adgang til det nasjonale, krypterte helsenettet.

Ettersom mange kommuner benytter NHN, har store deler av kommunal sektor forpliktet seg til å følge Normens krav.

Datatilsynet

Datatilsynet er et uavhengig forvaltningsorgan administrativ underordnet kommunal- og distriktsdepartementet (KDD). Datatilsynet er både tilsyn og ombud og har som oppgave å føre kontroll med at personvernregelverket etterleves, og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Kommunal sektor treffes av Datatilsynet både som tilsynsmyndighet og som veiledningsaktør. Alle meldepliktige avvik etter personvernforordningen skal meldes til Datatilsynet, som medfører at hele kommunal sektor i større eller mindre grad er i kontakt med Datatilsynet jevnlig.

Statsforvalteren

Statsforvalteren er statens representant i fylket og har ansvar for å følge opp vedtak, mål og retningslinjer fra Stortinget og regjeringen. Statsforvalteren er dessuten et viktig bindeledd mellom kommunene og sentrale myndigheter. Statsforvalteren driver også tilsyn, der Statsforvalteren fører tilsyn med kommunal styring, samfunnssikkerhet og beredskap.

Statsforvalteren er også ved flere anledninger pådriver til samling av kommunal ledelse, og igangsetter av ulike initiativ som øvelser og temamøter. Det er muligheter for å søke Statsforvalteren om skjønnsmidler, noe flere kommuner muliggjør seg av. Det er eksempler der Statsforvalteren bevilger midler til vurdering av digital modenhet, utredning av muligheter for sikkerhetssamarbeid og lignende.

KS og kommunene

KS er kommunesektorens organisasjon og er sektorens arbeidsgiverorganisasjon og interessepolitiske aktør. I tillegg til disse to rollene har KS en viktig oppgave som utviklingspartner for medlemmene. Alle landets kommuner og fylkeskommuner er medlemmer.

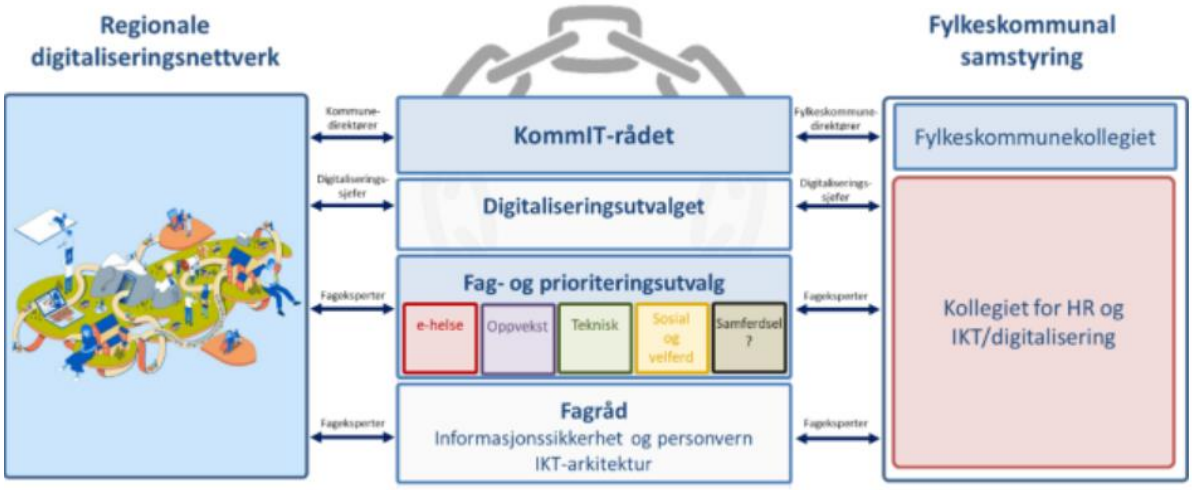
De siste årene har KS fått en sterkere rolle i å samordne sektoren, og understøtte kommunenes og fylkeskommunenes digitaliseringsarbeid. KS har i samarbeid med medlemmene etablert en rekke råd og utvalg som skal bidra til koordinering og samordning på digitaliseringsområdet i sektoren. Den strategiske samordningen foregår i dag gjennom det som kalles samstyringsstruktur for digitalisering.

Samstyringsstrukturen består av medlemsutvalg på ulike nivåer:

- KommIT-rådet (kommune- og fylkesdirektører)
- Digitaliseringsutvalget (digitaliseringssjefer)
- Fag- og prioriteringsutvalg (fageksperter og tjenesteledere) og
- Fagråd for henholdsvis IKT-arkitektur og informasjonssikkerhet og personvern (fageksperter)

Landstingsvedtaket i 2020 forutsatte at KS' oppdrag skulle løses i tett samarbeid med regionale digitaliseringsnettverk. Disse har en viktig oppgave både med å bidra til erfaringsdeling og utbredelse av felles løsninger, men også til å forankre det samlede arbeidet lokalt og regionalt og gi råd inn til det nasjonale arbeidet. I takt med at de regionale digitaliseringsnettverkene har utviklet seg, har omfanget og båndene til den nasjonale samstyringsstrukturen også blitt sterkere.

Det fylkeskommunale kollegiet for HR og IKT/digitalisering og de regionale digitaliseringsnettverkene bidrar til økt kompetanse og kapasitet, og som igjen bidrar en helt nødvendig forankring av det nasjonale arbeidet i hele kommune sektoren.



Figur 23 Samstyringsstrukturen. Kilde: https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/samstyringsstruktur/samstyringsstrukturen-for-digitaliseringsomradet/

Digitaliseringsstrategien, «Én digital offentlig sektor», ble utarbeidet og fremmet av KS og regjeringen i fellesskap. Den danner et viktig bakteppe og utgangspunkt for KS' samordning av digitalisering generelt, og for arbeidet i de regionale digitaliseringsnettverkene, og kommunene spesielt. Stortingsmeldingen «Digital agenda for Norge» omtaler også behovet for sterkere samordning mellom regionalt og statlig digitaliseringsarbeid. Dette er også ytterligere beskrevet i digitaliseringsstrategien.

Generell rådgivning og bistand til arbeidet med informasjonssikkerhet og personvern står sentralt i KS' digitaliseringsarbeid og i samstyringsstrukturen for digitalisering i kommunal sektor. Det er opprettet et eget fagråd for informasjonssikkerhet og personvern (fagrådet) som er etablert for å gi KS og kommunal sektor faglige råd. De øvrige organene i KS' samstyringsstruktur har også tematikk knyttet til informasjonssikkerhet og personvern jevnlig oppe til behandling[9] i fagrådet.

Fagrådet for informasjonssikkerhet og personvern (fagrådet)[10]

Det er etablert et eget fagråd innen informasjonssikkerhet og personvern i kommunal samstyringsstruktur med eksperter fra kommuner og fylkeskommuner.

Fagrådet for informasjonssikkerhet og personvern (fagrådet) er en del av samstyringsstruktur for kommunal sektor sammen med Digitaliseringsutvalget (DU) og KommIT-rådet som øverste organ. Fagrådet skal være kommunal sektors spydspiss innen informasjonssikkerhet, digital beredskap og personvern og ha et tverrsektorielt og tjenstlig perspektiv. Fagrådet deltar også i prosessen med å kvalitetssikre nye fellesprosjekter i og for kommunal sektor.

Fagrådet består i februar 2023 av 11 medlemmer, inkludert leder, som representerer fylkeskommuner og kommuner, samt ulike regioner i kommunal sektor.

Regionale digitaliseringsnettverk

Kommuner har gått sammen i regionale digitaliseringsnettverk. Formålet er å jobbe sammen for å gi bedre digitale tjenestetilbud til innbyggere og næringsliv. KS er av Landstinget gitt en rolle i å koordinere dette arbeidet som del av mandatet på digitaliseringsområdet. Hensikten er å jobbe sammen for å:

- Styrke den samlede kompetansen og dele på nøkkelkompetanse
- Øke gjennomføringskraften i utbredelse av, og gevinstrealisering av nasjonale løsninger og prosjekter
- Gjennom å ta del i nasjonalt arbeid, forsterke og påvirke det nasjonale utviklingsarbeidet, herunder delta i arbeidet med å få frem behovene i sektoren (kommunene).

Regionale digitaliseringsnettverk setter egne mål og prioriteringer. Disse gjenspeiler regionale behov og øvrige strukturer og samarbeid, men har også mange fellestrekk. Mange nettverk har det felles at de ønsker å utvikle et sterkere regionalt mottaksapparat for nasjonale digitale fellesløsninger og styrke den digitale kapasiteten, gjennom å ta del i et regionalt og nasjonalt nettverk. Felles for alle nettverkene er behovet for å jobbe for å realisere nasjonale og sentrale målsettinger: At innbyggerne får gode, helhetlige, brukerrettede tjenester.

Flere av digitaliseringsnettverkene har også etablert egne faggrupper for informasjonssikkerhet og personvern, blant annet DigiViken, DigiRogaland, DigiVestland og Digi Troms og Finnmark. Det er et mål at alle digitaliseringsnettverkene skal ha faggrupper innen informasjonssikkerhet og personvern. Formålet med dette er å speile den sentrale strukturen og utnytte kompetanse og ressurser på tvers av kommunal sektor. Videre, gi regionene en gevinst ved at samtlige kommuner løftes innen informasjonssikkerhet og personvern gjennom samarbeidet i digitaliseringsnettverkene.

KS digitale fellestjenester (DIF)

KS planlegger å stifte et selskap for felles kommunale digitale tjenester. Medlemmene har gjennom regionale kommunedirektørutvalg, KS fylkesstyremøter og fylkeskommunale møter har entydig gitt

[9] KS digitale fellestjenester - konseptutredning

[10] https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/samstyringsstruktur/fagradet-for-informasjonssikkerhet-og-personvern/

støtte til dette. Begrunnelsen er mer effektiv samstyring og ressursutnyttelse av ressursene, samt bedre, raskere og ikke minst sikrere digital tjenesteutvikling.

DIFs tjenester er primært rettet mot kommuner og fylkeskommuner. Noen interkommunale selskaper og statlige virksomheter benytter enkelte tjenester på Fiks-plattformen. I utredningen for KS' digitale fellestjenester (DIF) skrives det blant annet det kan vurderes om DIF kan tilrettelegge for å ivareta felles kommunale sikkerhetsfunksjoner.[11]

Andre aktører

Foreningen kommunal informasjonssikkerhet (KiNS)

KiNS en selveiende, ikke-kommersiell medlemsforening, men også en interesseforening. Foreningen får sine inntekter fra medlemmer, offentlige eller nøytrale tilskudd, eller fra aktører som fremmer foreningens formål.

KiNS har i dag av over 300 kommuner, fylkeskommuner og bedrifter som medlemmer. Styret i KiNS består av 5 styremedlemmer og 2 vararepresentanter, hvor samtlige representanter er kommunalt ansatte..

Formålet med KiNS er å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner[12]. De arrangerer primært kurs, konferanser og lokale/regionale seminarer. KiNS deltar også i en del ulike fora, og har en ressursbank med ulike verktøy innen informasjonssikkerhet og personvern.

Kommersielle aktører

I Norge er det en rekke nasjonale og internasjonale kommersielle aktører som leverer ulike tjenester innen sikkerhet, beredskap, personvern, drift, forvaltning og vedlikehold til kommunal sektor. I dette dokumentet trekkes ikke noen spesifikke leverandører eller tjenestetilbydere, men spekteret av produkter, tjenester og rådgivning innen sikkerhetsområdet spenner bredt.

Noen av aktørene tilbyr flere av tjenestene som omtales i dette dokumentet, deriblant Security Operation Center (SOC), Incident Response Team (IRT), sårbarhetsskanning, driftssikkerhetsoppgaver som patching/oppdatering, brannmursforvaltning, logginnhenting, samt rådgivning innen fagfeltet. Flere av disse tjeneste kan sammenliknes med CERT-tjenester, og kan med rette også kalles CERT-miljøer.

De ulike aktørene bistår den enkelte kommune etter avtale og innkjøp. I Norge er det varierende bruk kommersielle aktører, men utviklingen viser at særlig sikkerhetstjenester blir mer ettertraktet i kommunal sektor. Fra tidligere av har det vært flere, særlig mindre kommuner, som utplasserer drift av infrastrukturen til private aktører. Dette kan skyldes kapasitet, økonomi eller andre forhold som gjør det vanskelig for kommunen å drifte systemer- og infrastruktur selv. I tillegg benytter flere kommuner skytjenester fra store leverandører som også tilbyr sikkerhetstjenester i kombinasjon med skytjenestene.

Dette medfører at kommersielle aktører bidrar til kommunal tjenesteleveranse, da flere kommuner og fylkeskommuner er avhengig av de tjenestene som eksisterer og tilbys i det private markedet. Det private markedet tilbyr også ofte ettertraktet kompetanse, som kan være vanskelig for kommunal sektor å ansette internt i egen virksomhet.

Kommunal sektor er derfor avhengig av en velfungerende privat sektor med riktig og tilgjengelig kompetanse og tjenestespekter innen drift, vedlikehold og sikkerhet. Private aktører og deres

[11] KS digitale fellestjenester - konseptutredning

[12] https://kins.no/om-oss/vedtekter-kins/

tjenesteleveranser er en viktig komponent i kommunal sektors forebyggende, deteksjon og håndteringsevne. Ved utarbeidelse av rammeverk for IKT-hendelser og kommunal sikkerhets- og beredskapsevne, bør derfor også private virksomheter og deres posisjon i sektoren hensyntas.

Et eksempel om komplekst aktørbilde – Veiledning om bruk av skytjenester i offentlig forvaltning etter Schrems II

Som påpekt er aktørbildet innen digital sikkerhet kompleks og fragmentert. Det fører til at modenheten og robustheten for kommunal sektor kan bli skadelidende. For å illustrere dette, kan veiledning om bruk av skytjenester i offentlig forvaltning etter Schrems II benyttes som et eksempel.

Digitaliseringsdirektoratet (DigDir) og Direktoratet for Økonomistyring (DFØ) har utarbeidet «Veiledning for offentlig sektors bruk av skytjenester etter Schrems II»[13]. Veilederen skulle gi klarhet og praktiske råd om lovlig bruk av skytjenester. Anskaffelser av skytjenester etter Schrems II er komplekst, og mer praktisk veiledning har vært etterspurt.

DigDir og DFØ har på oppdrag fra Skate, tatt «stafettpinnen videre fra Datatilsynet for å gi ytterligere veiledning»[14]. En rekke store offentlige aktører fra Skate har vært involvert i arbeidet med å utvikle veilederen. Kort tid etter publiseringen av veilederen, ga Datatilsynet, DigDir og DFØ en felles uttalelse om nevnte veileder. I den felles uttales følgende «både Datatilsynet og DigDir har opplevd å få mange henvendelser om denne veilederen og at den har skapt noe usikkerhet». Det har medført flere debatter og usikkerhet blant flere aktører, inkludert kommunal sektor, om hvordan forvaltningen skal anskaffe skyløsninger, og hvilken veileder de skal benytte seg av når de gjør det.

I november 2022 advarte Tobias Judin, seksjonssjef i Datatilsynet, «at de som følger DigDirs råd må være forberedt på å ta saken mot Datatilsynet i rettsvesenet»[15].

Eksempelet gjelder spesifikt for Schrems II-dommen, men er illustrerende for hvor komplekst og utfordrende det kan være for kommunal sektor å orientere seg i aktørlandskapet som gir veiledning innen digitalisering, informasjonssikkerhet og personvern. Ved slike problemstillinger og utfordringer behøver den enkelte kommune utstrakt veiledning, rådgivning og ressurser for å kunne orientere seg i de krav som til enhver tid stilles til kommunal sektor.

[13] https://markedsplassen.anskaffelser.no/veiledning/veiledning-etter-schrems-ii

[14] https://www.digi.no/artikler/fersk-veileder-skulle-gjore-bruk-av-skytjenester-enklere-har-skapt-usikkerhet-sier-datatilsynet/522258?key=0OpYVW8Q

[15] https://www.digi.no/artikler/fortsatt-full-forvirring-etter-motstridende-statlige-rad-om-skytjenester/523742?key=4TOD26tl