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

Sammendrag 2
Bakgrunn for rapporten 3
Robusthet – en forutsetning for digitalisering 5
Målbildet for trygg digitalisering av kommunal sektor 6
Føringer for trygg digitalisering i kommunal sektor 6
Utfordringsbildet for kommunal sektor 7
Behov for økt digital robusthet i kommunal sektor 8
Dimensjoner i behovsbeskrivelsen 9
Operasjonalisering og gjennomføring av oppgaver 16
Behov kan møtes regionalt 18
Fremtidig organisering av drift og forvaltning av IKT i kommunal sektor 18
Samarbeid om tjenester og kompetanse innen sikkerhet 19
Oppsummering og anbefaling av tiltak 20
Behov kan møtes nasjonalt 21
Helhetlig veiledning for og til kommunal sektor 21
Styringsevne og samstyring 22
Økt tjenestespekter innen forebygging, oppdagelse og håndtering av digitale angrep 24
Behov for felles kommunale sikkerhetskrav, både internt og eksternt 27
Behov for felles tilnærming til personvern 27
Påvirkning i det digitale rom 28
Behov for sentrale vurderinger av systemer og behandlinger 28
Utvikle nasjonal virtuell operativ kommunal sikkerhetsorganisasjon 28
Oppsummering og anbefaling om tiltak 29
Vedlegg A – Detaljert oversikt over foreslåtte tiltak 30
Vedlegg B – Utfordringsbildet i kommunal sektor 30
Vedlegg C – Dagens aktørbilde for kommunal sektor innen digital sikkerhet 30
Vedlegg D – Definisjoner og forkortelser 30
Vedlegg E – Metode og datagrunnlag 30
Vedlegg F – Fagnotat SOC 30
Vedlegg G – Evaluering av sektorvise responsmiljøer 30
Vedlegg H – Digitaliseringsbrev til kommuner og fylkeskommuner 30
Vedlegg I – Vedlegg I - RSB - versjon 1.0 - Referansearkitektur sikkerhet beredskap og personvern (Akson-prosjektet) 30

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.

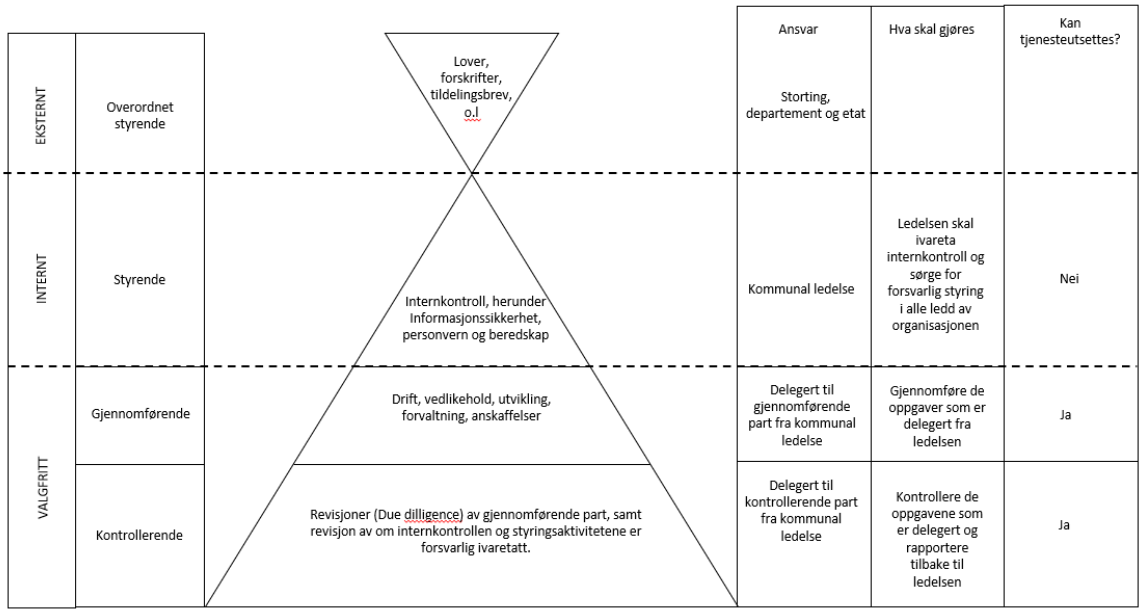
[10] https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102
[11] https://www.digdir.no/informasjonssikkerhet/felles-sikkerhet-i-forvaltningen/4115
[12] Se vedlegg E

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).

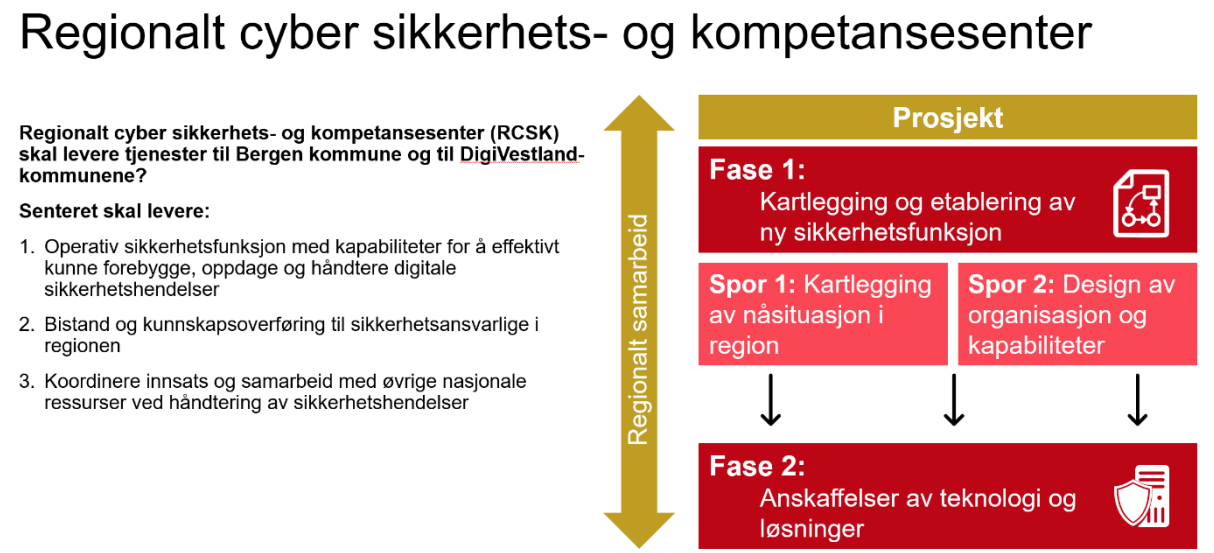
Tjenestene som kan inngå i en RCSK kan variere avhengig av medlemmenes behov og ønsker. RCSK kan bidra til at regionene i større grad kan nyttiggjøre og dele på kompetansen som eksisterer i regionen, og dermed redusere den enkelte kommunes kostander sammenlignet med å hente inn kompetansen selv. RCSK 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.

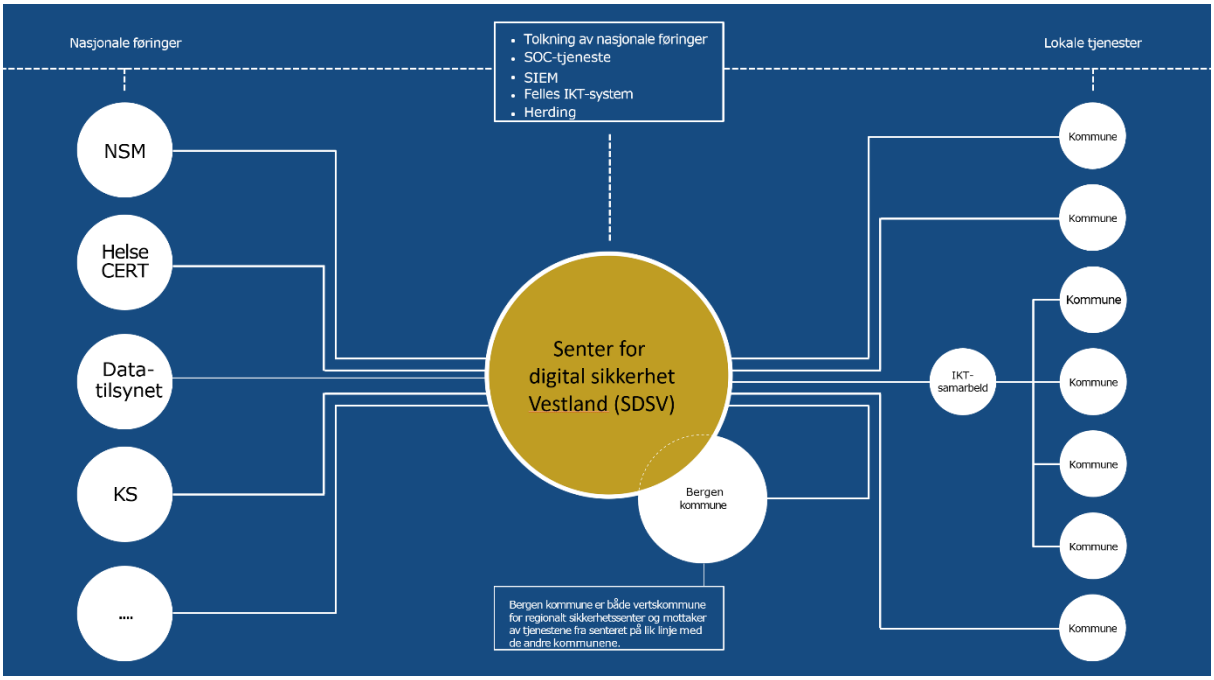
Basert på antall kommuner og fylkeskommuner, kan det være hensiktsmessig at det opprettes flere RCSK som kan samarbeide om å dekke hele sektoren. Kjernekompetansen som er nødvendig for å etablere og drifte tjenestene er svært ettertraktet, så det er ikke sannsynlig at det kan etableres mange slike enheter 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)

Vedlegg A – Detaljert oversikt over foreslåtte tiltak

Innhold

Innledning 1
Aktiviteter som bør gjennomføres i den enkelte kommune i henhold til ansvar 3
Utdyping av tiltak anbefalt i rapporten 6
Finansieringsmodeller 17
Selvfinansiering 17
Kostfordeling 17
Grunnfinansiering 17

Innledning

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

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

Vedlegget er inndelt i 2 hoveddeler:

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

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

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

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

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

[1] Vedlegg E

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

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

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

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

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

Utdyping av tiltak anbefalt i rapporten

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

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

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

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

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

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

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

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

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

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

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

Finansieringsmodeller

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

Selvfinansiering

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

Kostfordeling

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

Grunnfinansiering

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

Vedlegg B – Utfordringsbildet i kommunal sektor

Innhold

Varierende grad av styringsevne innen informasjonssikkerhetsområdet 1
Har varierende grad av nødvendig sikring av teknisk infrastruktur 2
Har varierende grad av nødvendig evne til å forebygge og oppdage hendelser 2
Har varierende grad av nødvendig evne til å håndtere hendelser 3
Årsaksforhold 3

Varierende grad av styringsevne innen informasjonssikkerhetsområdet

Evne til styring og prioritering innenfor digitalisering krever kompetanse og kapasitet også innen informasjonssikkerhet og personvern. Det er gjennomgående enighet blant kommunene om at det er ressurs- og kompetansemangel innen disse fagområdene[1].

De underliggende årsakene til den opplevde ressurs- og kompetansemangelen er sammensatte. Særlig for små kommuner vil det være utfordrende å prioritere dedikerte ressurser på informasjonssikkerhet og personvern, og i tillegg er arbeidsmarkedet på disse fagområdene presset. Det har også vist seg å være utfordrende å rekruttere spesialistkompetanse til distriktene, selv om unntak finnes. Små som store kommuner skal levere de samme lovpålagte tjenestene, der kommunene vil stå overfor de samme problemstillingene innen informasjonssikkerhet og personvern uavhengig av størrelse. De små og mellomstore kommunene har imidlertid mindre ressurser og kapasitet til å ivareta sitt ansvar og utføre oppgavene.

En annen stor utfordring for den enkelte kommune, er omfanget av kompetansen nødvendig for å digitalisere og hente ut gevinster fra dette arbeidet. Digitaliseringsprosjekter- og arbeid krever tverrfaglige team, sammensatt av ulike fag-, forvaltning-, og kompetanseområder. Som tidligere beskrevet har små og store kommuner de samme behovene, men ulik tilgang og mulighet til å allokere tilstrekkelig ressurser og kapasitet i digitaliseringsarbeidet.

I dag er det en lang rekke IKT-samarbeidsformer i sektoren, men det eksisterer fortsatt et potensiale for deling av ressurser, kompetanse og kapasitet mellom ulike aktører i kommunal sektor. Ulikt modenhetsnivå medfører også at det er ulik erfaringsdeling og nyttiggjørelse av kompetanse og kapasitet i digitaliseringsnettverkene.

Veiledere og retningslinjer som tilgjengeliggjøres av aktører med veiledningsansvar er i liten grad samkjørte, og det kan argumenteres for at disse ikke i tilstrekkelig grad tar høyde for hurtig teknologisk utvikling- og endring.

De fleste kommuner har tilpasset seg veiledere ved å etablere et styringssystem for informasjonssikkerhet, men det er ofte ikke innlemmet med kommunens øvrige virksomhet- og styring[2]. På lik linje som at styringssystemet for informasjonssikkerhet er etablert som en isolert prosess, som regel utenfor eksisterende kommunale styringsaktiviteter, er også beslutninger som

[1] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet».
[2] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet».

gjelder informasjonssikkerhet og personvern ofte ikke tilstrekkelig forankret og etablert i beslutningsprosesser og strukturer i kommunene og fylkeskommunene. Dette påvirker beslutninger, prosjekter, og til slutt digital robusthet i tjenestene på en negativ måte.

God styring fordrer at hele spektret av digital transformasjon innlemmes i kommunenes etablerte virksomsomhetsstyring og internkontroll. Alternativet blir svak styring av hele digitaliseringskjeden hvis kommunene ikke har en helhetlig tilnærming.

Har varierende grad av nødvendig sikring av teknisk infrastruktur

Kommunene og fylkeskommunene har, på samme måte som alle andre virksomheter i Norge, etablert digitale løsninger over tid. For de aller fleste kommunene er investeringer i digitale tjenester langsiktig. Utfordringene er at maskinvaren og digitale tjenestene har en kort levetid, typisk mellom 5 og 10 år.

Det finnes systemer i bruk i kommuner i dag som har vært i bruk over 20 år. Det finnes også eksempler på svært gamle maskinvareløsninger. Hovedutfordringen med gamle og utdaterte løsninger er vedlikehold. Slike systemer støttes ikke i lengden av leverandørene («end of life»-produkter), og eventuelle sårbarheter som blir avdekket vil ikke bli lukket. Over tid vil infrastrukturen til en vanlig kommune inneholde flere slike gamle løsninger, og sårbarhetsflaten øker.

Samtidig innføres det nye løsninger gjennom digitaliseringsløft, som ofte bygger oppå de gamle løsningene, og det innføres nye leverandører som også krever oppfølging dersom man skal ha kontroll med hele verdikjeden.

Selv for en liten kommune vil infrastrukturen inneholde hundrevis av systemer og løsninger for integrasjoner. Dette gjør at det er svært ressurskrevende å forsøke å vedlikeholde alle løsningene og å følge opp leverandørene, noe som igjen gjør det utfordrende å ivareta sikkerheten[3]. Det er en kjensgjerning at kommunal sektor har teknisk gjeld. Det gir bekymring for ytterligere manglende sikring av teknisk infrastruktur.

Drift av teknisk infrastruktur innebærer også oppdatering av sikringsmekanismene for infrastrukturen. Dette er en krevende oppgave både i form av kompetanse og kapasitet når det skal skje i en omfattende infrastruktur i stadig endring.

For å ha mulighet til å oppnå tilfredsstillende sikring av teknisk infrastruktur, må det gjøres løpende vurdering av risiko, vurdering av tiltak som ofte krever investeringer, prioritering og implementering er aktiviteter. Alle disse aktivitetene krever ulik kompetanse og en betydelig ressursinnsats selv for små kommuner.

Har varierende grad av nødvendig evne til å forebygge og oppdage hendelser

Informasjonsinnhentingen gir indikasjon på at kommunenes evne til å oppdage mulige og faktiske hendelser er begrenset[4]. Alle kommuner har enten gjennom etablering av egen organisasjon, samarbeid med andre kommuner eller innkjøp, sikret seg at de rent driftsoperative oppgavene blir løst. I tillegg er det mange kommuner som er i stand til å oppdage og håndtere avvik fra god praksis.

[3] Vedlegg E, «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

[4] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet» og «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

Det er likevel bare et fåtall kommuner som har etablert organisasjon og verktøy for å overvåke sikkerheten i egen infrastruktur, for eksempel gjennom et overvåkingssenter (Security Operations Center, SOC)[5], og dermed har etablert en evne til å oppdage og håndtere sikkerhetshendelser.

Mangelen på overvåking av hendelser i egen teknisk infrastruktur gjør det svært krevende å avdekke hendelser på et tidlig stadium, og gjør at trusselaktører får operere i kommunen tekniske infrastruktur uten å bli oppdaget. Eksempler fra tidligere hendelser har vist at enkelte trusselaktører har hatt tilgang til systemene i måneder før de slår til med utpressing eller andre handlinger.

Evne til å avdekke og håndtere en sofistikert angriper i sanntid krever svært mye av en virksomhet. Det er i dag en utfordring i kommunal sektor at det ikke i tilstrekkelig grad er etablert organisasjon og verktøy for å oppdage hendelser. Manglende tilgang på kompetanse svekker styringsevnen og gjør også at problemstillingen med manglende evne til å oppdage hendelser aldri kommer til beslutning i kommuneledelsen.

Har varierende grad av nødvendig evne til å håndtere hendelser

Det er få kommuner som har innarbeidet digitale hendelser i beredskapsplanverket, og det er enda færre som har trent eller øvet på slike hendelser[6].

Det er også svært få kommuner som har etablert eller anskaffet en hendelseshåndteringsenhet (Incident Response Team (IRT)). I bakkant av en hendelse vil det også kunne være aktuelt med å gjenopprette til normal drift, en oppgave som også kan være krevende. Østre Toten kommune og andre virksomheter som har blitt rammet av digital utpressing har brukt lang tid på å komme i normal drift. Å planlegge for, og ha tilgjengelig kompetanse over tid, blir derfor også helt sentralt i evnen til å håndtere hendelser og tiden etter.

Årsaksforhold

Det er som nevnt store forskjeller på kommunene når det gjelder hvilke og i hvilken grad de har utfordringer på disse områdene, men generelt for kommunene er det utfordringer på ett eller flere av de ovennevnte områdene. Årsaken til den varierende modenheten kan i stor grad forklares ut fra:

- Ressurstilgang (personell og økonomi).
- Kompetanse og informasjonstilgang.
- Evne til drift, vedlikehold, utvikling og innføring av teknologi og digitalisering.
- Forvaltningsmodeller.
- Strategisk styringskompetanse (politisk og administrativt nivå).

[5] Vedlegg E, «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

[6] Vedlegg E, «Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet» og «Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne».

Vedlegg C, Dagens aktørbilde for kommunal sektor innen digital sikkerhet

Innhold

Aktørbilde for kommunal sektor innen digital sikkerhet 2
Veiledende aktører 2
Rådgivende og forebyggende aktører 2
Operasjonelle aktører 3
Om CERT 3
Sektorvis responsmiljø som treffer kommunal sektor 5
HelseCERT 5
Nasjonalt cybersikkerhetssenter (NCSC) 5
KraftCERT/InfraCERT 5
Kommune CSIRT 5
Særlig om CERT 6
Offentlige aktører innen digital sikkerhet som treffer kommunal sektor 8
Digitaliseringsdirektoratet 8
Direktoratet for forvaltning og økonomistyring (DFØ) 8
Direktoratet for samfunnssikkerhet og beredskap (DSB) 8
Nasjonal sikkerhetsmyndighet (NSM) 9
Direktoratet for e-helse 9
Datatilsynet 9
Statsforvalteren 9
KS og kommunene 10
Fagrådet for informasjonssikkerhet og personvern (fagrådet) 11
Regionale digitaliseringsnettverk 11
KS digitale fellestjenester (DIF) 11
Andre aktører 12
Foreningen kommunal informasjonssikkerhet (KiNS) 12
Kommersielle aktører 12
Et eksempel om komplekst aktørbilde – Veiledning om bruk av skytjenester i offentlig forvaltning etter Schrems II 13

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.

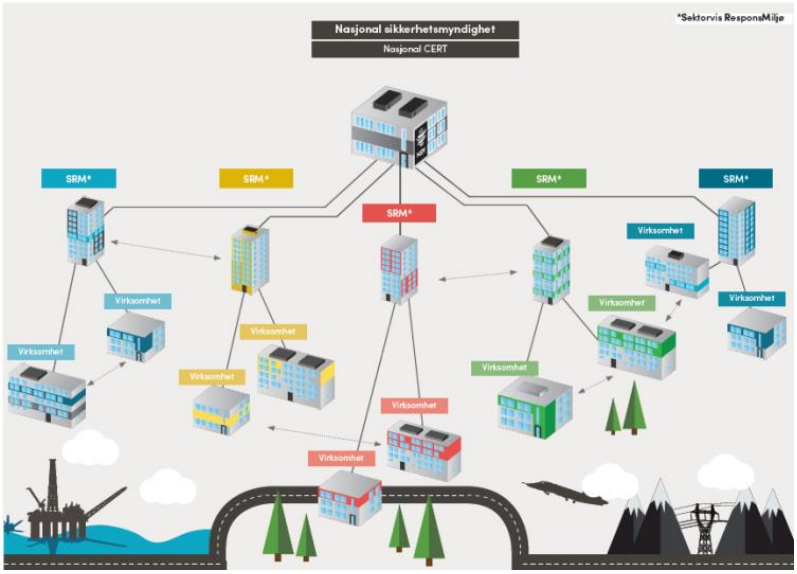
Reaktive tjenester	**Proaktive tjenester**	**Rådgivingstjenester**
Varsling Sårbarhet og hendelseshåndtering - Analyse - Bistand - Koordinering	Formidle sikkerhetsinformasjon og trusselbildet Overvåking av ekstern infrastruktur (typisk ekstern Internettrafikk) Utvikling av sikkerhetsverktøy Sikkerhetstesting	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.

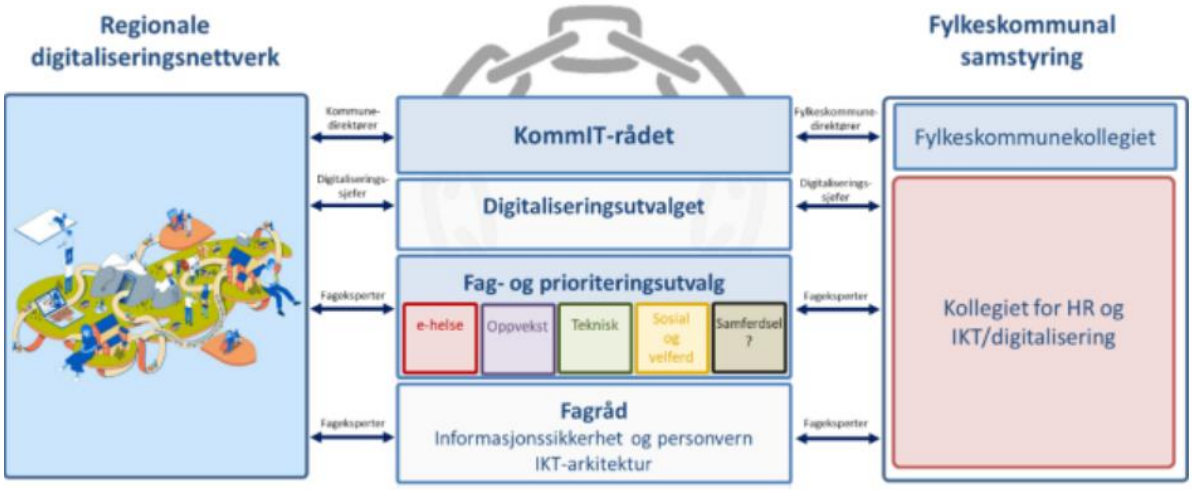
De siste årene har KS fått en sterkere rolle i å samordne sektoren, og understøtte kommunenes og fylkeskommunenes digitaliseringsarbeid. KS har i samarbeid med medlemmene etablert en rekke råd og utvalg som skal bidra til koordinering og samordning på digitaliseringsområdet i sektoren. Den strategiske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

Vedlegg D – Definisjoner og forkortelser

Beredskap: Planleggingen i forkant av en hendelse og selve håndteringen når en hendelse inntreffer eller er nært forestående. Beredskap omfatter også håndteringen av det etterfølgende gjenopprettingsarbeidet (NOU 2016:19)

DigDir: Digitaliseringsdirektoratet.

DFØ: Direktoratet for forvaltning og økonomistyring.

CERT: Computer emergency response team.

CSIRT: Computer security incident response.

Forebyggende sikkerhet: Omfatter tiltak som reduserer sannsynligheten for at en uønsket hendelse inntreffer og tiltak som reduserer skadevirkningene ved en slik hendelse (NOU 2016:19).

IRT: Incident response team.

JD: Justis- og beredskapsdepartementet.

KDD: Kommunal- og distriktsdepartementet.

Kommunal sektor: I denne rapporten menes både fylkeskommuner og kommuner.

Kommune: I denne rapporten menes både fylkeskommune og kommune.

NKRF: Norges kommunerevisorforbund - Kontroll og revisjon av kommunene.

NOU: Norges offentlige utredninger.

NSM: Nasjonal sikkerhetsmyndighet.

Robusthet: Robusthet er et uttrykk for den motstandskraft et system har mot en uønsket hendelse, samt den evne systemet har til å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

SOC: Security operations center.

SRM: Sektorvis responsmiljø.

Teknisk gjeld: En samlebetegnelse på uferdig, kompliserte eller utdaterte løsninger. Et gap mellom ønsket løsning og nåværende løsning.

Vedlegg E – Metode og datagrunnlag

Innhold

Datagrunnlag og metode 2
Gjennomgang av dokumenter og statistikk 2
Norges offentlige utredninger 2
Stortingsmeldinger 2
Rapporter 2
Veiledere, normer, rammeverk 2
Strategier 3
Andre relevante kilder 3
Statistikk 3
Samtaler og samarbeid med kommunal sektor 3
Dialog i sektoren før 2022 4
Møtevirksomhet våren/sommeren 2022 4
Nasjonalt program for informasjonssikkerhet (NPISK) 4
Innspillsrunder 4
Analyse og konklusjon fra dokumentasjonsgjennomgang og sektordialog 5
Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet 5
Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne 7
Oppsummering 9

Datagrunnlag og metode

Rapporten finner sitt kunnskapsgrunnlag i offisielle og publiserte dokumenter, samtaler, workshops og innspillsrunder med kommunal sektor og erfaringsgrunnlag fra innspillet til nasjonalt program for informasjonssikkerhet i kommunal sektor (NPISK). I det følgende redegjøres det for hvilke dokumenter som har vært gjenstand for dokumentanalyse, og hvilke samarbeid og initiativ som har skapt kunnskapsgrunnlaget for rapporten.

Gjennomgang av dokumenter og statistikk

I forbindelse med rapporten har sentrale dokumenter som regulerer rammer og ansvar for arbeid med digital sikkerhet, beredskap og personvern blitt gjennomgått. Dette omfatter veiledningsmateriell, konseptutredninger, rammeverk, strategier, etterretnings- og sikkerhetstjenestens risikovurderinger, årsrapporter, gjennomførte kartlegginger i kommunal sektor og lovverk. Gjennomgåtte dokumenter er fra perioden 2015-2023.

Norges offentlige utredninger

- NOU 2015:13 Digital sårbarhet – sikkert samfunn.
- NOU 2018:14 IKT-sikkerhet i alle ledd.
- NOU 2022:11 Ditt personvern – vårt felles ansvar — Tid for en personvernpolitikk.
- NOU 2023:4 Tid for handling Personellet i en bærekraftig helse- og omsorgstjeneste.
- NOU 2016:19 - Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.

Stortingsmeldinger

- Meld. St. 10 (2016-2017) Risiko i et trygt samfunn. Samfunnssikkerhet.
- Meld. St. 38 (2016-2017) IKT-sikkerhet. Et felles ansvar.
- Meld St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden.
- Meld. St. 9 (2022 –2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.

Rapporter

- Risiko 2022 (NSM, 2022).
- Risiko 2021 (NSM, 2021).
- Nasjonal trusselvurdering 2022 (PST, 2022).
- Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor (Riksrevisjonen, 2023).
- Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner (Digitaliseringsdirektoratet 2020).
- Personvern- og informasjonssikkerhet (DigiVestland, 2021-2022).
- Kartlegging av digital modenhet i kommunal sektor (KS, 2018).
- Fremtidig organisering av KS digitale fellestjenester (KS, 2022).
- Kommune CERT – utredning av behov og muligheter (NorSIS, 2015).

Veiledere, normer, rammeverk

- Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen).
- Hvordan jobbe med informasjonssikkerhet (Digitaliseringsdirektoratet).
- Grunnprinsipper for IKT-sikkerhet (NSM).

- Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet – orden i eget hus (KS).
- Rammeverk for håndtering av IKT-sikkerhetshendelser.

Strategier

- Internasjonal cyberstrategi for Norge (2017).
- Nasjonal strategi for digital sikkerhet (2019).
- Nasjonal strategi for digital sikkerhetskompetanse (2019).
- Digitaliseringsstrategien for offentlig sektor (2019-2025) – Én digital offentlig sektor

Andre relevante kilder

- Proposisjon 78 S (2021–2022).
- Felles sikkerhet i forvaltningen. Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning (Digitaliseringsdirektoratet, 2022).
- Offentlige og private tilbydere av SOC og CERT tjenester (DFØ, Markedsplassen).

Statistikk

Tabeller fra SSBs statistikk «Bruk av IKT i offentlig sektor»:

- Tabell 12041: «Tiltak/rutiner ved administrasjon av IKT-sikkerheten, etter antall innbyggere (Fylkeskommuner, kommuner)».
- Tabell 12038: «Rekruttering av IKT-spesialister (prosent), etter forvaltningsnivå, statistikkvariabel og år».
- Tabell 2019: «IKT-strategier (prosent), etter status for strategi, forvaltningsnivå, statistikkvariabel og år».
- Tabell 12036: «Hindringer for utvikling av elektroniske tjenester (prosent), etter statistikkvariabel, grad av hindring, forvaltningsnivå og år».
- Tabell 12617: «IKT-sikkerhetsproblemer (prosent), etter statistikkvariabel, status for sikkerhetsproblemet, forvaltningsnivå og år».
- Tabell 12618: «Tiltak for IKT-sikkerheten (prosent), etter statistikkvariabel, status for tiltak, forvaltningsnivå og år».

Samtaler og samarbeid med kommunal sektor

Kommunal sektor har over lang tid samarbeidet om ulike tiltak for å bedre digital robusthet. I KS har for eksempel Fagrådet for informasjonssikkerhet og personvern arbeidet med problemstillinger på området i en årrekke innenfor samstyringsstrukturen, i tillegg til at SNIP-nettverket og de regionale digitaliseringsnettverkene har gitt sine bidrag.

Prosjekter og aktiviteter i kommunal sektor har også hatt en tydelig involvering av informasjonssikkerhet og personvern, herunder utvikling av kompetansepakker, SkoleSec, og større prosjekter som Akson. Gjennom disse har kommunal sektor både kartlagt status innen digital robust, og samtidig fremme behov for tiltak, selv om dette arbeidet ikke har vært samlet under en felles paraply.

Det ble i løpet av året 2022 igangsatt flere initiativ og samarbeid, inkludert NPISK, arbeids- og avklaringsmøter, og samtaler med kommuner og fylkeskommuner i forbindelse med utvikling av grunnlaget for og arbeidet med rapporten. Innspillene fra sektoren har vært avgjørende for å beskrive utfordringsbildet i sektoren i dag, samt identifikasjon av målrettede og treffsikre tiltak.

Dialog i sektoren før 2022

I forbindelse med Akson-prosjektet ble det gjennomført mer enn 25 møter i perioden januar - juni 2020 for å utarbeide referansearkitektur for sikkerhet, beredskap og personvern for kommunal sektor (RSB) i forbindelse med Aksonprosjektet.

Ved utarbeidelsen av RSB ble det vektlagt hvordan utfordringene innen digital sikkerhet som kommunal sektor står ovenfor på kort og lang sikt kan møtes effektivt.

Det henvises til vedlegg I - *RSB - versjon 1.0 - Referansearkitektur sikkerhet beredskap og personvern* over hvilke kommuner som deltok i arbeidet og selve arbeidet.

Møtevirksomhet våren/sommeren 2022

Det har vært gjennomført mer enn 30 møter og workshops med kommuner, myndigheter og interessenter i løpet av våren/sommeren 2022. Møtene og workshopene har satt søkelys på status og behov for kommunene. Sentrale aktører har vært kommuner i SNIP-nettverket (tilnærmet alle kommuner) i workshops, samt NSM, HelseCERT, Kommune-CSIRT, Kraft/InfraCERT, JustisCERT og DFØ. Disse aktørene har også deltatt på flere oppfølgingsmøter.

I workshops med kommunene er det noen hovedmomenter om behov som spesielt går igjen:

- Innføre trusselovervåking og monitorering (SOC), og responsmiljø (IRT).
- Gjennomføre penetrasjonstester.
- Redusere ressursbruk på ROS og DPIA, forenkling av verktøy.
- Redusere ressursbruk på leverandøroppfølging og mulig –sertifisering.
- Redusere ressursbruk på teknisk forvaltning av infrastruktur (standardoppsett etc.).
- Støtte til tolkning og implementering av rammeverk (ISO, NSM grunnprinsipper etc.).
- Gjennomføre opplæring og kompetansebygging.
- Tydeliggjøring av ansvar og roller blant aktørene.
- Samarbeid for innkjøp og felles bestillingskompetanse.

Status i forbindelse med innspillet til nasjonalt program for informasjonssikkerhet i kommunal sektor har også vært gitt til KommIT, Digitaliseringsutvalget, Fagrådet og diginettverkene.

Nasjonalt program for informasjonssikkerhet (NPISK)

KS har sammen med fageksperter fra medlemmene, og i dialog med Kommunal- og distriktsdepartementet (KDD), utarbeidet et forslag til program for IKT-sikkerhet i kommunal sektor (NPISK). KS søker samarbeid med ulike aktører for å gjennomføre en rekke aktiviteter i tråd med Stortingets vedtak.

I utarbeidelsen av foreslåtte tiltak i NPISK ble det satt sammen en faggruppe med hensikt om å foreslå og utarbeide tiltak. Arbeidet pågikk fra mai 2022 – september 2022. Kunnskapsgrunnlaget fra NPISK har vært viktig for innsikt i utfordringene de enkelte kommunene står i, og hvilke strakstiltak som er nødvendig å innføre.

Innspillsrunder

I løpet av høsten 2022 ble første utkast av rapporten ferdigstilt. Rapporten ble delt og videresendt til store deler av sektoren, og inndelt i følgende arbeidsgrupper:

- Faggruppe innen digitalisering, informasjonssikkerhet og personvern. Faggruppen besto av medlemmer fra flere kommuner og fylkeskommuner.

- Diginettverkslederene. Alle Diginettverkslederene deltok.
- Strategisk faggruppe. Representanter med strategisk styringskompetanse innen digitalisering deltok.

Det ble gjennomført to arbeidsmøter på 3 timer med faggruppen. Basert på innspillene fra faggruppen, ble rapporten justert for å hensynta innspill og tilbakemeldinger. Det ble særlig satt søkelys på utarbeidelsen av målrettede tiltak i sektoren.

Det ble gjennomført ett møte med diginettverkslederene, med særlig søkelys på implementering og operasjonalisering av tiltakene i sektoren. Diginettverkslederene ga tilbakemeldinger skriftlig i etterkant av møtet.

Strategisk faggruppe deltok i 3 møter for å gi innspill på innretningen og tiltakene i rapporten.

Analyse og konklusjon fra dokumentasjonsgjennomgang og sektordialog

Dokumentasjonsgjennomgangen sammenholdt med sektordialogen har gitt et godt grunnlag for å forstå kommunenes situasjon innen informasjonssikkerhet og personvern. Selv om funnene og beskrivelsene spriker når man ser kommunene under ett, viser behovsbeskrivelsene etter workshops med kommunene at *behovene* i stor grad er de samme.

Styringsevne (herunder kontrollfunksjon) innen informasjonssikkerhetsområdet

KS sin kartlegging av digital modenhet i kommunesektoren fra 2018[1] viser at 86% av fylkeskommunene og kommunene har organisert arbeidet med informasjonssikkerhet gjennom en form for rolle/sikkerhetsfunksjon med ansvar for informasjonssikkerhet. Disse rollene varierer mellom å være en «dedikert sikkerhetsfunksjon som rapporterer til rådmann» (54 %), informasjonssikkerhetsfunksjon som rapporterer til IKT-ansvarlige» (13 %), «sikkerhetsfunksjon i hver enkelt virksomhet» (10 %) og en «tilfeldig utvalgt ressurs» (9 %).

Ved å sammenstille de ovennevnte data med SSB tabell 12041[2] gir denne en indikasjon på både sikkerhetsarbeidet og organisering i kommunal sektor:

12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år

		Har en skriftlig informasjonssikkerhetspolicy som er forankret i ledelsen		En formelt utnevnt person er fagansvarlig for informasjonssikkerheten		Risikovurderinger gjennomføres systematisk og periodisk		Ved nye risikovurderinger iverksettes nødvendig risikohåndtering	
		2018	2022	2018	2022	2018	2022	2018	2022
Fylkeskom	50 000 innbyggere eller flere	87,5	70,0	87,5	90,0	68,8	80,0	87,5	100,0
Kommune	0 - 1 999 innbyggere	57,8	58,4	54,2	59,7	36,1	44,2	60,2	71,4
	2 000 - 4 999 innbyggere	56,5	57,9	60,2	73,7	30,6	66,3	57,4	84,2
	5 000 - 9 999 innbyggere	55,7	74,6	57,0	81,7	45,6	63,4	69,6	87,3
	10 000 - 19 999 innbyggere	78,4	72,3	76,5	80,9	51,0	66,0	78,4	91,5
	20 000 - 29 999 innbyggere	84,0	82,8	72,0	82,8	44,0	75,9	88,0	86,2
	30 000 - 49 999 innbyggere	87,5	73,3	81,3	86,7	56,3	73,3	68,8	86,7
	50 000 innbyggere eller flere	86,7	80,0	93,3	85,0	86,7	95,0	100,0	95,0

Dataene er kun en indikasjon på sikkerhetsarbeid og organisering i kommunal sektor da de ikke inneholder informasjon om grundigheten av risikovurderingene, kompetanse- eller ressurskapasitetsnivå til fagpersonene, eller kvaliteten på informasjonssikkerhetspolicy.

[1] https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf

[2] https://www.ssb.no/statbank/table/12041/tableViewLayout1/

Denne indikasjonen støttes også opp av SSB tabell 12038[3], se nedenfor, om rekruttering.

I følge «Arbeid med informasjonssikkerhet i fylkeskommuner og kommuner» (Digitaliseringsdirektoratet, 2020), basert på DSBs tall fra 2018 er bildet mer underbygget med data: «Observasjonene viser at 44 % av kommunene har informasjonssikkerhet som et fast punkt i styringsdialogen i egen organisasjon. At under halvparten av kommunene har dette kan tyde på at informasjonssikkerhet ikke har tilstrekkelig plass i styringsdialogen hos kommunene.»

Rapporten fra Digdir peker videre på at:

«Observasjonene viser at over 75 % av fylkeskommunene i tidsperioden 2018-2019 svarte at de har evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Under 65 % av kommunene svarer tilsvarende i tidsperioden 2018-2020. […] Observasjonene viser videre at under 75 % av fylkeskommune i tidsperioden 2018- 2019 svarte at de rapporterte erfaringer fra håndtering av uønskede hendelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten. Under 55 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. […] Observasjonene viser videre at under 40 % av fylkeskommunene svarte at de rapporterte erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten i tidsperioden 2018 - 2019. Under 30 % av kommunene har gjort tilsvarende i tidsperioden 2018-2020. Dette kan indikere at fylkeskommuner og kommuner i liten grad rapporterer erfaringer fra øvelser til bruk i risikovurderinger».

Disse observasjonene sammen underbygger hypotesen om at styringsevnen til kommunene, som må ha en tilbakemeldingssløyfe fra oppdateringer, risikovurderinger og øvelser for å være til tilstrekkelig, ikke er tilstrekkelig innen informasjonssikkerhet og personvern.

I følge Digdirs rapport viser vurderinger Datatilsynet har gjort «at noen større kommuner ikke har tilstrekkelige tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet om personopplysninger. I enkelttilfeller har kommunen heller ikke hatt nok kompetanse rundt gjennomføringen av risikovurderinger. Dette indikerer at også blant store kommuner kan det i enkelttilfeller være utfordringer med risikostyring. Veiledning knyttet til kompetanseheving på risikovurdering og risikohåndtering bør spesielt rettes mot små og mellomstore kommuner.»

I forbindelse med workshops med kommunene fremkom også behovet for kompetanse i forbindelse med gjennomføring av risikovurderinger tydelig.

12038: Rekruttering av IKT-spesialister (prosent), etter forvaltningsnivå, statistikkvariabel og år

Informasjon om tabellen
Endre visning
Rediger og beregne
Lagre data som
Lagre spørring

Rotér mot venstre | Rotér mot høyre | Rotér manuelt | Excel (xlsx) | Fullskjerm

	Har forsøkt å rekruttere IKT-spesialister i løpet av det siste året			Hadde problemer med å rekruttere IKT-spesialister i løpet av det siste året		
	2018	2020	2022	2018	2020	2022
Fylkeskommuner	75,0	:	80,0	33,3	:	62,5
Kommuner	29,2	35,4	51,4	31,8	50,4	56,0

[3] https://www.ssb.no/statbank/table/12038/tableViewLayout1/

Tabell 12038 kan ses i sammenheng med tabell 12019[4], se nedenfor, som angår digitaliseringsstrategi. Denne tabell er lagt til grunn som en indikasjon da den ikke gir ytterligere verdier om kvalitet og grundighetsnivå på strategien. Det er også interessant å legge merke til at i 2022 hadde 84,8% av kommunene strategi for skytjenester mens 74,3% hadde digitaliseringsstrategi.

12019: IKT-strategier (prosent), etter status for strategi, forvaltningsnivå, statistikkvariabel og år

Informasjon om tabellen | Endre visning | Rediger og beregne | Lagre data som | Lagre spørring

Rotér mot venstre | Rotér mot høyre | Rotér manuelt | Excel (xlsx) | Fullskjerm

	Har IKT-/digitaliseringsstrategi			IKT-infrastruktur			Informasjonssikkerhet			Skytjenester		
	2018	2020	2022	2018	2020	2022	2018	2020	2022	2018	2020	2022
Har strategien												
Fylkeskommuner	93,8	87,5	60,0	86,7	100,0	66,7	93,3	100,0	83,3	80,0	85,7	83,3
Kommuner	67,9	73,8	74,3	89,5	85,8	80,6	93,8	94,2	94,7	76,6	84,2	84,8

Tabell 12036[5] gir også et annet perspektiv på digitalisering i kommunal sektor, nemlig hindringer for utvikling av elektroniske tjenester.

12036: Hindringer for utvikling av elektroniske tjenester (prosent), etter statistikkvariabel, grad av hindring, forvaltningsnivå og år

		Er i stor eller ganske stor grad en hindring	
		2020	2022
Mangel på politiske føringer	Fylkeskommuner	..	..
	Kommuner	14,5	8,2
Mangel på engasjement hos ledelsen	Fylkeskommuner	..	10,0
	Kommuner	12,6	12,1
Lovgivning og regler mangler tilpasning	Fylkeskommuner	12,5	50,0
	Kommuner	19,1	19,2
Mangel på felles standarder for datautveksling	Fylkeskommuner	37,5	40,0
	Kommuner	44,9	34,2
Mangel på felles offentlige løsninger og infrastruktur	Fylkeskommuner	25,0	40,0
	Kommuner	50,2	44,9
Vanskelig å integrere eksisterende IT- og fagsystemer med digital forvaltning	Fylkeskommuner	62,5	40,0
	Kommuner	46,8	47,7
Vanskelig å frigjøre ressurser til utvikling	Fylkeskommuner	87,5	70,0
	Kommuner	74,8	72,9
IKT-utgifter høyere enn forventet	Fylkeskommuner	25,0	40,0
	Kommuner	43,4	54,0
Manglende kompetanse i virksomheten	Fylkeskommuner	62,5	30,0
	Kommuner	45,8	49,7
Avhengig av utvikling hos andre virksomheter	Fylkeskommuner	37,5	40,0
	Kommuner	58,5	47,7

Ved å se disse tre tabellene under ett og koble dette med tilbakemeldingene fra kommunene gjennom kunnskapsinnhenting og dialog i forbindelse med denne rapporten, er det mulig å konkludere med at kommunal sektor har behov for å styrke kompetansenivået på dette området. Dette inkluderer behov for bistand til hvordan man kan innføre og utfase teknologi på en god måte som både understøtter og utvikler kommunal virksomhet.

Løpende sikring av all IT-infrastruktur, inkludert skytjenester, overvåking, analyse- og hendelseshåndtering og beredskaps- og gjenopprettingsevne

I media kan man nærmest daglig lese om dataangrep og hendelser mot norske virksomheter, herunder også kommuner.

[4] https://www.ssb.no/statbank/table/12019/tableViewLayout1/

[5] https://www.ssb.no/statbank/table/12036/tableViewLayout1/

Tabell 12617[6] under gir en indikasjon på sikkerhetsproblemer i kommunal sektor.

12617: IKT-sikkerhetsproblemer (prosent), etter statistikkvariabel, status for sikkerhetsproblemet, forvaltningsnivå og år		Har vært utsatt for sikkerhetsproblemet		Ukjent/ikke relevant	
		2019	2022	2019	2022
Sammenbrudd i forbindelsen til internett eller andre eksterne nettverk	Fylkeskommuner	18,8	30,0	..	..
	Kommuner	17,3	17,8	5,0	3,4
Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid	Fylkeskommuner	6,3	10,0	..	..
	Kommuner	10,5	2,0	8,0	5,6
Angrep av typen 'denial of service'	Fylkeskommuner	62,5	30,0	..	..
	Kommuner	11,3	9,6	13,3	8,8
Uautorisert tilgang til systemer eller data	Fylkeskommuner	31,3	50,0	6,3	10,0
	Kommuner	6,3	16,4	20,3	13,8
Datatap pga manglende backup	Fylkeskommuner	..	10,0	..	..
	Kommuner	4,5	0,8	8,8	4,8
IT-misbruk av økonomisk karakter	Fylkeskommuner	..	10,0	..	..
	Kommuner	6,8	7,9	10,0	6,8
Forsøk på identitetstyveri (phishing)	Fylkeskommuner	68,8	90,0	6,3	..
	Kommuner	52,1	65,3	17,8	13,0
Virksomhetens IKT-utstyr har kommet på avveie	Fylkeskommuner	50,0	50,0	37,5	10,0
	Kommuner	19,3	18,9	16,3	15,8

Det er altså hevet over enhver tvil at kommunene er, og har vært utsatt for sikkerhetsproblemer, jf dataangrep og hendelser i kommunal sektor. Det som også er interessant er andelen av kommuner som melder at sikkerhetsproblemer er ukjent. At det er ukjent om hendelser har oppstått eller ikke er en indikator på manglende rapporteringsmetodikk og/eller evne til å fange opp hendelser, noe som også underbygger funnene beskrevet under styringsevne over.

Tabell 12618[7] nedenfor gir en indikasjon på hvilke tiltak kommunal sektor har gjort for å øke sikkerheten og robustheten. Tiltakene i tabellen stemmer i stor grad med NSM sine grunnprinsipper[8] for IT-sikkerhet. Tabellen gir ikke informasjon om dybden eller effekten av tiltakene.

12618: Tiltak for IKT-sikkerheten (prosent), etter statistikkvariabel, status for tiltak, forvaltningsnivå og år		%	
		2019	2021
Oppbevaring av backup på annen lokalitet enn driftsmiljøet	Fylkeskommuner	100,0	100,0
	Kommuner	90,5	82,6
Rutinemessige tester som verifiserer at back-up ikke er korrupt eller manipulert	Fylkeskommuner	87,5	60,0
	Kommuner	60,9	65,5
Nødstrømsanlegg	Fylkeskommuner	75,0	90,0
	Kommuner	75,4	77,5
Program for avdekking og varsling av uønsket/uventet trafikk	Fylkeskommuner	75,0	80,0
	Kommuner	60,9	59,8
Program for avdekking av identitetstyveri (phishing)	Fylkeskommuner	68,8	80,0
	Kommuner	51,9	60,4
Rutinemessige penetrasjonstester på interne systemer	Fylkeskommuner	37,5	40,0
	Kommuner	29,3	30,8
Rutiner for installering av sikkerhetspatcher på systemer	Fylkeskommuner	100,0	100,0
	Kommuner	80,5	82,9
Nødløsning for kommunikasjon (alternativer for data- og telekommunikasjoner)	Fylkeskommuner	68,8	80,0
	Kommuner	73,7	73,8
Tofaktor-autentisering for ansatte ved ekstern innlogging til virksomhetens IKT-systemer	Fylkeskommuner	81,3	90,0
	Kommuner	59,4	77,8
Rollebasert brukersystem: en ansatt skal bare ha tilgang til området han/hun arbeider med (Least privilege prinsipp)	Fylkeskommuner	100,0	80,0
	Kommuner	86,2	84,9
Sentrale loggtjenester	Fylkeskommuner	87,5	60,0
	Kommuner	60,2	61,5
Tekniske tiltak for behandling av sensitive data (f. eks. kryptering, digital signering)	Fylkeskommuner	87,5	90,0
	Kommuner	70,2	74,6
Kryptering av virksomhetens bærbare IKT-utstyr	Fylkeskommuner	50,0	40,0
	Kommuner	20,8	28,5

Situasjonsbeskrivelsen som kommer frem ved å analysere tabellen kan sies å være noe bedre enn det som fremsettes muntlig i dialog med kommunene. Samtidig viser tabellen med all tydelighet at selv i 2021 er det mer enn 60 kommuner som ikke har noe så grunnleggende som rutiner for installering av sikkerhetspatcher på systemer på plass, og mer en 240 kommuner har ikke

[6] https://www.ssb.no/statbank/table/12617/tableViewLayout1/

[7] https://www.ssb.no/statbank/table/12618/tableViewLayout1/

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

rutinemessig penetrasjonstesting internt. Fravær av det første tiltaket øker sårbarhetsflaten og det vil være sannsynlig at disse kommunene kan bli rammet av for eksempel løsepengevirus. Hvis man regner disse kommunene inn i de som ikke gjennomfører penetrasjonstesting internt er det fortsatt mer enn 150 kommuner som ikke kjenner til sin faktiske tilstand på infrastrukturen.

Digdirs rapport fra 2020 trekker også frem tall fra 2018 som DSB har innhentet. Disse tallene er trolig bedre i 2023, men i dialog med kommunene har det kommet frem at situasjonen fra 2018 ikke har endret seg betydelig: «At under 25 % av både fylkeskommuner og kommuner gjennomfører beredskapsøvelser knyttet til informasjonssikkerhet, indikerer at øvelser ikke gjennomføres i tilstrekkelig grad. Dette indikerer at både fylkeskommuner og kommuner i stor grad trenger hjelp til å komme i gang med å gjennomføre jevnlige øvelser knyttet til informasjonssikkerhet.»

Oppsummering

Det er i stor grad sammenfall mellom de funn Riksrevisjonen, Digitaliseringsdirektoratet, DSB og KS har av funn og det kommunene selv rapporterer som behov. Situasjonen og dermed behovet for den enkelte kommune divergerer fra andre, og det er dermed ikke mulig å trekke en enkelt konklusjon på tilstand. Tiltak som bør innføres må dermed adressere alle behov. Dette innebærer at det i gjennomføring av tiltak må tas høyde for kommunenes ulike situasjon.

Vedlegg F – Fagnotat SOC

Security Operations Center i kommunal sektor

Innhold

Innledning 2
Avgrensning 3
Hva er et Security Operations Center? 3
Funksjon 3
Tjenesteleveranser 4
Struktur og kompetanse 5
Verktøy 5
Kommunenes rammevilkår og behov 6
Vurderingskriterier 6
A: Kompetanse 6
B: Økonomi 7
C: Kunnskap om lokale forhold 7
D: Respons/reaksjonstid 7
E: Volum 7
Muligheter og utfordringer for kommunal sektor og SOC-funksjoner 8
Lokal SOC – SOC i kommunen 8
Regional SOC – SOC-samarbeid 8
Nasjonal SOC for kommunal sektor 9
Kommersiell SOC – kjøp av SOC fra kommersielle aktører 10
Drøfting av alternativene 12
Anbefaling 13

Innledning

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

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

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

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

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

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

Alternativene som drøftes er:

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

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

Avgrensning

Dette notatet beskriver:

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

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

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

Hva er et Security Operations Center?

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

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

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

Funksjon

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

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

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

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

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

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

Tjenesteleveranser

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

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

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

Figure 3: First service framework – Typical SOC services

Sekundære tjenester:

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

Struktur og kompetanse

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

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

Verktøy

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

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

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

Kommunenes rammevilkår og behov

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

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

Vurderingskriterier

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

A: Kompetanse

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

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

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

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

B: Økonomi

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

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

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

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

C: Kunnskap om lokale forhold

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

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

D: Respons/reaksjonstid

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

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

E: Volum

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

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

Muligheter og utfordringer for kommunal sektor og SOC-funksjoner

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

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

Lokal SOC – SOC i kommunen

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

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

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

Regional SOC – SOC-samarbeid

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

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

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

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

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

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

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

Nasjonal SOC for kommunal sektor

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

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

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

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

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

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

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

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

Kommersiell SOC – kjøp av SOC fra kommersielle aktører

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

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

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

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

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

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

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

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

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

Drøfting av alternativene

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

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

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

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

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

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

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

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

Anbefaling

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

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

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

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

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

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

Rapport:
Evaluering av sektorvise responsmiljøer

Justis- og beredskapsdepartementet
Sak 21/6916

Juli 2022

www.kpmg.no

Sammendrag

På oppdrag for Justis- og beredskapsdepartementet (JD) har KPMG gjennomført en evaluering av ordningen med sektorvise responsmiljøer (SRM). Formålet med evalueringen er å bidra til JDs og Nasjonal sikkerhetsmyndighets (NSM) beslutningsgrunnlag for den videre utviklingen av SRM-ordningen.

Vi vil benytte anledningen til å takke alle de engasjerte og kunnskapsrike medarbeiderne i SRM-ordningen som har tatt seg tid og stilt opp. Dette har bidratt til å gi oss viktig innsikt i ordningens virkemåte. Vi vil også takke JD for en god og konstruktiv dialog gjennom hele prosjektperioden.

Bakgrunn

Etableringen av SRM i Norge har blant annet sitt utspring i Nasjonal strategi for informasjonssikkerhet (2012). I 2017 kom den første stortingsmeldingen om IKT-sikkerhet «IKT-sikkerhet – Et felles ansvar», der styrking av den nasjonale evnen til å avdekke og håndtere digitale angrep var et av hovedområdene. For å understøtte sektorene og virksomhetene i deres arbeid med å etablere responsmiljøer, og for å klargjøre forholdet mellom virksomhet, SRM og det nasjonale responsmiljøet hos NSM, ble det i 2017 gitt ut et Rammeverk for håndtering av IKT-sikkerhetshendelser. Rammeverket legger til grunn at SRM skal ha en sentral rolle i hendelseshåndteringen. En rekke sektorer har utpekt SRM, men det er stor variasjon i modenhet, omfang, kompetanse og innretning mellom SRM.

Sentrale observasjoner

KPMGs overordnede inntrykk gjennom evalueringsoppdraget er at samarbeidet mellom de ulike aktørene fungerer godt, det er god utveksling av informasjon, metoder, erfaringer og kompetanse på tvers av miljøene, og at ordningen med SRM har gitt et mer samlet cybersikkerhetsmiljø i Norge.

Gjennom dokumentanalyse, spørreundersøkelse og intervjuer har KPMG 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

KPMGs anbefalte prinsipper for videreutvikling

KPMG foreslår et sett med prinsipper med formål om å styrke nasjonal evne til å avdekke og håndtere hendelser:

1. Rammeverket bør i større grad inkludere forebyggende arbeid med IKT-sikkerhet i tillegg til operative aktiviteter innen hendelseshåndtering
2. Den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner
3. Spesifikke sektorvise behov skal ligge til grunn for opprettelsen av SRM

4. Det bør etableres formelle minimumskrav for et utpekt SRM
5. De ulike aktørenes rolle i hendelseshåndteringen bør nyanseres og tydeliggjøres

Forslag til videreutvikling av ordningen med sektorvise responsmiljøer

Formålet med forslagene til videreutvikling av dagens ordning med SRM er å nyansere ordningen og gjøre den mer behovstilpasset. Dette innebærer å bevege seg fra like krav og forventninger til alle sektorer og SRM, til å tillate ulike løsninger basert på om det er behov for en sektorspesifikk funksjon.

Det anbefales å stille ulike nivå av krav til responsmiljøene og samhandlingen mellom dem og sikkerhetsmyndigheten basert på følgende:

- ✓ hvor kritisk tilhørende virksomheter er for den nasjonale sikkerheten, og følgelig
- ✓ hvor omfattende konsekvenser en IKT-sikkerhetshendelse i disse virksomhetene vil få

Ettersom det pågår et arbeid i departementene med å identifisere grunnleggende nasjonale funksjoner og virksomheter som har vesentlig eller avgjørende betydning for disse, anbefales det å knytte nivåene i SRM-ordningen til dette arbeidet.

Det foreslås en tre-nivå modell der samhandlingsnivået og minimumskravene øker med virksomhetenes betydning for grunnleggende nasjonale funksjoner. Det er viktig å påpeke at forslaget utgjør et minimumsnivå, og at et SRM står fritt til å tilby ytterligere tjenester til sektoren der man vurderer dette som hensiktsmessig.

Nivå 0 – Basisnivå

Formålet med basisnivået er å sikre at varsling innenfor alle sektorer blir ivaretatt, og at alle virksomheter har tilgang til generell kunnskapsdeling i form av veiledere og annen generell rådgivning fra NSM. Dette nivået er et minimumsnivå som gjelder for alle sektorer, og bør dekke alle virksomheter uavhengig av tilknytning til SRM.

Nivå 1 – Vesentlig betydning

Formålet med nivå 1 er å sikre sektorspesifikk kompetanse i forbyggende og operativ IKT-sikkerhet i sektorer med virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner (GNF) eller av andre grunner har behov for sektorspesifikk kompetanse og koordinering.

På dette nivået er det utpekt et SRM av departementet. Disse skal oppfylle et sett med minimumskrav for dette nivået. For å sikre at SRM har nok kapasitet og kompetanse til å ivareta minimumskravene kan ulike departementer velge å samarbeide om en funksjon, spesielt i sektorer med begrenset rolle i samfunnskritiske funksjoner.

Nivå 2 – Avgjørende betydning

Formålet med nivå 2 er å styrke det forebyggende og operative samarbeidet på tvers av sektorer for å sikre samfunnets viktigste funksjoner.

Offentlige og private virksomheter som har avgjørende betydning i å understøtte grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM, der det er tett samhandling mellom aktørene på alle områder i hendelseshåndteringen.

Innholdsfortegnelse

Innholdsfortegnelse 4

1 Innledning 5

1.1 Bakgrunn 5

1.2 Problemstillinger og formål 5

1.3 Metodisk tilnærming 6

1.4 Begrep og definisjoner 8

1.5 Rapportens videre oppbygging 9

2 SRM: Organisering og virkemåte 11

2.1 Om SRM-ordningen og rammeverk 11

2.2 SRM inkludert i evalueringen 12

3 Utfordringer i dagens ordning og KPMGs vurderinger 13

3.1 Store variasjoner i organisering, ansvarsfordeling og virkemåte 13

3.2 Utfordringer vedrørende sektorprinsippet 16

3.3 Kompetanse og kapasitet 17

3.4 Private aktørers rolle 17

3.5 Kommunikasjon og samarbeid 18

3.6 Oppsummerende vurderinger og anbefalte prinsipper for videreutvikling 20

4 Videreutvikling av ordningen med SRM 24

4.1 Forslag til videreutvikling av ordningen med SRM 24

4.2 Vurdering av administrative og økonomiske konsekvenser 29

Vedlegg 33

1 Innledning

I dette kapittelet gir vi kort rede for bakgrunnen for oppdraget, problemstillinger og formål. Videre beskrives oppdragets metodiske tilnærming, begrepsbruk og definisjoner. Avslutningsvis presenteres rapportens struktur og videre oppbygging.

1.1 Bakgrunn

Etableringen av sektorvise responsmiljøer (SRM) i Norge har blant annet sitt utspring i Nasjonal strategi for informasjonssikkerhet (2012). Behovet for SRM ble aktualisert i august 2014 da det for første gang ble oppdaget at Norge var utsatt for et målrettet digitalt angrep mot en hel sektor. Om lag 50 bedrifter i olje- og energisektoren mottok én eller flere e-poster med skadevare. Omfanget av angrepet var uavklart, og Nasjonal sikkerhetsmyndighet (NSM) valgte derfor å varsle hele sektoren, totalt 300 bedrifter. Arbeidet med denne brede varslingen avdekket at man på nasjonalt nivå ikke hadde nødvendig oversikt over ulike sektorer. Basert på anbefaling fra NSM utarbeidet Justis- og beredskapsdepartementet (JD) "Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer" i 2014.

Parallelt arbeidet Lysneutvalget med utredningen «Digital sårbarhet – Sikkert samfunn» som ble lagt frem i november 2015. Utvalget ble nedsatt for å kartlegge samfunnets digitale sårbarhet. I utredningen ble det gjentatte ganger påpekt et behov for en sektortilnærming, uten at utvalget hadde det nødvendige grunnlaget for å vurdere i hvilken grad modellen var hensiktsmessig og innført i tråd med anbefalingene.

I 2017 kom den første stortingsmelding om IKT-sikkerhet «IKT-sikkerhet – Et felles ansvar», der styrking av den nasjonale evnen til å avdekke og håndtere digitale angrep var et av hovedområdene. Et sentralt tiltak for å bidra til en slik styrking var etableringen av et rammeverk for håndtering av IKT-sikkerhetshendelser. Som en følge av dette ble også ordningen med sektorvise responsmiljøer etablert. Responsmiljøene skulle ha oversikt i egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM. Et utkast til rammeverk ble benyttet under den nasjonale øvelsen IKT-16, slik at erfaringer fra øvelsen kunne benyttes i arbeidet med å ferdigstille rammeverket.

Rammeverk for håndtering av IKT-sikkerhetshendelser ble fastsatt av JD og Forsvarsdepartementet (FD) i desember 2017 og sendt ut til departementene for implementering innenfor de respektive forvaltningsområdene.

I 2018 leverte IKT-sikkerhetsutvalget en rapport der mandat og organisering innen IKT-sikkerhet var vurdert. Som en del av dette arbeidet så man på i hvilken grad rammeverket var innført i tråd med intensjonen og om man hadde oppnådd ønsket effekt. Et funn var at flere sektorer ikke hadde etablert egne responsmiljøer. Manglende finansiering, begrenset tilgang på relevant kompetanse og at ikke alle virksomheter hadde naturlig tilhørighet i en sektor ble trukket frem som mulige årsaker.

1.2 Problemstillinger og formål

Etter noen års erfaring med ordningen med sektorvise responsmiljøer ønsker JD å gjennomføre en ekstern evaluering av ordningen. Formålet med evalueringen er å bidra til JDs og NSMs beslutningsgrunnlag for den videre utviklingen av ordningen med sektorvise responsmiljøer.

Følgende formål og problemstillinger er satt for evalueringen:

- ✓ Kartlegge utfordringer i den nasjonale modellen for håndtering av IKT-sikkerhetshendelser slik denne er beskrevet i Rammeverk for håndtering av IKT-sikkerhetshendelser, med særlig vekt på sektorvise responsmiljøer.
- ✓ Vurdere hvordan ordningen med sektorvise responsmiljøer kan forbedres og anbefale tiltak for videreutvikling, herunder:
    - fordeling av ansvar og oppgaver mellom responsmiljøer på sektornivå og den nasjonale responsfunksjonen i Nasjonal sikkerhetsmyndighet, herunder informasjonsdeling på tvers og mellom nivåer
    - om kompetanse og kapasitet i større grad bør kraftsamles
    - om det er behov for et sett med formelle minimumskrav og kriterier for et sektorvis responsmiljø, f.eks. plikt til informasjonsdeling og varsel om hendelser, og formell utpeking fra et departement
    - forholdet mellom en myndighet og et utpekt sektorvis responsmiljø, som ikke er en del av myndigheten
    - hvordan responsfunksjonene kan utøves for virksomheter som ikke naturlig hører inn under en sektor eller som kan omfattes av flere sektorer
    - om det er alternative former for samarbeid i og mellom sektorer, særlig for å omfatte alle offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner
    - hvilken rolle private aktører kan ha i den nasjonale responsmiljøstrukturen
- ✓ Vurdere de økonomiske og administrative konsekvensene av tiltak som anbefales.

Resultatet av evalueringen er sammenfattet i denne rapporten, og inkluderer både en beskrivelse av dagens situasjon og utfordringer i ordningen så langt.

1.3 Metodisk tilnærming

For å besvare problemstillingene har KPMG valgt en tilnærming som er basert på analyse av dokumenter, en spørreundersøkelse sendt til alle SRM og semi-strukturerte intervjuer med et utvalg SRM og andre interessenter. Det har underveis i prosjektet blitt gjennomført jevnlige møter med JD. Avslutningsvis ble det også gjennomført en workshop med representanter fra SRM. Workshopen var viktig for å innhente synspunkter på våre konklusjoner, vurderinger og anbefalinger. Workshopen har også vært viktig for å forankre rapporten i aktuelle, berørte miljøer.

1.3.1 Metode og datagrunnlag

Det er gjennomført en omfattende analyse av dokumenter som et ledd i arbeidet med rapporten. Sentrale, styrende dokumenter som belyser organiseringen av SRM er gjennomgått, herunder Rammeverk for håndtering av IKT-sikkerhetshendelser, ulike stortingsmeldinger og utredninger. Dernest har det blitt samlet inn en rekke rutiner og annen styringsdokumentasjon fra SRM som har blitt undersøkt. I de fleste tilfeller lyktes KPMG med å samle inn dokumentene før spørreundersøkelse og intervjuguider ble utferdiget. I så måte har dokumentene hatt en særlig sentral plass i det innledende arbeidet med å spesifisere undersøkelsesdesign og i den innledende fasen i forbindelse med utarbeidelse av spørreundersøkelse og intervjuguide. Samtidig har dokumentene også blitt benyttet til å verifisere og kontrollere opplysninger fra intervjuene der dokumentene inneholder informasjon som kan sees i lys av disse. På denne måten har dokumentene også vært benyttet for å kvalitetssikre informasjon fra intervjuer og observasjoner i spørreundersøkelsen.

Spørreundersøkelsen ble distribuert til samtlige SRM. Spørreundersøkelsen er i denne evalueringen et metodisk grep for å kartlegge bredt og skaffe oversikt over SRM på et overordnet nivå. Informasjonen i spørreundersøkelsen bidrar i hovedsak med å gi et helhetlig bilde over status og oppfatninger om SRM-ordningen i det brede lag av SRM.

KPMG har i arbeidet med evalueringen gjennomført intervjuer med et utvalg SRM i forskjellige sektorer. Intervjuobjektene har primært vært ledere i SRM-er, men i enkelte intervjuer har også operative rådgivere/fagpersoner vært med. KPMG har også deltatt i et møte med Nettverk for digital sikkerhet for å samle innspill fra representantene i departementene. I tillegg har det blitt gjennomført intervjuer med andre interessenter og fagpersoner som har bidratt med f.eks. styringsperspektiver eller input til erfaringer fra andre land. Videre er det avholdt flere intervjuer med NSM, og andre private og offentlige virksomheter med en sentral rolle i ordningen. Utvalget er gjort i dialog med JD. Intervjuene har gått i dybden på problemstillingene og forsøkt å belyse hvorfor det er sider ved rammeverket og ordningen som oppleves utfordrende/mindre relevant samt hva som kan gjøres for å styrke det. Det har også vært vektlagt å forstå samarbeidsmønstre opp mot medlemmer, andre SRM, myndighetene og andre sentrale interessenter. Der spørreundersøkelsen har gitt oversikt på et overordnet nivå bidrar intervjuene til at evalueringen i større grad går i dybden. Fullstendig oversikt over informanter og gjennomførte intervjuer er inntatt som vedlegg 2.

Før ferdigstilling av rapporten ble det gjennomført en workshop med flere SRM som har deltatt i prosjektet gjennom intervju og spørreundersøkelse. Formålet med workshopen var å gå ytterligere i dybden av funn som har framkommet med de øvrige metodene, bidra til å vurdere økonomiske og administrative konsekvenser og ellers korrigere eventuelle mangler og misforståelser. Det var videre et mål at workshopen skulle gi prosjektteamet et godt grunnlag for å ytterligere spisse våre vurderinger og anbefalinger.

Observasjonene fra dokumenter, spørreundersøkelsen og intervjuene, ble gruppert etter temaer relatert til gjennomgangens problemstillinger i et analyseskjema, som utgjør grunnlaget for rapporten. De sammenstilte observasjonene ga videre grunnlag for å identifisere anbefalinger om mulige tiltak som kan vurderes iverksatt. Observasjoner og foreløpige anbefalinger ble deretter presentert og diskutert i den nevnte workshopen.

Utredningsinstruksen har ligget til grunn for evalueringen. Dette innebærer at KPMG, ut fra tilgjengelig informasjon, har gjort vurderinger av de økonomiske og administrative konsekvensene av forslag til anbefalinger og alternative modeller/forslag til tiltak som har blitt tilrettelagt som et ledd i evalueringen. Videre har det i gjennomføringen blitt lagt vekt på minimumskravene til utredning som beskrevet i utredningsinstruksen.

1.3.2 Forbehold

Rapporten er utarbeidet på bakgrunn av de opplysninger som er gitt og den dokumentasjonen som har vært gjort tilgjengelig for KPMG. KPMG fraskriver seg ethvert ansvar for mulige feil eller utelatelser som følge av at det har blitt gitt uriktige eller ufullstendige opplysninger eller dokumentasjon.

Evalueringen og forslag til videreutvikling fokuserer kun på aktørene innenfor ordningen med SRM. Alle aktører i ordningen har i tillegg andre samarbeidspartnere, leverandører, kilder og kanaler til situasjonsbilde og informasjon mv., men de inkluderes ikke i denne evalueringen.

KPMG har undersøkt et stort og komplekst område med relativt kort gjennomføringstid. Vi mener likevel at rapporten belyser status for SRM-ordningen og gir konkrete forslag til anbefalinger for JDs videre oppfølging og forbedringsarbeid hva gjelder SRM-ordningen.

Følgende problemstillinger er blitt identifisert, men ikke inkludert i evalueringsoppdraget og forslag til videreutvikling av ordningen med SRM:

- ✓ Nasjonal deteksjonsevne er ikke berørt i rapporten. I hvilken grad dagens juridiske rammer og teknologisk løsninger muliggjør en effektiv nasjonal deteksjonsevne bør utredes videre.
- ✓ Felles samhandlingsplattform for SRM. Forenkling av dagens løsning med mange ulike kanaler kan bidra til enda mer effektiv samarbeid og informasjonsdeling.
- ✓ Felles modell for klassifisering av informasjon. Rapporten nevner kort enkelte utfordringer knyttet til bruk av Traffic Light Protocol (TLP).

- ✓ De fleste norske virksomheter har utarbeidet planverk og motstandsdyktighet i sine IKT-systemer for å detektere og håndtere hendelser i fredstid. Det kan være hensiktsmessig å se nærmere på tiltak, robusthet og beredskap i hele krisespennet samt definere grensesnitt mot Nasjonalt beredskapssystem.
- ✓ Et eventuelt behov for å etablere et «felles-SRM» under departement eller NSM for sektorer som ikke alene har behov for og/eller ressurser til et fullverdig SRM i sin sektor, men har behov for mer enn bare varsling og generell kunnskapsdeling.
- ✓ Forholdet mellom NIS 2 -direktivet og prosessen med å identifisere GNF (se vedlegg 3)

1.4 Begrep og definisjoner

Begrep	Forklaring
IKT-sikkerhetshendelse	«Tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og /eller kritiske samfunnsfunksjoner» (NSM, 2017).
Håndtering av IKT-sikkerhetshendelse / Hendelseshåndtering	«Defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense» (NSM, 2019)
Sektorvis responsmiljø (SRM)	Et sektorvis responsmiljø er en IKT-sikkerhetsfunksjon som skal kunne bistå sin respektive sektor med kompetanse innen operativ IKT-sikkerhet og samtidig være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå.
IKT-sikkerhet / digital sikkerhet	«… at digitale tjenester og produkter er sikre og pålitelige fra starten, og i hele tjenestens eller produktets levetid» (Regjeringen, 2019).
Operativ IKT-sikkerhet	Operativ IKT-sikkerhet er en sikkerhetsdisiplin som kombinerer mennesker, teknologi og prosesser for å avdekke og håndtere trusler og sårbarheter i IKT-domenet. Operativ IKT-sikkerhet har til hensikt å forhindre, detektere, analysere og respondere på IKT-sikkerhetshendelser.
Kritisk infrastruktur	De anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghet.
CERT	«Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. CERT er en lisensbelagttittel. I Norge eksisterer ulike CERT-miljøer. NorCERT er det nasjonale CERT-miljøet. Se også CSIRT.
CSIRT	«Computer Security Incident Response Team" er en koordinerende enhet for IKT-sikkerhet. CSIRT er ikke en lisensbelagt tittel.
Trussel	«Mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet» (NS 5830:2012, s. 4).

Sårbarhet	«Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (NS 5830:2012, s. 5).
Trusselaktør	En kjent eller ukjent aktør (person, organisasjon, land eller annen) som forbindes med en trussel. (NS 5830:2012)
Virksomhet	Betegnelse for en organisatorisk enhet som eksempelvis kan være et departement, et direktorat, en etat, en organisasjon eller et privat foretak. For dette rammeverket må det skilles mellom departementet som sekretariat for politisk ledelse, departementet som en virksomhet som skal ivareta egen sikkerhet, og departementet som overordnet ansvarlig for sikkerhet i egen sektor.
Grunnleggende nasjonal funksjon, GNF	Tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.
Varsling	Med varsling menes initiell rapportering av digitale hendelser, datainnbrudd, eller nylig oppdagede sårbarheter. Varsling innebærer informasjonsoverføring til en eller flere parter.
Rapportering	Med rapportering menes forløpende/jevnlig informasjons-overføring mellom to eller flere parter for å skape situasjons-forståelse. Rapportering knyttes til overføring av informasjon relatert til hendelser, potensielle trusler, sårbarheter eller annen relevant informasjon som bidrar til situasjonsforståelse.
Rammeverk for håndtering av IKT-sikkerhetshendelser, «rammeverket»	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. Siste versjon av rammeverket ble utgitt 07.12.17 av NSM. Rammeverket erstattet "Modell for håndtering av IKT-hendelser" utgitt av Justis -og beredskapsdepartementet i 2014.

Tabell 1 Begrep og definisjoner brukt i rapporten

1.5 Rapportens videre oppbygging

Rapporten er videre delt inn i ytterligere tre kapitler i tråd med de overordnede temaområdene for denne analysen.

I kapittel 2 redegjøres det kort for SRM-ordningen og de SRM som er inkludert i evalueringen.

I kapittel 3 gjøres det rede for observerte utfordringer knyttet til rammeverket og dagens ordning, herunder utfordringer opplevd av aktørene som inngår i rammeverket. Beskrivelsen av de opplevde utfordringene peker på mulige forbedringsområder og er følgelig et viktig grunnlag for å definere hva som ønskes oppnådd for derigjennom å skissere ulike tiltak. Siste del av kapittelet presenterer KPMGs vurderinger av utfordringene og skisserer noen prinsipper som KPMG mener det vil være hensiktsmessig å legge til grunn for det videre arbeidet med utviklingen av ordningen med sektorvise responsmiljøer.

I kapittel 4 presenteres våre anbefalinger, i form av en ny mulig modell. KPMG vurderer mulige virkninger av tiltakene, begrunner hvorfor KPMG anbefaler tiltakene og skisserer hvem som blir berørt og på hvilken måte.

2 SRM: Organisering og virkemåte

2.1 Om SRM-ordningen og rammeverk

Rammeverk for håndtering av IKT-sikkerhetshendelser

NSM beskriver at hensikten med rammeverket er å avklare og tydeliggjøre innsatsen mellom relevante aktører for å være bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. Videre skal det bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser.

Rammeverket bygger på tre aktørnivåer; virksomheter/systemeiere, sektorvise responsmiljøer og NSM. Det er således lagt opp til at SRM har en sentral rolle i håndteringen av IKT-sikkerhetshendelser. For hvert av aktørnivåene stilles det en rekke forventninger og krav knyttet til hvert av prosesstegene i rammeverket.

Sektorvise responsmiljøer

Etablering av sektorvise responsmiljøer er omtalt i stortingsmeldingen «Samfunnssikkerhet» fra 2012, der det står at «som en minimumsløsning skal det etableres et kontaktpunkt i sektoren for alvorlige IKT-hendelser og prosedyrer for varsling internt i sektoren og opp mot NorCERT[1]". Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere IKT-kriser og hvordan de eventuelt skal skalere opp sine responsmiljøer.» Ordningen omtales også i Nasjonal strategi for informasjonssikkerhet fra 2012, og senest i nasjonal strategi for digital sikkerhet fra 2019. Der står det beskrevet at «Ambisjonen med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT).»[2]

I «Rammeverk for håndtering av IKT-sikkerhetshendelser (2017)» står det at det er departementenes oppgave å påse at det er etablert sektorvise responsmiljøer med et operativt ansvar for å dekke virksomheter innen hele eller deler av departementets myndighetsområde. Frem til et slikt miljø er etablert er det departementet selv som må ivareta oppgavene som ligger til SRM slik som beskrevet i rammeverket. Rammeverket oppgir videre en rekke oppgaver som tillegges de sektorvise responsmiljøene i forbindelse med håndtering av IKT-sikkerhetshendelser.

Det enkelte departementet har stor fleksibilitet knyttet til å vurdere hvorvidt det er hensiktsmessig med ett eller flere SRM i egen sektor.

[1] Nå Nasjonalt Cybersikkerhetssenter (NCSC)

[2] Tiltaksoversikt, Nasjonal strategi for digital sikkerhet (2019), https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

2.2 SRM inkludert i evalueringen

Følgende etablerte SRM er inkludert i evalueringen:

Navn	Overordnet departement	Årsverk	Finansiering	Dekningsområde	Formelt utpekt
JustisCERT	Justis- og beredskapsdepartementet (JD)	< 5	Over statsbudsjett	Hele sektoren	Etablert på oppdrag fra departement i 2012
HelseCERT	Helse- og omsorgsdepartementet (HOD)	>10	Hovedsakelig gjennom statsbudsjett, betalt monitorering i spesialisthelsetjenesten	Hele sektoren	Etablert av departement i 2011
NFCERT	Finansdepartementet (FIN)	>10	Medlemsavgift	Virksomheter som velger medlemskap. NFCERT operer i alle nordiske land (FI, DK, IS, NO, SE)	Forening etablert i 2013. Samarbeider med Finanstilsynet, som formelt er utpekt SRM.
KraftCERT	Olje- og energidepartementet (OED)	>10	Medlemsavgift, samt over statsbudsjett for varsling til ikke-medlemmer	Virksomheter som velger medlemskap, i tillegg til at ikke-medlemmer mottar varsler	Etablert av Statkraft, Statnett og Hafslund i 2014 etter initiativ fra NorCERT og NVE. NVE er formelt utpekt som SRM.
MiljøCERT	Klima- og miljødepartementet (KLD)	< 5	Over statsbudsjett	Direkte underliggende etater	Etablert på oppdrag fra departement
CSS/MilCERT	Forsvarsdepartementet (FD)	N/A	Over statsbudsjett	Forsvarsektoren med enkelte unntak	Forsvaret utpekt av FD. Etablert i Cyberforsvaret på oppdrag fra Forsvarssjefen.
DSS CERT	Kommunal- og distriktsdepartementet (KDD)	< 5	Over statsbudsjett (bevilgningsfinansiert over rammene til DSS).	Alle departementer unntatt FD, JD og UD. Visse andre organisasjoner, slik som Regjeringsadvokaten.	Startet som team for operativ sikkerhet i 2009. Re-etablert som DSS CERT i 2016. Er del av driftsmiljøet for departementenes felles IKT-løsning hos DSS.
Landbruks- og matCERT	Landbruks- og matdepartementet (LMD)	< 5	Over statsbudsjett.	Direkte underliggende etater	Etablert og driftet av Landbruksdirektoratet på oppdrag fra departement.
EkomCERT	Kommunal- og distriktsdepartementet (KDD)	< 5	Over Nkom sine budsjetter. Disse består hovedsakelig av lisenser/sektoravgifter som betales av norske ekomtilbydere.	Alle virksomheter som defineres som ekomtilbydere. Ca. 130 virksomheter har gitt kontaktinformasjon og mottar dermed varsler og informasjon.	Arbeidet med å kartlegge behov og lage kravspesifikasjon for SRM startet i 2015. Operasjonalisert i 2017, etter ett års testing.
eduCSC (tidligere Uninett CERT)	Kunnskapsdepartementet	6 – 10	Gjennom sentrale satsningsmidler og brukerbetaling i perioden 2019-2022. Fra 2023 vil de sannsynligvis kun være finansiert av brukerbetaling.	SRM for høyere utdanning og forskning. Leverandør av sikkerhetstjenester for hele kunnskapssektoren. Dagens kunder er i hovedsak utdanningsinstitusjoner og forskningsinstitutter.	Formelt utpekt som SRM av Unit på vegne av KD i 2020. Forløperen til eduCSC, Uninett CERT har eksistert siden 90-tallet.
Kommune-CSIRT	N/A (IKS, Gjøvik og Lillehammer kommune)	1 – 5	Medlemsavgift	Kommuner som velger medlemskap	Etablert og eid av Gjøvik kommune og Lillehammer kommune. Ikke utpekt som SRM av departementet, men deltar SRM-ordningen etter avtale med NSM.

Tabell 2 Sektorvise responsmiljøer i evalueringen

3 Utfordringer i dagens ordning og KPMGs vurderinger

Gjennom dokumentanalyse, spørreundersøkelse og intervjuer har KPMG identifisert en rekke utfordringer i dagens ordning. Dette kapittel beskriver de identifiserte utfordringene samt KPMGs vurderinger. Kapittelet er strukturert i følgende temaer:

- ✓ Organisering, ansvarsfordeling og virkemåte
- ✓ Sektorprinsippet
- ✓ Kompetanse og kapasitet
- ✓ Private aktørers rolle
- ✓ Kommunikasjon og samarbeid

Basert på vurderingene anbefaler KPMG fem prinsipper for videreutvikling av ordningen med sektorvise responsmiljøer. Disse presenteres i slutten av kapitlet.

3.1 Store variasjoner i organisering, ansvarsfordeling og virkemåte

Vårt overordnede inntrykk er at de sektorvise responsmiljøene er svært forskjellige i måten de er organisert på, hvilke oppgaver de gjennomfører for sitt departement og hvilket dekningsområde de har i sin sektor. Det er identifisert flere utfordringer knyttet til organisering, ansvarsfordeling og virkemåte:

- ✓ Ulikheter i organisering og virkemåte kan føre til at det oppstår gap og uklare grensesnitt hvor enkelte virksomheter ikke dekkes tydelig av SRM.
- ✓ Det er ulike tolkninger av hvorvidt føringer i rammeverket for håndtering av IKT-sikkerhetshendelser er veiledende eller krav.
- ✓ Det er enkelte uklarheter knyttet til, og et ønske om å tydeliggjøre, rolle- og ansvarsfordelingen opp mot NSM, særlig knyttet til håndtering av hendelser.
- ✓ Rammeverket forutsetter at virksomhetene selv følger opp pålagt ansvar, herunder grunnsikring, men det er stor variasjon i hvorvidt virksomhetene har den nødvendige kompetansen og kapasiteten til det.

I det følgende gås det nærmere inn på utfordringer knyttet til hvert enkelt punkt.

3.1.1 Ulikheter i organisering og virkemåte

Det har i forbindelse med evalueringen blitt påpekt av flere SRM at responsmiljøene varierer betydelig når det gjelder organisering, kapasitet og virkeområde. Blant de SRM som KPMG har snakket med varierer antall ansatte mellom ett og over 20 årsverk. Variasjonen i antall årsverk reflekterer naturlig nok også responsmiljøenes oppgaveportefølje samt evne og kapasitet til å løse oppgavene. Det er store variasjoner også hva gjelder antall virksomheter som betjenes av det enkelte SRM. Enkelte SRM

har stort dekningsområde, med flere tusen virksomheter, mens andre kun betjener et lavt antall etater underlagt det overordnede departement eller direktorat.

Som det fremkommer av Tabell 2 er det også store variasjoner knyttet til hvordan dekningsområdet i praksis avgjøres. For de fleste SRM er dekningsområdet definert formelt via føringer gitt av overordnet departement. For enkelte SRM som blir finansiert gjennom medlemsavgifter, blir dekningsområdet definert i praksis av hvorvidt virksomheter selv velger å inngå medlemskap og få tilknytning til responsmiljøene og tjenestene som tilbys.

De ulike SRM har også ulik tjenesteportefølje. Eksempelvis har noen en koordinerende rolle, mens andre har en operativ rolle i hendelseshåndtering eller bistår virksomhetene med teknisk IKT-drift. De fleste SRM som KPMG har gjennomført samtaler med oppfatter ikke at deteksjon og operativ hendelseshåndtering i utstrakt grad skal være en del av deres tjenester. Imidlertid er det eksempler på SRM som definerer hendelseshåndtering som en tjeneste de skal yte til sine medlemmer.

Tjenestetilbudet er i enkelte tilfeller påvirket av finansieringsmodellen, når virksomhetene selv kan velge om de inngår medlemskap med SRM eller ikke, og dermed får tilgang til ulike tjenester.

Store variasjoner i organisering og virkemåte har blitt trukket frem som en utfordring av flere SRM, samt av andre aktører på overordnet nivå, NSM inkludert. Det uttrykkes blant annet at dette fører med seg usikkerhet rundt hvorvidt hele sektorer er dekket eller ikke, og hvilke tjenester som tilbys. I disse tilfellene er det vanskelig for NSM å vite om hele sektoren blir varslet, eller hvilke deler av sektoren ikke er dekket av varslingen via SRM, og dermed ikke inkludert i systematisk varsling fra NSM via SRM til virksomhetene. Det oppleves også av flere SRM at det i liten grad er gitt klare føringer og forventninger til hensiktsmessig organisering.

3.1.2 Ulike tolkninger av føringer i Rammeverk for håndtering av IKT-sikkerhetshendelser

De sektorvise responsmiljøene er tillagt flere ulike ansvarsområder i den nasjonale modellen for håndtering av IKT-sikkerhetshendelser, herunder et særskilt ansvar for å holde oversikt over egen sektor, være informasjonsknutepunkt for alle relevante virksomheter, samt være sektorens bindeledd mot nasjonal responsfunksjon. NSM er etter sikkerhetsloven § 9 tillagt det nasjonale ansvaret for å koordinere håndtering av alvorlige IKT-sikkerhetshendelser mot kritisk infrastruktur. Selv om ansvaret for håndtering av IKT-sikkerhetshendelser er fordelt og lagt til flere aktører på ulike nivå, følger det av ansvarsprinsippet at virksomhetene selv har et særskilt ansvar for å håndtere IKT-sikkerhet i egen virksomhet.

Til tross for at det legges en rekke føringer for SRMs ansvarsområder i rammeverket, foreligger det ingen rettslig plikt for sektorer til å implementere krav og tiltak i rammeverket. Flere har i intervjuer uttrykt at det er delvis uklart hvorvidt føringene som er gitt i rammeverket er veiledende eller fastsatte krav, og ikke alle krav oppleves like relevante. Dette, i kombinasjon med at SRM har store variasjoner i organisering, størrelse og medlemsmasse har ledet til at ulike SRM har tilnærmet seg sitt ansvar ulikt. Det er blant annet store variasjoner i hvilke kjerneoppgaver og tjenester de tilbyr overfor sine underlagte virksomheter.

Videre oppleves det at man ikke i tilstrekkelig grad tolker nasjonale føringer likt, samt at overordnet departement har ulike tilnærminger og behov for ivaretakelse av egen sektor.

3.1.3 Ansvars- og oppgavefordeling mellom SRM og NSM

Den nasjonale modellen for håndtering av IKT-sikkerhetshendelser involverer et mangfold av aktører på ulike nivåer i det norske forvaltningssystemet. I Rammeverk for håndtering av IKT-sikkerhetshendelser er ansvar og grensesnitt beskrevet for en rekke av disse rollene, og spesielt for de tre nivåene rammeverket bygger på; virksomhet/systemeier, SRM og NSM.

Selv om både SRM og NSM opplever at samarbeidet fungerer godt, er det identifisert enkelte utfordringer knyttet til ansvars- og oppgavefordeling mellom dem. Flere opplever at rammeverket ikke

er tydelig nok i beskrivelsen av rollene og oppgavene, eller hvilken informasjon som deles med hvilken aktør, hvilket skaper uforutsigbarhet. De største uklarhetene gjelder forventningene til hendelseshåndtering; i hvilken grad kan SRM forvente å få bistand av NSM i en hendelse og hvordan vil ulike hendelser bli prioritert. Det påpekes at det er liten grad av transparens knyttet til NSMs prioriteringer, hvilket skaper usikkerhet rundt hva SRM kan forvente av NSM ved parallelle hendelser.

Klart definerte ansvarsforhold er viktig for å tydeliggjøre forventninger mellom partene. Til tross for at NSM i rammeverket ikke forventes å bistå med analysekapasitet i hendelseshåndtering, er dette kapasiteter NSM besitter og kan bistå med ved behov. At NSM ved enkelte anledninger yter flere tjenester enn hva som presenteres i rammeverket synes å skape en viss usikkerhet knyttet til hva SRM kan forvente av NSM, og den reelle leveranseevnen innen ulike analysedisipliner. Dette kan føre til en (potensielt feilaktig) oppfattelse av at egen sektor ikke prioriteres.

At dagens SRM har såpass ulik størrelse og modenhet skaper utfordringer for NSM. Ettersom NSM i dag i stor grad utveksler den samme informasjonen til alle SRM blir det utfordrende å finne riktig nivå på informasjonen som deles. Noe informasjon vil eksempelvis bli for avansert for de minst modne SRM, som i større grad ønsker seg informasjon og rådgivning knyttet til etablering av kapasiteter. Det er utfordrende for NSM å vite hvilke forventninger de kan ha til SRM, og hvilken rolle SRM forventer at NSM har overfor dem.

3.1.4 Ansvars- og oppgavefordeling mellom SRM og virksomheter

Rammeverket tar utgangspunkt i at virksomhetene selv har implementert god grunnsikring og har kompetanse innen deteksjon, vurdering og håndtering av hendelser samt at de varsler SRM. Det fremstår derimot for flere SRM som at virksomhetene selv har varierende grad av kjennskap til sitt ansvar, samt mulighet til å ivareta dette som følge av blant annet manglende kompetanse og kapasitet. Følgelig opplever en del SRM å bruke mye tid på å bistå med oppgaver som virksomhetene skal ivareta selv. Flere SRM opplever det som uklart hvor operativt SRM skal bistå virksomhetene, og hva som er den beste måten å støtte virksomhetene på. Enkelte har bevisst valgt å ikke tilby tjenester som kan leveres av private aktører. Flere ser behovet for å gjøre mer enn å oppdage og varsle hendelser, herunder å bistå med mer forebyggende arbeid. NSMs grunnprinsipper nevnes i flere samtaler som et godt verktøy for å støtte virksomhetene med grunnsikring.

Det nevnes også en viss bekymring for at de større medlemmer får litt mindre nytte av ordningen, siden de har omfattende kapasitet og kompetanse selv. Samtidig finnes det tilfeller hvor man utnytter samarbeidet med de store virksomhetene bedre, og virksomhetene ser verdien av å bidra til økt sikkerhet i sektoren.

3.1.5 Formalisering og tilknytning til overordnet departement

Det er variasjoner i SRMs tilknytning til overordnet departement. Noen SRM er tydelig utpekt av overordnet departement og har en klart definert sektor som sitt dekningsområde. Andre er ikke direkte utpekt som SRM av sitt overordnede departement, men har inngått en avtale med aktører som er utpekt SRM slik at disse to til sammen ivaretar SRM-funksjonen for sin sektor. Det er viktig å påpeke at dette nødvendigvis ikke oppleves som en utfordring. Samtidig kan en slik rollefordeling fordre ekstra avklaringer vedrørende ansvarslinjer og grensesnitt mellom de involverte aktørene.

Intervjuene gir et overordnet inntrykk av at SRM opplever varierende klarhet i føringer fra overordnet departement. Enkelte har relativt stor grad av frihet til å utføre sine oppgaver, med lite kontroll fra overordnet departement. Enkelte ønsker i denne sammenhengen mer strategisk styring og dialog. Samtidig oppgir andre å ha klare instrukser og føringer om hvilke oppgaver som skal legges til SRM, spesielt de SRM som har et aktivt styre med representanter med bakgrunn fra informasjonssikkerhet.

3.1.6 Forholdet mellom en myndighet og et utpekt som ikke er en del av myndigheten

Det er noe variasjon i dag om SRM er en del av myndigheten eller ikke. Fra evalueringen fremstår dette ikke som en særskilt utfordring. SRM som ikke er en del av myndigheten har ofte avtalefestet hvilke oppgaver de skal løse i kontrakt med den myndigheten som er formelt utpekt som SRM. Så lenge slike avtaler er på plass fremstår det ikke som problematisk at SRM ikke er direkte underlagt myndigheten. Det er eksempler på at ekstra oppgaver som departementet pålegger SRM knyttet til eksempelvis varsling av virksomheter som ikke er medlemmer, er finansiert via statsbudsjettet.

3.2 Utfordringer vedrørende sektorprinsippet

Gjennom intervjuer er det blitt identifisert enkelte utfordringer knyttet til sektorprinsippet. Flere peker på et gap mellom cybersikkerhetsområdets sektorovergripende natur og sektorprinsippet i staten. Det oppleves videre at sektorbegrepet ikke er tydelig nok definert i rammeverket eller i den nasjonale strategien for digital sikkerhet. Det er også stor variasjon i hvordan en sektor er definert som dekningsområde for SRM; for enkelte er det kun direkte underliggende etater, mens andre har en bredere definisjon som også inkluderer private virksomheter.

Begrepet «sektorvist responsmiljø» kan derfor føre med seg en viss grad av falsk trygghet, all den tid dekningsområdet varierer så mye som den gjør i dagens situasjon. På papiret er det utpekt og etablert et SRM som pålagt i rammeverket, men i realiteten er det uklart om hele sektoren er ivaretatt og for eksempel blir varslet gjennom SRM.

Enkelte departement har brede ansvarsområder, og opplever at det er problematisk å samle dette under en og samme sektorbetegnelse med et utpekt SRM. I disse tilfellene vurderer departementet å etablere flere SRM. Fra NSM sitt ståsted er det en utfordring om flere departement har flere «undersektorer» med respektive SRM, da dette vil øke antall SRM betydelig. Det oppleves også at rammeverket ikke passer inn i tverrsektorielle samarbeid, da det er uklart hvilket departement som i så fall er ansvarlig for SRM.

Det oppleves utfordrende å implementere rammeverket på en måte som inkluderer det private næringslivet i dekningsområdet. Virksomheter kan være del av flere sektorer, hvilket gjør det krevende å avgjøre et tilhørende SRM. Når departementet kan styre de underlagte virksomhetene direkte, er rammeverket relativt enkelt å gjennomføre. Når private aktører er inkludert i dekningsområdet, oppleves det at departementet ikke kan pålegge private aktører oppgaver, men må basere seg på frivillighet.

Enkelte departement har vurdert at de økonomiske rammene begrenser muligheten til å etablere SRM, samt at det finnes få samfunnskritiske funksjoner i sektoren. I noen tilfellene har departement avtalt samarbeid med en annen sektor for de relevante virksomhetene, eller har en mindre enhet som formidler varsling mellom virksomhetene og NSM. Enkelte har etablert samarbeid direkte mellom operative miljøer og NSM og ser ikke merverdi i å etablere SRM.

Flere departement fremhever spesielle behov i sin sektor som en av grunnene til å utpeke et eller flere SRM i egen sektor. Etter KPMGs erfaring er behovene knyttet til forebyggende og operativ IKT-sikkerhet ofte sammenfallende som gjør det hensiktsmessig å vurdere felles løsninger så langt det lar seg gjøre.[3]

Sektorprinsippets effekt for håndtering av og forberedelse til akutte kritiske hendelser har vært kritisert og diskutert både før og etter kriser i samfunnet. Utfordringene er gjentakende og henger nært sammen med at det ikke er en enkelt person som sitter med det fullstendige ansvaret for beredskapen og håndteringen av konkrete hendelser. Sektorprinsippet er først og fremst utfordrende i

[3] Relevant rapport i denne sammenheng: ENISA Report - Sectoral CSIRT capabilities - Energy & Air Transport.pdf

den grad det fører til sektoriell tankegang blant aktørene i de forskjellige sektorene og på den måten hindrer samhandling og effektiv planlegging for håndtering av akutte hendelser. Effektiv krisehåndtering krever samhandling på tvers av etater og tverrsektoriell koordinering[4]. For å minimere utfordringene som følger av sektorprinsippet er det vesentlig å kunne gjennomføre øvelser og annen type samhandling på tvers av sektorene før en kritisk hendelse finner sted. Et av de viktigste premissene for å kunne håndtere tverrsektorielle hendelser av ukjent natur er at sektorene finner sammen og kjenner til hverandres kapasitet og handleevne. På den måten vil en bryte ned de utfordringene sektorprinsippet skaper og heller dra nytte av sektoriell spisskompetanse i hvert enkelt tilfelle – hvilket er begrunnelsen for sektorprinsippet i seg selv.

3.3 Kompetanse og kapasitet

En felles utfordring for alle aktører i ordningen er at det er krevende å tiltrekke seg, og å beholde, relevant digital sikkerhetskompetanse. Etterspørselen etter slik kompetanse har økt kraftig de siste årene. Stadig flere tjenester flyttes over i det digitale domenet, og digitale trusler har blitt noe alle virksomheter må forholde seg til. Dette betyr at det er høy etterspørsel etter et begrenset antall ressurser. Mange SRM rapporterer om at det er vanskelig å beholde kompetanse i organisasjonen. NSM samt SRM innen offentlig sektor med tilhørende lønnsnivå kan komme til kort i rekrutteringsprosessen, fordi privatmarkedet kan tilby mer gunstige betingelser. Når de klarer å tiltrekke seg nyutdannede, er det ikke uvanlig at disse beveger seg videre til privatmarkedet etter noen år, når de har opparbeidet seg erfaring. Dette gjør at det brukes mye tid på opplæring av ressurser som beveger seg videre etter relativt kort tid.

Størrelsen på organisasjonen oppleves som en mulig faktor i å tiltrekke og beholde kompetanse. Det å være et større fagmiljø med høy modenhet synes å være et konkurransefortrinn hva gjelder å tiltrekke og beholde relevant kompetanse. Dette kan være knyttet til at miljøene oppleves som mer interessante for potensielle arbeidstagere – for eksempel vil de ha mer kapasitet til å utøve opplæringsaktiviteter, og arbeidsoppgavene vil i noen tilfeller være mer varierte.

Dagens modell legger opp til at alle departementer skal utnevne et responsmiljø for sin sektor. Dette innebærer at kompetanse plasseres mange ulike steder, og til dels i funksjoner der det reelle ressursbehovet er lavt. Modellen legger med andre ord opp til at kompetanse «smøres tynt utover» de ulike sektorene. Dette er en utfordring, fordi det kan føre til ineffektiv ressursbruk i en bransje med stor konkurranse om kompetanse.

3.4 Private aktørers rolle

Den nasjonale motstandsdyktigheten mot digitale angrep er i stor grad avhengig av IKT-infrastruktur som eies av private aktører. Dette inkluderer internasjonale leverandører som Google, Microsoft og Amazon, samt norske aktører som Telenor og Telia.

I dagens Rammeverk for håndtering av IKT-sikkerhetshendelser fremkommer det ikke hvilken rolle private leverandører av IKT-infrastruktur og andre samfunnsviktige tjenester skal ha i den overordnede modellen. Det samme gjelder for leverandører av sikkerhetstjenester knyttet til deteksjon og hendelseshåndtering, som eksempelvis de godkjente aktørene innen hendelseshåndtering i NSMs kvalitetsordning.

Inkludering av private aktører i SRM-forum i dag synes å bære preg av en organisk vekst av forumet. Noen SRM opplever at flere private aktører burde vært inne i SRM-forumet, andre mener at private aktører ikke burde opptre i SRM-forumet. Det er enighet i at samarbeid med private aktører er viktig for den nasjonale motstandsdyktigheten, men at det er en utfordring at kun enkelte private aktører har

[4] Boin, A., 'T Hart, P. (2007). The Crisis Approach. I: Handbook of Disaster Research. Handbooks of Sociology and Social Research. Springer, New York, NY. https://doi.org/10.1007/978-0-387-32353-4_3

tilgang, uten at begrunnelsen for det er tydelig. Det fører blant annet med seg kommersielle utfordringer, ved at det oppleves at private aktører kan få et konkurransefortrinn gjennom slik tilstedeværelse, og dette igjen kan forhindre effektivt samarbeid og informasjonsdeling i SRM-forumet.

Både NSM og SRM ser behov for et tett samarbeid med private aktører og ønsker en klargjøring av private aktørers rolle i rammeverket for håndtering av IKT-sikkerhetshendelser. eksempelvis i form av klare retningslinjer og kriteria for hvem som skal og ikke skal ha en rolle i den nasjonale ordningen for hendelseshåndtering.

3.5 Kommunikasjon og samarbeid

God kommunikasjon og godt samarbeid er en grunnleggende forutsetning for å skape god situasjonsoversikt og for å effektivt kunne håndtere og redusere konsekvensene av alvorlige IKT-sikkerhetshendelser. Kommunikasjon handler om å formidle og dele informasjon rettidig og ved hjelp av egnede kommunikasjonskanaler. Effektiv utveksling av informasjon innebærer ikke bare overføring av relevant informasjon til mottakeren – like viktig er det at mottakeren får god forståelse av situasjonen og har tilstrekkelig kompetanse til å forstå det som kommuniseres.

Rammeverket beskriver en rekke forventninger til virksomheter, SRM og NSM når det kommer til hvordan de ulike aktørene i ordningen skal samarbeide for å skape god situasjonsoversikt og for å best mulig utnytte samfunnets samlede ressurser for å effektivt håndtere hendelser. Prosedyrer for koordinering, rapportering og ansvarsdeling er med på å definere samarbeidsklimaet og legge til rette for effektive prosesser på tvers av organisatoriske enheter. SRM forventes blant annet å besitte en viss kunnskap om kritisk infrastruktur i egen sektor og virksomheter skal delta i samhandlingsøvelser.

Videre presenteres identifiserte utfordringer knyttet til kommunikasjon og samarbeid mellom NSM og SRM, mellom SRM og til slutt mellom SRM og virksomheter.

3.5.1 Samarbeid mellom NSM og SRM

NSM er det nasjonale fagmiljøet for IKT-sikkerhet og har en nøkkelrolle i koordinering og distribusjon av sikkerhetsrelatert informasjon. Ettersom NSM også er tillagt det nasjonale ansvaret for å koordinere håndtering av alvorlige IKT-sikkerhetshendelser er samarbeid en svært viktig del av NSMs virke. Det har fremkommet gjennom våre intervjuer at det utføres mye godt arbeid fra NSM knyttet til samarbeid og informasjonsdeling, men enkelte forhold blir også utfordret og problematisert.

Flere SRM trekker frem viktigheten av å bygge relasjoner på tvers av SRM og NSM. Det bemerkes av enkelte SRM at tillitt er ekstra viktig for personell som jobber med sikkerhet og at strukturer og prosedyrer i liten grad kan erstatte mellommenneskelig tillitt og relasjoner. Gode relasjoner kan skape effektivt samarbeid. Samtidig er det problematisk dersom samarbeidet i for stor grad beror på mellommenneskelige relasjoner i et arbeidsmarked med stor turnover.

NSM legger til rette for samarbeid med SRM ved hjelp av flere ulike fora og kanaler, blant annet Teams, IRC, Mattermost, og e-post. Blant SRM er det noe misnøye knyttet til de tekniske løsningene som skal understøtte samarbeidet med NSM. Et høyt antall kanaler og verktøy blir trukket frem som en utfordring både av SRM og NSM.

SRM er ikke underlagt sikkerhetsloven, og ikke klarert for skjermingsverdig informasjon og har således ikke tilgang til gradert samhandling. Dette opplever alle parter - NSM, SRM og departementene - som en utfordring som forsinker og forhindrer informasjonsdeling, spesielt i nasjonale kriser.

3.5.2 Samarbeid mellom SRM

I dagens modell legges det også opp til samarbeid mellom SRM. Det forventes blant annet at SRM skal varsle om IKT-sikkerhetshendelser til andre SRM, og på den måten skape effektiv informasjonsflyt om relevante hendelser på tvers av sektorer.

NSM legger til rette for samarbeid mellom SRM. For å sikre bred informasjonsdeling har NSM etablert flere fora for informasjonsdeling fra NSM til SRM. I disse foraene blir det også oppfordret til deling av informasjon fra SRM slik at kunnskap og erfaringer flyter på tvers. Eksempelvis gjennomføres det virtuelle koordineringsmøter annenhver uke og fysiske SRM-møter kvartalsvis. Under disse møtene oppfordres SRM til å dele informasjon om hendelser innen sitt respektive dekningsområde slik at NSM får oppdatert situasjonsforståelse både sektorvis og tverrsektorielt.

En fundamental forutsetning for informasjonsdeling er tillit blant SRM. Også blant SRM er tillit i stor grad basert på at deltakere kjenner hverandre, har jobbet sammen over en lengre periode og kjenner hverandres kompetansenivå. En utfordrende faktor i dagens situasjon er det økende antallet deltakere i samarbeidsforaene. Ettersom stadig flere SRM etableres, blir det flere deltakere i foraene, og det oppleves som mindre oversiktlig.. Dette fører til tilbakeholdenhet knyttet til informasjonsdeling. Når i tillegg modenheten i SRM varierer, svekkes tilliten til at alle i SRM-ordningen evner å håndtere informasjonen i henhold til behovet for skjerming. Mindre modne SRM kan også ha høyere terskel til å dele informasjon eller delta diskusjonen i ulike fora. Dette medfører at det formes mindre grupper av SRM som jobber tettere med hverandre.

Tillit kan også fasiliteres ved hjelp av felles struktur og retningslinjer. Trafikklysprotokollen[5] (TLP) blir trukket frem som et eksempel i denne kontekst. Flere SRM benytter TLP ved deling av informasjon til andre SRM. Samtidig er enkelte SRM usikre på hvorvidt alle SRM forstår hvordan informasjon skal håndteres i henhold til TLP og de velger derfor å sende med en beskrivelse av TLP-definisjonen når informasjonen merkes med TLP. I tillegg er det noen juridiske utfordringer i bruk av TLP, spesielt med TLP:RØD når en enkelt ansatt har informasjon som kan ramme virksomheten, men ikke er tillatt av protokollen å dele informasjon videre inn i organisasjonen.

Det synes å være ganske store forskjeller på hvor mye de ulike SRM deler i de etablerte samarbeidsforaene. Enkelte SRM er veldige aktive og deler mye. På den andre siden er det flere SRM som i all hovedsak mottar informasjonen uten å selv dele, hvilket påvirker villigheten til å dele og tilliten hos andre SRM. Konkret blir det vist til at det for enkelte SRM er ønskelig med mer avgrensede fora for å fremme delingsvilje. Det råder en oppfatning blant en del SRM om at spennet mellom de SRM er i ferd med å bli såpass stort at verdien av å samhandle på tvers avtar.

For å formalisere samarbeidet mellom SRM, etterlyses det en formell samarbeidsavtale. Dette er en forutsetning for effektivt samarbeid ved en hendelse for å kunne dele eksempelvis ressurser, kompetanse og informasjon logger som kan inneholde personopplysninger. Enkelte SRM trekker også frem et behov for felles øvelser.

3.5.3 Samarbeid mellom SRM og virksomheter

Hvordan SRM samarbeider med virksomhetene i deres sektor varierer avhengig av SRMs størrelse, tjenesteportefølje og modenhet, i tillegg til sektorens generelle modenhet innen IKT-sikkerhet. Generelt sett synes det å være en sammenheng mellom sektorens generelle modenhet innen IKT-sikkerhet og SRMs modenhet. Sektorer som over tid har vært særlig utsatt for digitale trusler har også over tid hatt behov for å utvikle kapasiteter, og således kommet lenger når det kommer til samhandling og informasjonsdeling.

De mest modne SRM har på bakgrunn av sin kompetanse og tjenesteportefølje bedre forutsetninger for å rådgi virksomhetene i sin sektor. Et SRM kan kjenne godt til trussel- og sårbarhetsbildet i egen sektor ved å kun være en informasjonsknutepunkt for denne type informasjon. Likevel vil SRM som også utfører deteksjon og/eller sårbarhetshåndtering gjerne besitte en dypere kunnskap om aktuelle

[5] Traffic Light Protocol (TLP) (first.org)

trusler og sårbarheter, og på bakgrunn av denne kunnskapen være bedre rustet for å gi konkrete råd om hvordan virksomhetene i sektoren skal kunne sikre seg og oppdage relevante trusler, eller hvilke tiltak som bør iverksettes for å utbedre sårbarheter.

Det er stor variasjon i IKT-sikkerheten i norske virksomheter. Disse variasjonene gir utslag på virksomhetenes opplevde behov for SRM-ordningen. Virksomhetene som over tid har opparbeidet seg høy modenhet innen operativ IKT-sikkerhet synes i mindre grad å se verdien av SRM, da de selv mottar trusselinformasjon gjennom egne kilder noen ganger til og med raskere enn hva som deles fra SRM og samtidig har etablert samarbeid med andre modne virksomheter. Til tross for at de modne virksomhetene har mindre bruk for SRM, så har de mest å bidra med inn i SRM-ordningen og generelt sett synes det å være slik at det er de mest modne virksomhetene som samarbeider tettest opp mot sitt SRM.

I andre enden har man virksomheter med lav modenhet innen IKT-sikkerhet. For at virksomhetene skal kunne få verdi av trussel- og sårbarhetsvarsler fra et SRM må virksomheten ha en viss kompetanse og kapasitet til å motta, behandle og agere på informasjonen som kommer fra SRM. Uten tilstrekkelig kapasitet vil varslene gi liten verdi for virksomhetene som mottar disse. Virksomhetene med lav modenhet er således også de virksomhetene som jobber minst opp mot sitt SRM. Enkelte ønsker derfor at NSM skal kunne pålegge virksomhetene et grunnleggende sikkerhetsnivå.

Hvor mye rådgivning SRM gir til virksomhetene i sin sektor varierer, og det samme gjør virksomhetenes ønske om råd og veiledning fra SRM. Slike tjenester har enkelte SRM avtaleregulert for å skape tydelighet i SRMs leveranser. Flere SRM ønsker å skille mellom tjenester som SRM kan levere sammenlignet med tjenester som private virksomheter tilbyr for å unngå å konkurrere med private virksomheter, mens andre har tjenester som kan sammenlignes med drift- eller rådgivningstjenester innen IT og informasjonssikkerhet.

3.6 Oppsummerende vurderinger og anbefalte prinsipper for videreutvikling

Dette kapittelet introduserer noen overordnede prinsipper for den videre utviklingen av ordningen. Formålet med prinsippene er å bidra til styrking av den nasjonal evnen til å avdekke og håndtere digitale angrep gjennom å fokusere ressurser til de sektorene som har virksomheter med betydning for grunnleggende nasjonale funksjoner, men samtidig sørge for en grunnleggende dekning i alle sektorer.

Hvert prinsipp hviler på vurderinger av utfordringsbildet som er presentert i delkapitlene overfor. Kapittel 4 presenterer en alternativ modell for ordningen med SRM som bygger på prinsippene. KPMG mener, uavhengig av endelig valgt organisering og retning for ordningen, at prinsippene under bør legges til grunn for å møte utfordringene og behovene som har blitt identifisert i denne evalueringen.

Følgende prinsipper foreslås for videreutvikling av ordningen med SRM:

Prinsipp 1: Rammeverket bør i større grad inkludere forebyggende arbeid med IKT-sikkerhet i tillegg til operative aktiviteter innen hendelseshåndtering

For å redusere konsekvensene og raskest mulig gjenopprette normaltilstand ved en hendelse er det nødvendig å håndtere den effektivt etter en definert prosess. Hendelseshåndtering er en prosess som

kan beskrives med følgende faser; forberedelse; deteksjon og analyse; skadebegrensning og gjenoppretting; og evaluering og læring. Når hendelsen inntreffer er det for sent å utarbeide planverk, prosedyrer, rapporteringsrutiner og kommunikasjonsstrategier. Derfor inngår forberedelse som en sentral del av selve prosessen. Selv om dagens rammeverk beskriver sentrale aspekter og forventninger til aktørene innen håndtering av IKT-sikkerhetshendelser, mangler både tydeliggjøring og oppfølging av oppgavene. Metoden for å klassifisere IKT-sikkerhetshendelser fremstår lite hensiktsmessig og vil gi lite verdi ved en reell hendelseshåndtering.

Rammeverket for håndtering av IKT-sikkerhetshendelser dekker i liten grad de forebyggende aktivitetene som bør gjennomføres av en operativ IKT-sikkerhetsfunksjon, utover ren hendelseshåndtering. Anerkjente rammeverk for operative IKT-sikkerhetsfunksjoner belyser viktigheten av å levere flere ulike tjenestekategorier. FIRST sitt rammeverk (se Vedlegg 1 for mer informasjon om rammeverket), benytter tjenestekategoriene deteksjon, hendelseshåndtering, sårbarhetshåndtering, situasjonsforståelse og kunnskapsdeling. Disse tjenestekategoriene gjenspeiler viktigheten av koblingen mellom det forebyggende og det operative arbeidet som gjøres av operative IKT-sikkerhetsfunksjoner.

Erfaring viser at operative IKT-sikkerhetsfunksjoner bør ha en helhetlig tilnærming og utnytte synergier av å etablere kapabiliteter som understøtter hverandre. Det bør være klare koblinger mellom utførelse av operativt arbeid innen deteksjon og hendelseshåndtering og videreutvikling av egne operative kapabiliteter. På samme måte bør arbeid med trussel- og sårbarhetsinformasjon benyttes for å styrke motstandsdyktigheten mot angrep og evnen til å avdekke og håndtere digitale angrep.

En ny eller revidert modell bør i større grad inkludere forebyggende arbeid innen IKT-sikkerhet og balansere dette mot det operative arbeidet som utøves. Samtidig bør forventninger til partene innen de ulike tjenestekategoriene tydeliggjøres og følges opp. Det vil også være hensiktsmessig å videreutvikle rammeverkets klassifisering av IKT-sikkerhetshendelser. Klassifiseringen kan forenkles til konkrete nivåer og til å inkludere hvem som er ansvarlig eller bør være involvert innenfor de ulike nivåene, samt hva de ansvarlige bør gjøre[6].

Prinsipp 2: Den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner

Sektorprinsippet som ligger til grunn for dagens ordning har den begrensning at digitale sikkerhetshendelser svært ofte rammer på tvers av sektorielle skillelinjer. Samhandlingen mellom SRM, som i hovedsak foregår i SRM-forumet, fungerer som et organ der erfaringer og innsikt kan deles og diskuteres.

Det vil være hensiktsmessig å danne samarbeidsstrukturer som i større grad er fokusert mot koordinert innsats mot felles mål, der man jobber sammen både forebyggende og operativt. Det er ikke realistisk å få til slikt samarbeid rettet mot alle virksomheter – til det er antall virksomheter for stort. Det bør heller gjøres et utvalg av virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner.

En slik samarbeidsstruktur vil kunne styrke den helhetlige motstandsevnen mot digitale angrep rettet mot samfunnets viktigste funksjoner. Det vil i mindre grad være bundet av sektorprinsippet, men heller være fokusert mot grunnleggende nasjonale funksjoner, uavhengig av sektortilhørighet. Offentlige og private virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM. Dette kan åpne for tettere samarbeid både forebyggende og operativt der det kan legges til rette for deling av gradert informasjon og der tillitsnivået er høyt. Man vil videre kunne basere seg på lovkrav gitt i sikkerhetsloven (ettersom disse virksomhetene vil være underlagt denne).

[6] NCSC-UK har utarbeidet et system for kategorisering av IKT-sikkerhetshendelser som kan benyttes som utgangspunkt eller inspirasjon: New Cyber Attack categorisation system to improve UK... - NCSC.GOV.UK

Prinsipp 3: Spesifikke sektorvise behov skal ligge til grunn for opprettelsen av SRM

SRM skal løse oppgaver som ikke kan løses på nasjonale nivå eller av virksomhetene selv. Dette innebærer at hvis det ikke avdekkes oppgaver som mest hensiktsmessig kan løses på sektornivå, bør man ikke opprette SRM. For de sektorene der det er vurdert hensiktsmessig med et SRM, men man ikke alene har nok kapasitet eller kompetanse til å ivareta minimumskravene kan det være et alternativ å søke samarbeid med andre SRM som kan dekke mer enn en sektor. Slik kan man bedre utnytte ressursene og sikre sterkere miljøer.

Det bør også vurderes om en felles-funksjon bør løftes til nasjonalt nivå og ligge under NSM. En sånn fellesfunksjon kan dekke alle virksomheter som ikke har naturlig tilknytning til sektor eller i en sektor uten SRM.

En viktig forutsetning for god informasjonsdeling, sparring og samhandling mellom miljøene er at det er høy tillit mellom samarbeidspartene. Flere peker på at en av suksessfaktorene med dagens ordning er at det størrelsesmessig er en oversiktlig gruppe med høy tillit og stor delingsvilje. I et scenario med et stadig økende antall SRM og et samarbeidsforum som vokser i størrelse, risikerer man redusert oversikt og tillitspulverisering. Det fremstår derfor lite hensiktsmessig å komme i en situasjon der antall SRM blir uhåndterlig høyt.

Prinsipp 4: Det bør etableres formelle minimumskrav for et utpekt SRM

Basert på utfordringsbildet er det flere forhold som taler for at man bør etablere formelle minimumskrav for SRM. Først og fremst vil det trolig lede til større grad av tydelighet overfor NSM og andre SRM, andre sentrale aktører i ordningen og sektoren de representerer. Dette kan igjen redusere eventuelle forventningsgap og tydeliggjøre rollen de har overfor virksomhetene i sektoren og øvrige nøkkelaktører.

Som det fremkommer av utfordringsbildet er det også variasjoner i hvordan ulike SRM har tilnærmet seg og tolket føringer i rammeverket for håndtering av IKT-sikkerhetshendelser. Det er i svært varierende grad 1) operasjonalisert og 2) implementert som integrert, styrende dokument. Minimumskrav knyttet til for eksempel noen nøkkelfunksjoner og dekningsgrad i sektoren vil etter vår vurdering gi tydelighet rundt hva som faktisk skal dekkes av et SRM, både overfor virksomhetene i sektoren, de øvrige SRM og for NSM.

Et sett med minimumskrav vil sikre at et miljø må oppfylle en viss funksjon i tråd med ordningens formål før det får status som sektorvis responsmiljø. SRM bør fortsatt stå fritt til å utvide tjenestetilbudet utover dette, i tråd med sektorens behov.

Det kan være hensiktsmessig å knytte minimumskravene til bredden av tjenestekategorier, herunder deteksjon, hendelseshåndtering, sårbarhetshåndtering, situasjonsforståelse og kunnskapsdeling (se prinsipp 1).

Minimumskravene som settes bør følges av tilstrekkelig finansiering for å innfri kravene i de tilfeller der SRM ikke er finansiert over statsbudsjettet.

Prinsipp 5: De ulike aktørenes rolle i hendelseshåndteringen bør nyanseres og tydeliggjøres

I rammeverket bør det fremkomme tydelig i hvilke tilfeller de ulike aktørene (NSM, SRM og virksomheter) skal bidra i hendelseshåndteringen, med hvilken kapasitet og på hvilken måte. Slik kan man redusere variasjonen av forventninger til de ulike aktørene og gi økt forutsigbarhet for samarbeidspartnere og virksomheter. Det vil også tydeliggjøre overfor virksomhetene hva de selv forventes å håndtere. En omforent modell for samhandling som inkluderer en tydelig beskrivelse av oppgaver og ansvar vil kunne bidra til tydeliggjøring av rollene.

Observasjoner gjennom arbeidet med denne rapporten har vist at private aktørers rolle, enten som SRM eller annen part involvert i IKT-hendelser varierer, og i liten grad er formalisert. Det foreligger ikke en avtalemodell som formaliserer samarbeidet mellom de ulike SMR og øvrige parter. Hvilken rolle private aktører skal ha i de ulike samarbeidsstrukturene bør formaliseres og inkluderingen av disse bør baseres på noen fastsatte kriterier. Dette bør være basert på GNF-prosessen og i hvilken grad en virksomhet er av vesentlig eller avgjørende betydning. For aktører som leverer sikkerhetstjenester innen områdene deteksjon og hendelseshåndtering bør deltagelse knyttes til om de leverer sikkerhetstjenester til virksomheter som er avgjørende for grunnleggende nasjonale funksjoner.

4 Videreutvikling av ordningen med SRM

Kapittel 4.1. beskriver KPMGs forslag til videreutvikling av ordningen med sektorvise responsmiljøer.

Kapittel 4.2. vurderer de administrative og økonomiske konsekvensene av foreslått modell (alternativ 1). For å vurdere de administrative konsekvensene har det også blitt gjennomført tilsvarende vurderinger for to andre alternativer:

- ✓ Alternativ 0 (fortsette som i dag, fortsatt mangelfull implementering av rammeverket for håndtering av IKT-sikkerhetshendelser)
- ✓ Alternativ 0+ (implementere føringer i Rammeverk for håndtering av IKT-sikkerhetshendelser, herunder at departementene utpeker SRM i de sektorene der det ikke er SRM per i dag)

Modellene med tilhørende antatte administrative og økonomiske konsekvenser er nærmere beskrevet i kapittel 4.2.

4.1 Forslag til videreutvikling av ordningen med SRM

Formålet med forslagene til videreutvikling av dagens ordning med sektorvise responsmiljøer er å nyansere ordningen og gjøre den mer behovstilpasset. Dette innebærer å bevege seg fra at det stilles like krav til alle sektorer og SRM, til å tillate ulike løsninger basert på om det er behov for en sektorspesifikk funksjon.

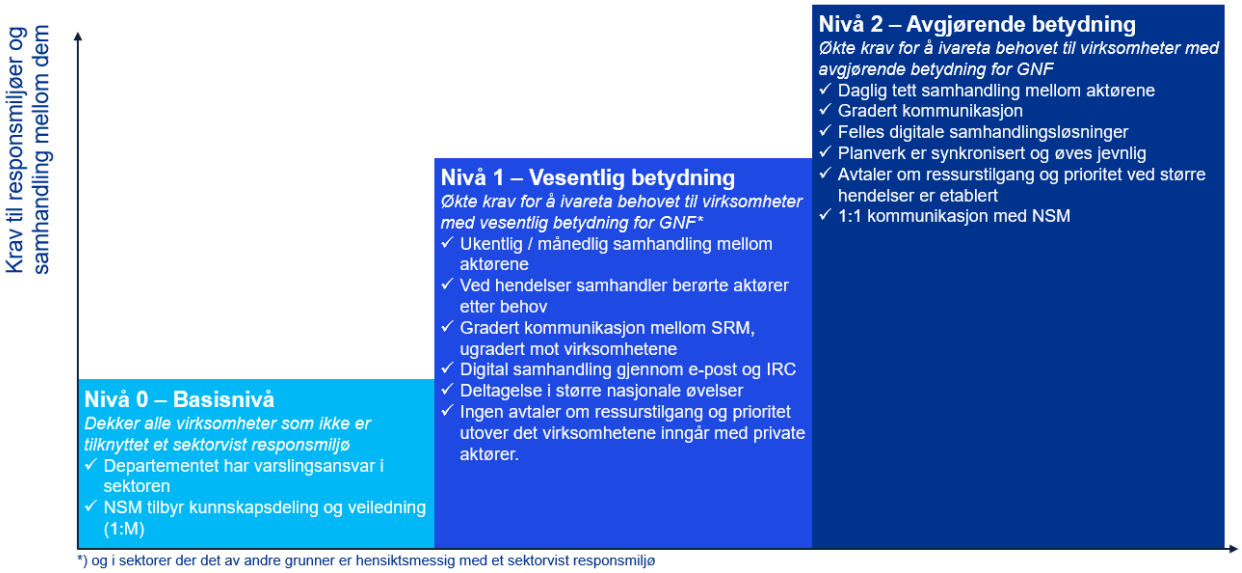
Det anbefales å stille ulike nivå av krav til responsmiljøene og samhandlingen mellom dem og sikkerhetsmyndigheten basert på følgende:

- ✓ hvor kritisk tilhørende virksomheter er for den nasjonale sikkerheten, og følgelig
- ✓ hvor omfattende konsekvenser en IKT-sikkerhetshendelse i disse virksomhetene vil få

Ettersom det pågår et arbeid i departementene med å identifisere grunnleggende nasjonale funksjoner og virksomheter som har vesentlig eller avgjørende betydning for disse, anbefales det å knytte nivåene i SRM-ordningen til dette arbeidet. Det foreslås en tre-nivå modell der samhandlingsnivået og minimumskravene øker med virksomhetenes betydning for grunnleggende nasjonale funksjoner. Det er viktig å påpeke at forslaget om minimumskrav utgjør et minimumsnivå, og at et SRM står fritt til å tilby ytterligere tjenester til sektoren der man vurderer dette som hensiktsmessig.

I tillegg anbefales det at det stilles noen basiskrav som gjelder uavhengig av tilknytning til SRM. Dette gjelder ivaretagelse av varsling i hele sektoren, samt generell kunnskapsdeling og tilgang til veiledere og kvalitetsordning for hendelseshåndtering fra NSM.

Figuren under illustrerer de tre ulike nivåene i forslaget til videreutvikling av modellen.



Figur 1 Anbefalt nivåinndeling for krav til responsmiljøer og samhandlingen mellom dem

Nivå 0 – Basisnivå

Formålet med basisnivået er å sikre at varsling innenfor alle sektorer blir ivaretatt, og at alle virksomheter har tilgang til generell kunnskapsdeling i form av veiledere og annen generell rådgivning via NSM.

Dette nivået er et minimumsnivå som gjelder for alle sektorer, og bør dekke alle virksomheter uavhengig av tilknytning til sektorvist responsmiljø. Dette innebærer blant annet at departementene har varslingsansvar i hele sektoren og til NSM. For de sektorene der det ikke er opprettet et SRM må varslingsansvaret ivaretas av departementet (eller delegeres til en annen aktør). Generell kunnskapsdeling og veiledning som er relevant for virksomhetenes håndtering av IKT-sikkerhetshendelser bør tilbys fra NSM i en én-til-mange-modell (1:M).

Minimumskravet om å utgjøre et kontaktpunkt i sektoren er i tråd med tiltak 38 i nasjonal strategi for digital sikkerhet.[7]

For alle virksomheter som ikke har naturlig tilknytning til sektor eller er i en sektor uten SRM, bør det vurderes hvorvidt det er behov for å danne en fellesfunksjon, for eksempel i NSM, som skal ha som oppgave å bistå denne gruppen virksomheter med informasjonsdeling, sårbarhetsvurderinger og lignende.

Nivå 1 – Vesentlig betydning

Formålet med nivå 1 er å sikre sektorspesifikk kompetanse i forbyggende og operativ IKT-sikkerhet i sektorer med virksomheter som har vesentlig betydning for GNF eller av andre grunner har behov for sektorspesifikk kompetanse og koordinering.

For sektorer der det er vurdert hensiktsmessig, skal det utpekes et SRM av departementet. Disse skal oppfylle et sett med minimumskrav for dette nivået. For å sikre at SRM har nok kapasitet og kompetanse til å ivareta minimumskravene kan ulike departementer velge å samarbeide om en funksjon, spesielt i sektorer med begrenset rolle i samfunnskritiske funksjoner.

SRM har ansvar for samarbeid og koordinering innenfor sektoren og mot andre sektorer for å ivareta sektorspesifikke behov. Det kan være behov knyttet til for eksempel medisinsk teknisk utstyr innen helse eller 5G innen Ekom. SRM skal formidle sektorspesifikk informasjon til NSM, og berike generell

[7] «Som en minimumsløsning skal det etableres et kontaktpunkt i sektoren for alvorlige IKT-hendelser og prosedyrer for varsling internt i sektoren og opp mot NSM NorCERT. Utover dette må sektorene selv vurdere hva slags behov de har for å håndtere alvorlige IKT-hendelser og hvordan de eventuelt skal skalere opp sine responsmiljøer»

informasjon fra NSM til virksomhetene i sektoren. SRM ivaretar også behovet for koordinering, informasjonsdeling og samarbeid mellom virksomhetene i sektoren. SRM koordinerer og deler informasjon innenfor sektoren og er bindeledd til/fra NSM. De sørger for at sektoren er oppdatert og at NSM er oppdatert på sektorens situasjon.

SRM samarbeider med hverandre og NSM i SRM-forum fasilitert av NSM. Virksomhetene har tilgang til en-til-mange dialog med NSM gjennom sårbarhetsvarsling, generell situasjonsforståelse, veiledere og kunnskapsdeling.

Virksomhetene er selv ansvarlig for deteksjon og hendelseshåndtering, og dette må ivaretas av virksomheten selv eller ved kjøp av kapabilitetene som en tjeneste. SRM er ikke direkte involvert i deteksjon med mindre SRM og sektoren/virksomheten spesifikt avtaler det og dermed ønsker å utvide tjenester utover minimumsnivået i modellen, slik som operativ eller rådgivende støtte i hendelseshåndtering. Behovet for dette står SRM fritt til selv å vurdere i samråd med virksomhetene i sektoren.
Ved håndtering av hendelser kan SRM bistå virksomheten med å formidle informasjon fra/til NSM, og eksempelvis via deling av tekniske indikatorer eller annen informasjon som kan støtte virksomheten i håndtering av hendelsen. NSM er ikke direkte involvert i hendelseshåndtering, med mindre hendelsen kan ramme kritisk infrastruktur og/eller kritiske samfunnsfunksjoner.

SRM er ansvarlig for å varsle alle virksomheter sektoren, uavhengig av hvordan SRM er organisert.

Nivå 2 – Avgjørende betydning

Formålet med nivå 2 er å styrke det forebyggende og operative samarbeidet på tvers av sektorer for å sikre samfunnets viktigste funksjoner.

Offentlige og private virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner bør inngå i en slik samarbeidsstruktur sammen med NSM og tilhørende SRM der det er tett samhandling mellom aktørene. Ved hendelser av en viss kritikalitet samarbeider aktørene tett på alle områder i hendelseshåndteringen. På dette nivået bør det tilrettelegges for at de samhandlende partene (både SRM og virksomhetene) har tilgang til gradert samhandlingsplattform. Virksomhetene har tilgang til 1:1 dialog med NSM ved behov.

SRM som inngår i dette samarbeidet bør oppfylle noen ytterligere krav i tillegg til nivå 1- og nivå 0 -kravene. Det er hensikten at et SRM skal dekke hele sin sektor, uavhengig av hvilket nivå av krav de oppfyller – men at de på nivå 2 i tillegg skal være i stand til å kunne imøtekomme behovene til virksomheter som har avgjørende betydning for GNF. På dette nivået vil enkelte områder dekkes av sikkerhetsloven. Virksomheter med avgjørende betydning for GNF er underlagt sikkerhetsloven, og dermed eksempelvis pålagt varslingsplikt.

Dette nivået vil være naturlig begrenset i antall SRM og virksomheter, hvilket gjør at man kan opprettholde et høyt tillitsnivå.

NSM, SRM og virksomhetene som inngår i dette samarbeidet bør etablere en samarbeidsavtale som muliggjør deling av informasjon, kapasitet, ressurser ved behov, uten at avtalepartene er forpliktet til å gi fra seg ressurser. Deling av persondata bør reguleres i avtalen slik at det er mulig å dele eksempelvis loggdata ved hendelser.

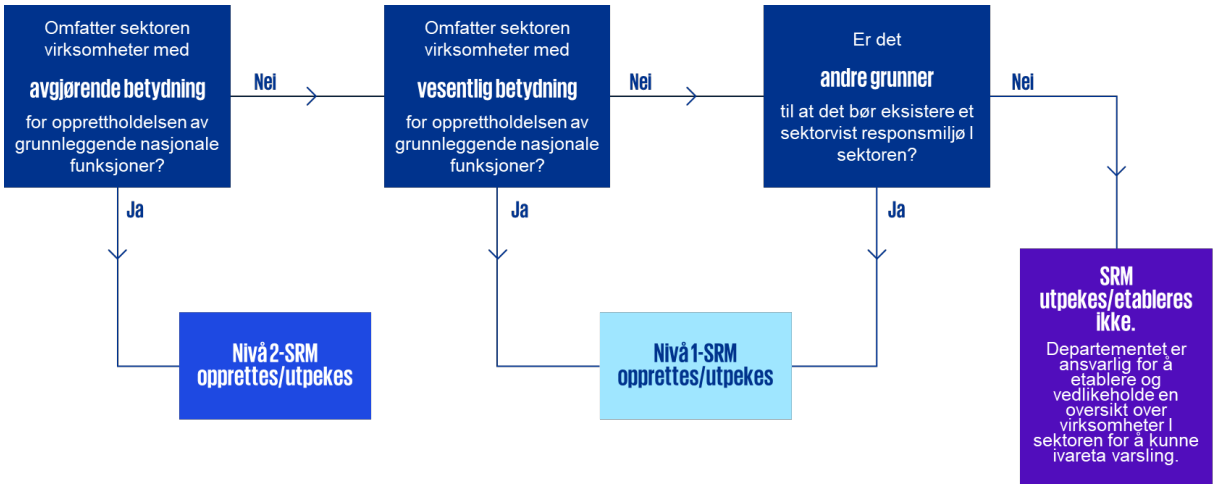
4.1.1 Utpeking av SRM

Hvert departement er ansvarlig for å vurdere hvorvidt sektoren har virksomheter som har vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. KPMGs forslag er å benytte denne prosessen som utgangspunkt for vurdering av eventuelt behov for SRM. I tillegg til at departementene er ansvarlige for vurderingen i sin sektor, anbefaler vi at NSM har en rådgivende funksjon i vurderingen for å sikre en helhetlig oversikt over behovene.

For de sektorene som har virksomheter med avgjørende betydning, utpeker departementet et SRM på nivå 2.

Dersom sektoren ikke har virksomheter med avgjørende betydning for GNF, men har virksomheter med vesentlig betydning eller vurderer at det ellers eksisterer behov for et eget SRM, utpeker departement et SRM på nivå 1.

Dersom departement ikke identifiserer noen virksomheter med avgjørende eller vesentlig betydning, og heller ikke vurderer andre behov for et SRM, kan departement velge å ikke utpeke SRM. I dette tilfellet er departement ansvarlig for å etablere og vedlikeholde en oversikt over virksomheter i sektoren for å kunne ivareta varsling av virksomhetene.



Figur 2 Prosess for utpeking av SRM

Ved behov kan det etableres et felles SRM for sektorene som ikke har behov for og/eller ressurser til et fullverdig SRM alene i sin sektor. Dette «felles-SRM» kan etableres under departementene eller NSM. Hva som er mest hensiktsmessig vil kreve en grundigere vurdering/utredning. Hensikten med anbefalingen er å samle kompetanse og ressurser i store nok fagmiljøer, slik at SRM som minimum har kapasitet til å utføre oppgavene i henhold til de minimumskrav som stilles. Størrelsen på fagmiljøene er også nevnt av SRM som mulig virkemiddel for å ansette og beholde ressurser med riktig kompetanse; i større fagmiljøer er det mulig å sikre faglig utfordrende oppgaver, faglig utvikling og økte muligheter for sparring med kollegaer.

4.1.2 Videreutvikling av rammeverket

En videreutviklet versjon av rammeverket for håndtering av IKT-sikkerhet bør gi et mer helhetlig svar på de utfordringer man står oppe i hva gjelder cybersikkerhet enn det dagens rammeverk gir. Det foreslås å erstatte dagens rammeverk med en «Nasjonal samhandlingsmodell for cybersikkerhet». Formålet med modellen er å tilrettelegge for god tverrsektoriell samhandling. Modellen bør beskrive de ulike aktørenes roller, ansvar og oppgaver. Den bør også beskrive de ulike samhandlingsnivåene, tilhørende kriterier for å inngå i de ulike og kravene som følger av dette.

Det anbefales videre å bytte navn på ordningen fra «sektorvise responsmiljø» til «sektorvis cybersikkerhetssenter». Dette er for at navnet i større grad skal reflektere bredden av tjenester som dagens miljøer leverer, som inkluderer forebyggende oppgaver. Dette innebærer ikke at navnene på dagens etablerte miljøer må endres.

4.1.3 Forutsetninger for en vellykket gjennomføring

I dette avsnittet diskuterer vi forutsetninger for en vellykket gjennomføring. Den helt sentrale forutsetningen for å sikre en vellykket gjennomføring av foreslått modell er å sikre forankring blant de sentrale aktørene som inngår i modellen.

Etter KPMGs vurdering er det særlig avgjørende at forankringen starter i departementsfellesskapet. Særlig viktig er en tett og god dialog mellom JD (sivil sektor) og FD (forsvarssektoren). Som ansvarlig departement på området er det også av kritisk betydning at JD legger til rette for å involvere andre berørte departementer på et tidlig tidspunkt. Det vil også være viktig at ansvaret for gjennomføring tydelig plasseres med nødvendige ressurser og løpende rapportering til JD.

Viktige forutsetninger ved implementering av modellen er en erkjennelse av et trussel- og sårbarhetsbilde i stadig endring og at modellen jevnlig må evalueres og forbedres.

Dernest er det vesentlig å sikre tilstrekkelig involvering av øvrige, berørte aktører. Av Rammeverk for håndtering av IKT-sikkerhetshendelser fremgår at dette er særlig aktuelt for følgende aktører[8]:

- ✓ NSM (herunder FCKS)
- ✓ Politiet (herunder Kripos, PST)
- ✓ Etterretningstjenesten
- ✓ Nasjonal kommunikasjonsmyndighet
- ✓ (Regjeringens kriseråd)
- ✓ SRM
- ✓ CERT og CSIRT-miljøer som ikke har status som SRM
- ✓ Andre myndigheter og etater

I tillegg skal SRM-ordningen først og fremst betjene de virksomheter som inngår i det enkelte SRMs dekningsområde. Som det fremgår av rapporten er behovene for støtte fra SRM-miljøer sterkt varierende mellom sektorer og virksomheter, det samme gjelder tilbudet fra det enkelte SRM. På bakgrunn av dette oppfatter KPMG behov for medvirkning fra virksomhetene som betjenes av SRM for å lykkes med å gjennomføre foreslått modell. Under redegjør vi for vår tenkning knyttet til tidsbruk for gjennomføring av foreslått modell:

- ✓ Ettersom foreslåtte modell vil ha budsjettmessige implikasjoner ut over dagens tilstand (se kapittel 4.2) mener vi at det, basert på erfaring, er rimelig å anta at det vil medgå omtrent ett år på å sikre finansiering.
- ✓ En involveringsprosess som skissert ovenfor vil av erfaring kunne ta inntil ett år, litt avhengig av om det er ønskelig å avgrense involveringsprosessen til departementsfellesskapet og de mest sentrale myndighetsaktørene eller også å inkludere virksomhetene i bred forstand.
- ✓ Et nøkternt anslag med en middels ambisiøs involvering av berørte parter tilsier følgelig en tidshorisont for gjennomføring på to til tre år. Foreslått modell bør følgelig være mulig å gjennomføre fullstendig senest innen 1. juli 2025.

[8] Listen bør oppdateres for å gjenspeile aktørlandskapet slik det er i dag

4.2 Vurdering av administrative og økonomiske konsekvenser

SSBs lønnsstatistikk har vært sentral for våre beregninger. I henhold til statistikken hadde lønnsmottakere i yrke 2529 «Sikkerhetsanalytikere» 67 010 kr i gjennomsnittlig månedslønn i 2021[9]. I beregningene nedenfor er det tatt utgangspunkt i disse lønnskostnadene som tilsvarer en årslønn på om lag 804 000 kroner. Kostnaden for et årsverk er beregnet basert på årslønn pluss 30 % til dekning av arbeidsgiveravgift og andre fastsatte kostnader knyttet til den enkelte ansatte; totalt 1 045 200 per årsverk.

Det er i tillegg lagt til kostnader på 15 000 kr for klient på gradert nett der det vil være aktuelt (gjelder primært ansatte i SRM og virksomheter med avgjørende betydning for GNF på nivå 2 i foreslått modell/alternativ 1). Ettersom det vil tilkomme ekstra kostnader til safer og annen infrastruktur for å håndtere gradert utstyr og informasjon er det lagt til en skjønnsmessig fastsatt kostnad på 10 000 kr per årsverk i tillegg for dekke denne typen kostnader.

Det hefter stor usikkerhet ved beregningene, noe som er illustrert ved det relativt brede kostnadsestimatet. Den største kostnadsdriveren i alternativ 0+ og alternativ 1 vil være knyttet til opprettelsen av nye SRM. Kostnaden vil trolig være mindre ved valg av alternativ 1 enn alternativ 0+ som følge av at en del SRM antakelig ikke blir etablert innenfor rammene av foreslått modell.

4.2.1 Alternativ 0: videreføring av dagens ordning

Til nullalternativet vil det ikke knytte seg økonomiske og administrative konsekvenser ut over dagens situasjon. Alternativet forutsetter at dagens situasjon videreføres. Det vil si at rammeverket for håndtering av IKT-sikkerhetshendelser fortsatt ikke er fullt implementert, herunder at nye SRM ikke utpekes. Dette alternativet er ikke ønskelig med henblikk på å håndtere identifiserte utfordringer (se kapittel 3). Samtidig foreligger det, innen dette alternativet, ikke formelle hindre som umuliggjør nye løsninger for økt og bedre samhandling/deling mellom de ulike SRM og NSM enn dagens situasjon.

KPMG tilrår ikke at dagens situasjon videreføres gitt utfordringene som er beskrevet i kapittel 3.

4.2.2 Alternativ 0+: full implementering av rammeverket

I alternativ 0+ implementeres rammeverket fullstendig slik som det er beskrevet i dag. Viktigst innebærer en full implementering av rammeverket at departementene peker ut SRM i de tilfeller der det ikke er gjort per i dag. KPMG har ikke totaloversikten over hvor mange SRM dette innebærer, men basert på vår kjennskap til sektorer med manglende dekning av SRM kan det være aktuelt å etablere 5-15 nye SRM i tiden fremover. Det typiske SRM har 5-10 årsverk. Ut fra dette vil full implementering av rammeverket innebære følgende mulige økonomiske og administrative konsekvenser:

- ✓ Et sted mellom 25 og 150 nye årsverk i nye SRM (basert på en antakelse om at det vil etableres 10-15 SRM med 5-10 medarbeidere) vil innebære økonomiske konsekvenser i størrelsesordenen fra om lag 52 millioner kroner til 157 millioner kroner.
- ✓ Det er sannsynlig at det, i tillegg til de økonomiske konsekvensene som følger av etableringen av nye SRM, også vil tilkomme kostnader knyttet til økt kapasitetsbehov i NSM for å ivareta nettverket og betjene et større antall SRM. Disse kostnadene er anslått til størrelsesordenen 5-10 millioner kroner.
- ✓ Totalt vil de økonomiske konsekvensene beløpe seg til et sted mellom 57 millioner og 167 millioner kroner ved alternativ 0+.

[9] Ifølge statistikkbankens kildetabell 11418

- ✓ Blant de administrative konsekvensene er det verdt å merke seg at utfordringen knyttet til antallet deltakere i møter og samarbeidsfora vil bli forsterkede.
- ✓ Tendensen til at ressursinnsatsen er for fragmentert i for mange enheter vil tilta.

KPMG anbefaler ikke at dagens rammeverk implementeres fullt ut som følge av at flere opplevde utfordringer med dagens situasjon vil videreføres og forsterkes ved full implementering av det eksisterende rammeverket.

4.2.3 Alternativ 1: KPMGs forslag

Forslaget som beskrevet i kapittel 4.1 innebærer følgende sentrale endringer av dagens ordning:

- ✓ Kravet om at hvert departement må peke ut et SRM erstattes med et minimumskrav til varslingsansvar som kan håndteres av departementet i de tilfeller der det ikke er vurdert hensiktsmessig med et SRM. I noen tilfeller kan dette medføre at SRM ikke blir etablert, men at departementet selv forvalter en kontaktliste for å sikre varsling av virksomheter i egen sektor. Dette vil kunne medføre noe økt arbeidsmengde i enkelte departementer (et sted mellom 0,2 og 0,5 årsverk per departement) som velger denne løsningen.
- ✓ Det etableres to nivåer for samarbeid for SRM, sektornivå og nasjonalt nivå. SRM med tilhørende virksomheter som har avgjørende betydning for GNF, vil få kostnader for klienter og annet utstyr for å få tilgang til gradert samhandling som SRM ikke har i dag.
- ✓ Foreslått modell vil ikke hindre departementene i å utpeke SRM i de tilfeller der det vurderes som en hensiktsmessig løsning. Således vil kostnadsbildet være sammenliknbar med 0+ alternativet selv om det er rimelig grunn til å anta at initiativer til å etablere små SRM med 1-2 ansatte vil blir bremset med dette forslaget.

De viktigste økonomiske og administrative konsekvensene av alternativ 1 følger:

- ✓ For SRM med virksomheter som har avgjørende betydning for GNF, samt disse virksomhetene, vil det påløpe kostnader knyttet til tilgang til gradert plattform. Kostnadene for gradert samhandling anslås til 25.000 kroner per årsverk, inkludert kostnader knyttet til utstyr for å håndtere gradert informasjon er skjønnsmessig fastsatt[10].
  - Vår foreløpige vurdering er at SRM i nivå 2 vil inkludere 6-8 SRM i dagens ordning.
  - For aktuelle SRM i disse sektorene vil tilgang til gradert samhandling innebære en kostnad på om lag 750 000 – 2 000 000 kroner[11].
- ✓ Som følge av at foreslått modell ikke endrer muligheten til å peke ut nye SRM vil det også innen rammene av modellen tilkomme nye SRM. Det er imidlertid vår vurdering at de minste, SRM ikke vil bli etablert og/eller håndtert av ansvarlig departement. Det antas at dette vil medføre noe lavere økonomiske konsekvenser enn 0+ alternativet (etablering av 4-8 nye SRM med 5-10 ansatte). De økonomiske konsekvensene av nye SRM vil dermed være i størrelsesordenen om lag 21 millioner kroner til 84 millioner kroner.
- ✓ I tillegg vil de departementer som ikke utpeker SRM selv måtte ajourføre varslingsliste og eventuelt varsle virksomheter i sin sektor ved hendelser. Dette anses å være en relativt avgrenset arbeidsoppgave som bør kunne løses innenfor rammen av inntil 0,2 årsverk per departement. Det antas at inntil 10 departementer vil kunne ha behov for å ivareta slike lister for deler av sektoren som ikke er dekket av et SRM, eller for hele sektoren der det eventuelt vurderes som unødvendig med et SRM. Anslåtte kostnader blir dermed mellom 0 og 2 millioner kroner.
- ✓ Behovet for styrking av NSM vurderes likt som i alternativ 0+ og settes til 5-10 millioner kroner.

[10] Dersom virksomheten allerede har tilgang til NBN trenger de ikke å få det på nytt. KPMG er ikke kjent med omfanget av slike tilfeller og det er derfor ikke hensyntatt i våre overslag.

[11] Ansatte i forsvaret har allerede tilgang til gradert samhandling og er ikke hensyntatt i regnestykket.

- ✓ De totale økonomiske konsekvensene av alternativ 1 er dermed innenfor spennet 27 millioner kroner og 98 millioner kroner. Anslåtte, maksimale økonomiske konsekvenser er dermed noe lavere enn for alternativ 0+.
- ✓ Alternativ 1 vil medføre en økt ressursinnsats, muligheter for deling og økt samhandling mellom utpekte SRM på nivå 2. Samtidig er det rimelig å anta at det vil utpekes færre SRM i sektorer med avgrenset behov for responsmiljøer og at en derigjennom kan begrense ressursbruken på små SRM og samtidig oppnå en mer hensiktsmessig ressursbruk med større fagmiljøer som har større dekningsområde.

Vedlegg

Appendix 1 FIRST CSIRT Services Framework v2.1

I rapporten henvises til rammeverket «FIRST CISRT Services Framework v2.1».

First (Forum of Incident Response and Security Teams) er en global anerkjent organisasjon, og ledende innen hendelsesrespons. FIRST tilrettelegger for at responsmiljø responderer mer effektivt på sikkerhetstruende hendelser og effektivt oppdager og håndterer kritiske sårbarheter. Organisasjonen er et forum for klarerte responsmiljøer og stiller tydelige krav til medlemsorganisasjonene. Sammen utvikler og deler FIRST teknisk informasjon, verktøy, metodikk, prosesser og beste praksis.

«CSIRT Services Framework» er et rammeverk som på en strukturert måte beskriver de funksjoner og tjenester som ofte ivaretas og leveres av operative IKT-sikkerhetsfunksjoner (CSIRT, SOC eller CERT). Rammeverket er utarbeidet av anerkjente eksperter fra sikkerhetsbransjen (tilknyttet FIRST), med støtte fra Task Force CSIRT (TF-CSIRT) og International Telecommunications Union (ITU).

Formålet med rammeverket er å støtte arbeidet med etablering og videreutvikling av operative IKT-sikkerhetsfunksjoner, med spesielt fokus på innledende fase der det arbeides med valg, utvidelse og styrking av tjenesteporteføljen. Tjenestene som beskrives er i all hovedsak alle de tjenestene som en operativ IKT-sikkerhetsfunksjon kan levere. En operativ IKT-sikkerhetsfunksjoner er ikke forventet å levere alle tjenestene i rammeverket, men enhver CSIRT, SOC eller CERT velger de tjenestene som best understøtter måloppnåelse sett i lys av eget oppdrag og egne forutsetninger.

Tjenestene i rammeverket skal bidra til å forebygge, detektere, håndtere IKT-sikkerhetshendelser og sårbarheter. Tjenestekategoriene er som følger:

- ✓ Deteksjon
- ✓ Hendelseshåndtering
- ✓ Sårbarhetshåndtering
- ✓ Situasjonsforståelse
- ✓ Kunnskapsdeling

Disse tjenestekategoriene inneholder videre et sett med tjenester som illustrert i figur X[12]:

Figur 3 Illustrasjon av tjenestene i FIRST CSIRT Services Framework

[12] KPMG gjør oppmerksom på at de norske benevningene i figuren er oversatt av KPMG og ikke verifisert av FIRST.

Appendix 2 Intervjuoversikt

Dato	Organisasjon	Deltakere
24.5.2022	Nettverk for digital sikkerhet	Bjørn Astad, Trine-Lise Waldorff, Katarina de Brisis, Gard Kjølholdt, Mia Thore Ronde Harlyng, Torill A. Østrem Tørlen, Gustav Birkeland, Lasse Gråberg, Aino von Düring, Jarl-Andre Skarsten, Hilde Goutal Müller, Ola Berge, Kristine Wennberg, Kenneth Jacobsen
24.5.2022	MiljøCERT	Ågot Marianne Stornes
24.5.2022	NFCERT	Morten Tandle
30.5.2022	KraftCERT	Margrete Raaum, Martin Bore
30.5.2022	Kommune-CSIRT	Bjørn Tveiten
31.5.2022	HelseCERT	Gunnar A. Johansen
01.06.2022	JustisCERT	Berit Schmidt, Oddvar Kaaby, Stian Kristoffersen
03.06.2022	CSS	Cecilie Østlund Hammer
17.06.2022	Equinor, Hydro	Lars Idland, Torstein Gimnes Are
20.06.2022	NSM, NVE	Harald Kristian Næss, Janne Merete Hagen
20.06.2022	NSM	Øivind Mandt, Svenn Richard Andersen
21.06.2022	NSM	Svenn Richard Andersen, August Verholdt
22.06.2022	SRM	Morten Tandle, Bjørn Tveiten, Mike Andersen, Margrete Raaum, Berit Schmidt, Frank Stien, Cecilie Østlund Hammer, Oddvar Kaaby, Rune Sydskjør, Gunnar A. Johansen
21.06.2022	NSM	Truls Campe Pettersen, Mari Kvaal
21.06.2022	Justisråd ved EU-delegasjonen	Josefine Aaser
22.06.2022	Den norske ambassaden i Washington DC.	Samfunnssikkerhetsråd Per Kristen Brekke

Appendix 3 Om NIS 2 -direktivet

Formålet med NIS 2 -direktivet er å styrke motstandsdyktighet gjennom effektivt samarbeid mellom myndighetene i medlemsstatene. Forslaget til nytt direktiv øker dekningsområdet sammenlignet med det nåværende direktivet ved å utvide antall sektorer som defineres som kritiske. Direktivet vil skille mellom to kritikalitetsnivåer, «vesentlig» og «viktig». Sektorer som i forslaget defineres som «vesentlig» er for eksempel energi, transport, bank, finansmarkedsinfrastrukturer, helse, drikkevann, avløpsvann, digital infrastruktur, offentlig forvaltning og romvirksomhet[13].

Forslaget for videreutvikling av ordningen med sektorvise responsmiljøer i denne rapporten er knyttet til prosessen å definere grunnleggende nasjonale funksjoner. Utvalget av «vesentlige» sektorer i forslaget til NIS 2 -direktiv er noe bredere enn identifiserte GNF på tidspunkt denne rapporten ble skrevet. Det viktigste i forholdet mellom NIS 2 -direktivet og ordningen med sektorvise responsmiljøer blir å avgjøre forholdet mellom NIS 2 -direktivet og identifiserte GNF, og vurdere om sektorer som defineres som «vesentlig» i NIS 2 -direktivet vil resultere i flere GNF og dermed flere virksomheter som har avgjørende betydning for GNF. Samtidig vil NIS 2 -direktivet innføre avgrensninger mot mindre virksomheter slik at det kun vil være større virksomheter som blir underlagt NIS 2 -direktivet. Dermed kan det antas at antall virksomheter som i forslaget i denne rapporten inkluderes i Nivå 2 Avgjørende, ikke nødvendigvis øker betydelig som følge av NIS 2 -direktivet.

[13] NIS2 - direktivet - regjeringen.no

Kontakt oss:

Hans Christian Pretorius
Partner
T +47 90879077
E **hans.christian.pretorius@kpmg.no**

kpmg.no

DET KONGELIGE
KOMMUNAL- OG DISTRIKTSDEPARTEMENT

Ifølge liste

Deres ref	Vår ref	Dato
	22/1621-5	20. februar 2023

Digitaliseringsbrev til kommuner og fylkeskommuner

Regjeringen ønsker en sterk og effektiv offentlig sektor som gir innbyggerne gode tjenester, valgfrihet og medbestemmelse. Alle innbyggere, uansett bosted, skal ha et godt tjenestetilbud i sitt nærmiljø. Digital infrastruktur blir avgjørende for å bygge landet videre i fremtiden. Regjeringen vil legge til rette for at folk kan bo der de vil, blant annet gjennom å sikre gode grunnleggende digitale tjenester for innbyggere og næringsliv.

Teksten nedenfor inneholder tema og tiltak som Kommunal- og distriktsdepartementet (KDD) finner særlig relevant for kommuner og fylkeskommuner å være kjent med i forbindelse med deres digitaliseringsarbeid.

Oppfølging av Én digital offentlig sektor – Digitaliseringsstrategien for offentlig sektor 2019-2025

Digitaliseringsstrategien for offentlig sektor (2019-2025) – Én digital offentlig sektor er felles for kommunesektoren og staten. Stat og kommune må samarbeide tett for å realisere målene i strategien. Oppfølging av tiltakene understøttes av felles handlingsplan for realisering av strategien, der Digitaliseringsdirektoratet og KS følger opp denne i felleskap. Regjeringen vil følge opp med tiltak som understøtter Hurdalsplattformens ambisjoner om et taktskifte i digitaliseringen av offentlig sektor.

Sentralt i strategien er utvikling av sammenhengende tjenester innenfor syv prioriterte livshendelser. Disse er Få barn (*AID*), Alvorlig sykt barn (*HOD*), Miste og finne jobb (*AID*), Ny i Norge (*AID*), Starte og drive bedrift (*NFD*), Starte og drive frivillig organisasjon (*KUD*) og Dødsfall og arv (KDD). Øverste ansvar for livshendelsene er lagt til departementene i parentes, som skal bidra til å realisere livshendelsene, involvere andre departementer og KS

Postadresse	Kontoradresse	Telefon*	Avdeling	Saksbehandler
Postboks 8112 Dep 0032 Oslo postmottak@kdd.dep.no	Akersg. 59 www.kdd.dep.no	22 24 90 90 Org.nr. 972 417 858	Avdeling for IT- og forvaltningspolitikk	Line Richardsen 22 24 72 36

og forankre arbeidet overfor involverte og for omverdenen. Status for arbeidet med de livshendelsene kan følges her: Prioriterte livshendelser | Digdir

KDD legger stor vekt på det tette samarbeidet med kommunal sektor. KS og KDD er i gang med å utarbeide ny samarbeidsavtale om digitalisering. Dagens samarbeidsavtale mellom KS og KDD om digitalisering gikk ut i september i 2022, men videreføres inntil ny avtale er på plass før sommeren 2023. Avtalen er en bilateral samarbeidsavtale under konsultasjonsordningen. Konsultasjonsordningen er den faste hovedarenaen for regjeringen og KS til dialog og samarbeid om makroøkonomiske forhold og enkeltsaker som er knyttet til det økonomiske opplegget for kommunesektoren i statsbudsjettet. Bilaterale samarbeidsavtaler er en del av virkemiddelapparatet og styringsdialogen mellom staten og kommunesektoren. Avtalene skal bidra til utvikling av kommunal og statlig tjenesteproduksjon, og kommunen som samfunns- og utviklingsaktør.

Digital hele livet – digital inkludering
Det vises til *strategi for økt digital deltakelse og kompetanse i befolkningen – Digital hele livet*. Regjeringen følger opp strategien gjennom en egen handlingsplan i starten av 2023. I 2022 har KDD tildelt åtte millioner kroner i engangsstøtte til 27 søkere i 45 kommuner som ønsker å heve den digitale kompetansen til innbyggerne. Tilskuddordningen understøtter regjeringens og KS felles ambisjon om å gi alle innbyggere mulighet til å delta i det digitale samfunnet. I samarbeid med KS er det etablert en rådgivningstjeneste som skal hjelpe kommuner som ønsker å utvikle eller videreutvikle veiledningstilbud i grunnleggende digital kompetanse for sine innbyggere (Digihjelpen). Her finner man tips og råd for etablering og utvikling av et kommunalt veiledningstilbud.

Universell utforming
Universell utforming av digitale løsninger, herunder nettsider, apper og digitale dokument, er en forutsetning for digital inkludering. Forskrift om universell utforming av ikt er utvidet med nye krav til nettsteder og apper i offentlig sektor, som følge av innlemmelse av EUs webdirektiv i norsk rett. Kravene gjelder fra 1. februar 2023. Fra samme tidspunkt skal også kommunenes, fylkeskommunenes og statlig sektors digitale løsninger som brukes for å tilby informasjon og tjenester over internett, ha publisert tilgjengelighetserklæringer som viser i hvilken grad løsningene er i samsvar med regelverket.

UU-tilsynet i Digitaliseringsdirektoratet har utviklet en sentral løsning for offentlig sektors tilgjengelighetserklæringer. Det er obligatorisk å ta løsningen i bruk. Tilgjengelighetserklæringen er rullet ut til virksomheter i kommunal, fylkeskommunal og statlig sektor fra oktober 2022. Tilsynet gir veiledning og hjelp ved utfyllingen av erklæringen.

For å sikre universelt utformede og inkluderende digitale løsninger anbefales det å:

- Ivareta kravene til universell utforming i utvikling og forvaltning av digitale løsninger gjennom hele livssyklusen

- Stille krav om universell utforming av ikt i anskaffelse av digitale løsninger, herunder også å be leverandører og andre bidragsytere om å dokumentere hvordan de ivaretar kravene til universell utforming i løsningene
- Digitalisere for mangfold, herunder også brukerteste digitale løsninger for å ivareta ulike brukerbehov, inkludert behovene til personer med fysiske og kognitive funksjonsnedsettelser, ulik alder, språkbakgrunn og digitale ferdigheter.

Informasjon om kravene til universell utforming og tilgjengelighetserklæringen, finnes på UU-tilsynets nettsider.

Informasjonssikkerhet
God informasjonssikkerhet er en forutsetning for vellykket digitalisering. Dette er også en grunnleggende forutsetning for å opprettholde tillit til offentlig sektors IT-systemer og offentlige digitale tjenester. En vellykket digitalisering handler derfor også om å ivareta krav til sikkerhet og den enkeltes personvern på en god måte. Det handler om å styre risiko i oppgavene og tjenestene.

Det er viktig at alle offentlige virksomheter arbeider godt med informasjonssikkerhet for å kunne levere effektive, brukervennlige og sikre tjenester til innbyggerne. eForvaltningsforskriften § 15 stiller krav om at alle offentlige virksomheter skal ha et styringssystem som beskriver hvordan virksomhetens aktiviteter innenfor sikkerhetsstyring planlegges, utføres, kontrolleres og forbedres. Dette styringssystemet for informasjonssikkerhet bør samordnes med virksomhetsstyringen for øvrig. Dette vil gi grunnlag for felles tilnærming i håndteringen av de risikoer virksomheten står overfor.

Digitaliseringsdirektoratet har i samarbeid med andre veiledningsaktører utarbeidet veiledningsmateriell som kan benyttes av kommunene for å lykkes med informasjonssikkerhetsarbeidet. Digitaliseringsdirektoratet tar også initiativ til et tverrsektorielt samarbeid mellom sentrale veiledningsaktører på området. Initiativet kalles «Felles sikkerhet i forvaltningen», og målsetningen er at det skal bli enklere for kommuner og statlige virksomheter å lykkes i arbeidet med informasjonssikkerhet. Arbeidet vil starte opp i 2023. En beskrivelse av initiativet, og hvilke muligheter og gevinster det kan gi, finnes i et notat publisert på Digdirs nettsider, Felles sikkerhet i forvaltningen | Digdir.

KS og Foreningen kommunal informasjonssikkerhet (KINS) vil være sentrale samarbeidspartnere for kommunene. Videre er nasjonale råd og anbefalinger, særlig NSMs grunnprinsipper og 10 nasjonale råd i Nasjonal strategi for digital sikkerhet, viktig for kommunene å benytte og følge opp. Vi anbefaler også å bruke øvingsportalen ovelse.no som er et gratistilbud til alle norske virksomheter.

Regjeringen ønsker at alle kommuner skal være tilknyttet et responsmiljø som kan støtte i forebygging og håndtering av IKT sikkerhetshendelser, og jobber for at alle kommuner skal kunne knytte seg til et sektorvis responsmiljø (SRM) for kommunesektoren. Kommunene oppfordres til å aktivt benytte de responsmiljøene de allerede er knyttet til, slik som

HelseCERT og de tjenestene som er tilgjengelige gjennom HelseCERTs Nasjonalt beskyttelsesprogram (NBP).

Departementet viser til at kommunene i henhold til forskrift om kommunal beredskapsplikt er pålagt å gjennomføre helhetlige risiko- og sårbarhetsanalyser for å ivareta befolkningens sikkerhet og trygghet. Vi minner om at kommunene som del av dette arbeidet også bør vurdere risiko og sårbarhet knyttet til infrastruktur og tjenester for elektronisk kommunikasjon (mobil- og bredbåndstjenester og datasenter).

Regulatorisk sandkasse for personvern og kunstig intelligens
For å stimulere til personvernvennlig innovasjon og digitalisering er det etablert en regulatorisk sandkasse hos Datatilsynet. Her kan aktører i både privat og offentlig sektor få praktiske råd og veiledning om hvordan de kan bruke personopplysninger på innovative måter og i nye digitale tjenester innenfor rammene av personvernregelverket. Kommuner som ønsker praktisk veiledning i personvernvennlig digitalisering kan søke opptak i den regulatoriske sandkassen. Mer informasjon om arbeidet i sandkassen finnes på Sandkassesiden | Datatilsynet

Tilrettelegging for bredbånd og mobil – Ekomportalen
Mobil- og bredbåndsnettene binder Norge sammen og er nødvendige for digitalisering av offentlige tjenester, samt næringsutvikling og økt produktivitet i samfunnet. Kommunene har en viktig rolle for å legge til rette for utbygging av slik infrastruktur, blant annet som grunneier, planmyndighet og veimyndighet. Kommunene kan f.eks. bidra til mer effektiv utbygging gjennom å tillate utplassering av basestasjoner på offentlige bygg og ved ikke å stille for strenge krav til etablering av fiberkabel i og langs kommunal vei.

Bredbåndsutbyggingsloven, som trådte i kraft 1. juli 2020, skal bidra til billigere og mer effektiv bredbåndsutbygging. I forbindelse med loven har Nasjonal kommunikasjonsmyndighet (Nkom) etablert Ekomportalen: https://ekomportalen.nkom.no/. Ekomportalen skal bidra til økt bredbåndsutbygging i Norge ved å dele informasjon som er relevant for bransjen og andre interessenter. Kommunene vil være omfattet av definisjonen av nettoperatører, og har plikter etter loven til å levere informasjon til Ekomportalen. Kommuner som eier infrastruktur egnet til framføring av bredbånd, skal legge inn opplysninger om fysisk infrastruktur (for eksempel stolper og trekkerør) i Ekomportalen, samt oppdatere disse opplysningene innen to måneder etter eventuelle endringer i infrastruktur. Kommunene skal også registrere i portalen opplysninger om søknadspliktige bygge- og anleggsarbeider som de gjennomfører i egen regi, eksempelvis sanering av vann og avløp. Ved å gjøre denne informasjonen tilgjengelig, kan kommunene bidra til at samfunnet sparer ressurser f.eks. ved at unødvendig graving unngås og ved at det legges til rette for gjenbruk av infrastruktur. Kommunene kan på denne måten bidra til et mer bærekraftig samfunn. Nkom kan kontaktes dersom kommunene har spørsmål i tilknytning til dette.

Departementet vil også oppfordre kommunesektoren til å etablere effektive og enhetlige prosesser i forbindelse med søknader om innplassering av infrastruktur for mobilnett på

offentlige arealer, samt aktivt å legge til rette for videre utbygging av mobilkommunikasjonsnett. Vi viser i denne forbindelse til Nkoms veileder: Innplassering av infrastruktur for mobilnett på offentlige arealer - Nkom

Revidert datasenterstrategi og kommuneveileder
Datalagrings- og dataprosesseringsevne utgjør en sentral del av den digitale grunnmuren, og datasentre er viktige for å sikre en robust nasjonal infrastruktur over hele landet. Alle digitale tjenester kjøres fra datasentre i dag og mange datasentre leverer viktige tjenester for både digitalisering og effektivisering av offentlige tjenester og for ny teknologi- og databasert industri- og næringsutvikling. God tilgang på datasentre i Norge er en nødvendig forutsetning for å ha en god nasjonal datalagringsevne for hele samfunnet og regjeringen ønsker å legge til rette for datasenteretableringer i Norge. Samtidig står vi i en krevende kraftsituasjon nasjonalt og en utfordrende sikkerhetspolitisk situasjon i Europa. Det er også utfordringer knyttet til manglende lokale ringvirkninger og verdiskaping når det gjelder kryptoutvinning. Regjeringen er derfor i gang med å revidere og videreutvikle den nasjonale datasenterstrategien, og har som mål å legge frem en oppdatert strategi i løpet av våren. Regjeringen er også i sluttfasen av arbeidet med en veileder for kommunene i forbindelse med datasenteretableringer. Veilederen vil inneholde informasjon om hva kommunen bør tenke over ved henvendelser fra interessenter om å etablere datasenter, eller kommunen selv ønsker å etablere datasenter. Hensikten er å gjøre det enklere for kommunene å ta velbegrunnede valg når et datasenter ønsker å etablere seg i kommunen.

Kobo – system for kommunalt disponerte boliger
Husbanken har siden 2020 samarbeidet med KS og ca. 40 kommuner om å utvikle et digitalt system for kommunale utleieboliger. Systemet vil lette prosessen med å søke, tildele og administrere kommunale utleieboliger, følge opp beboere og skaffe datagrunnlag. Målet er at det skal bli enklere å søke kommunal bolig for de som trenger det. En boligsøker skal få lettere og raskere søknadsprosess, innsyn i egen sak, trygg behandling av personopplysninger, mer egnet bolig og bedre oppfølging. For kommunen skal det bli enklere å fatte vedtak, finne og tildele egnet bolig, sikre rett oppfølging og administrere leieforholdet. Med god oversikt over søkere, boliger og leietakere kan kommunen planlegge ut fra behov og utnytte boligmassen bedre. Det digitale systemet skal være et tilbud til alle norske kommuner. Seks pilotkommuner har brukt løsningen siden våren 2021 og løsningen åpnes nå gradvis for flere og flere kommuner. Etter planen skal alle norske kommuner som ønsker det få koble seg på i løpet av prosjektperioden som varer ut 2023. Seks pilotkommuner har brukt løsningen siden våren 2021, og i 2022 har Husbanken sammen med KS og utvalgte digitaliseringsnettverk tilpasset utrullingsmetodikken slik at alle norske kommuner som ønsker, kan få koble seg på i løpet av prosjektperioden som varer ut 2023.

Digital plan- og byggesaksbehandling
Direktoratet for Byggkvalitet (DiBk) har etablert Fellestjenester BYGG - en digital regelverksplattform på Altinn - som kontrollerer og sender inn byggesøknader til riktig kommune. Fellestjenester BYGG kommuniserer med FIKS-plattformen til KS. Dermed er det blitt enklere å levere komplette byggesøknader til kommunen. Fellestjenester BYGG sjekker

innsendte byggesøknader mot gjeldende regelverk, og sikrer informasjonsflyt mellom partene i byggesaken. De første nettbaserte søknadsløsningene kom på plass høsten 2018.

Over halvparten av de profesjonelle byggesøknadene sendes nå gjennom plattformen Fellestjenester BYGG og over 200 kommuner har anskaffet eByggesak som saksbehandlingssystem. Prosjektet eByggesak er eid av KS, og utvikles i samarbeid med DiBK, Kartverket, SSB, og en rekke pilotkommuner. Systemet innebærer at kommunene får byggesøknadene direkte inn i sitt saksbehandlingssystem med nødvendige data. Det reduserer arbeidsmengden knyttet til behandling og arkivering. Kommuner kan etter eForvaltningsforskriften bestemme at byggesøknader fra profesjonelle aktører må sendes inn gjennom digitale søknadsløsninger. Sandnes kommune har lenge praktisert stenging av søknader fra profesjonelle på epost. Det innebærer at profesjonelle aktører ikke lengre kan sende inn byggesøknader på e-post.

Digital plan- og byggesaksbehandling henger tett sammen og vi er i ferd med å få på plass flere selvbetjeningsløsninger også på planområdet. De nye tjenestene på planområdet utvikles rundt samme struktur som Fellestjenester BYGG og har fått betegnelsen Fellestjenester PLAN og BYGG.

KS utvikler også ePlanSak, som på sikt vil ivareta informasjonsflyten mellom aktørene i en plansak. ePlanSak er en produktspesifikasjon som kommunene kan benytte når de skal digitalisere planprosessen og anskaffe nytt fagsystem/sakstøtte for saksbehandling av planforslag fram til vedtak. eByggeSak og ePlanSak i samspill med nasjonale fellesløsninger, vil etter hvert sørge for mer standardiserte og effektive plan- og byggesaksprosesser.

For å få gode digitale plan- og byggesaksløsninger framover, er det viktig å ha oppdaterte digitale planregistre i bunnen. Det er avgjørende at kommunene fortløpende fører planregisteret etter Kart- og planforskriftens bestemmelser. Dette vil bli mer automatisert med bruk av ePlanSak og FIKS-plattformen til KS.

Digitalarkivet – fellesløsning for historiske arkiver og data
Arkivverket har etablert Digitalarkivet som fellesløsning for å sikre effektiv og trygg bevaring og tilgjengeliggjøring av samfunnets historiske arkiv og data. Kommuner, interkommunale arkivinstitusjoner, statlige virksomheter og private bevaringsinstitusjoner kan benytte løsningen, slik at arkivdata bevares og er mulig å finne og bruke – både for virksomhetene selv og innbyggerne.

Fellesløsningen utvikles i nært samarbeid med arkivsektoren, og har blitt testet og evaluert opp mot behov i kommunal sektor. Flere kommuner og interkommunale arkivinstitusjoner har inngått avtaler om bruk av Digitalarkivet for lovpålagte oppgaver for arkiv- og informasjonsforvaltning. Kommunene som knytter seg til Digitalarkivet vil ikke ha utgifter til utvikling av fellesløsningen.

Innebygd arkivering
Arkivverket vil hjelpe kommunene og statlig forvaltning til å lykkes med arkivering i en digital tid. Det er et stort behov for at man på en enklere og mer effektiv måte tar vare på dokumentasjonen som produseres og behandles. For å tilrettelegge for dette er særlig to tiltak relevante:

- I regulatorisk sandkasse for arkiv, data og offentlighet kan offentlige og private virksomheter utforske nye måter å ivareta arkivfaglige hensyn, inkludert måter som kan utfordre deler av regelverket. Flere prosjekter i kommunal sektor har vært med, og erfaringsrapporter er tilgjengelig for læring og inspirasjon (Tidligere prosjekter - Arkivverket). Arkivverket kan gi veiledning til kommunene på innovative prosjekter på området.
- I StandardLab identifiserer man behov for framtidas standardisering innenfor dokumentasjonsforvaltning og arkiv, og utvikler standarder gjennom involverende og behovsstyrte prosesser. Kommunal sektor er en viktig behovseier og interessent, og Arkivverket oppfordrer kommunene til å komme med innspill til arbeidet.

Digitalisering av gravferdsmeldingen
Statsforvalteren i Vestfold og Telemark arbeider med å digitalisere gravferdsmeldingen (begjæring om gravlegging/kremasjon). Digital gravferdsmelding skal sørge for en sikker digital informasjonsflyt mellom etterlatte, gravferdsbyrå og gravplassmyndigheten/kommunen. Tjenesten er en del av livshendelsen Dødsfall og arv.

Helsedata.no – enklere tilgang til helsedata
Helsedata skal gjøres raskere og enklere tilgjengelig og saksbehandlingstiden skal reduseres. Direktoratet for e-helse samarbeider med Kreftregisteret, Folkehelseinstituttet, Helsedirektoratet, de regionale helseforetakene og Norsk helsearkiv (Arkivverket) for å skape bedre løsninger for brukere av helsedata. Direktoratet for e-helse samarbeider også med UH-sektoren om mer effektiv bruk av etablerte data- og analysetjenester for å forenkle tilgangen til helsedata. Helsedata.no er en felles søknadsportal for tilgang på helsedata, og Helsedataservice (Direktoratet for e-helse) er etablert som én vei inn for tilgang til helseregisterdata.

Digitalisering i kommunal helse- og omsorgstjeneste
Digitale løsninger og bedre digital samhandling skal bidra til at innbyggere får gode, sammenhengende og tilgjengelige tjenester der de bor. Bruk av digitale løsninger skal gjøre det enklere å være pasient og ansatt i vår felles helse- og omsorgstjeneste og gjøre tjenesten bærekraftig for fremtiden. Innbyggerne skal ha tillit til at opplysninger om helsen deres blir behandlet på en trygg og sikker måte. Regjeringen vil legge frem en strategi for digital sikkerhet i helse- og omsorgssektoren i stortingsmeldingen om helseberedskap.

Regjeringen ønsker at bruk av innovative e-helseløsninger skal bidra både til en trygg og effektiv helse- og omsorgstjeneste og til å skape et hjemmemarked for leverandører. I Norge er det mange aktører som hver for seg digitalisere og omstiller tjenestene for å levere helse-

og omsorgstjenester på nye måter. Regjeringen vil jobbe for nasjonal koordinering på e-helsefeltet og sikre at vi bruker de samlede ressursene på en god måte.

Regjeringen tar sikte på å fremme en stortingsmelding om Nasjonal helse- og samhandlingsplan innen utgangen av 2023. Meldingen vil utgjøre rammene for utviklingen av vår felles helse- og omsorgstjeneste. Sentrale mål er gode og sømløse pasientforløp og gode tjenester i hele landet. Nasjonal helse- og samhandlingsplan vil omhandle utvikling av både den kommunale helse- og omsorgstjenesten og spesialisthelsetjenesten. Meldingen vil inkludere temaene samhandling, rehabilitering, digitalisering, kvalitetsforbedring og pasientsikkerhet, kompetanse, og svangerskap-, føde- og barseltilbud.
Helse- og omsorgsdepartementet og KS vil videreføre samarbeidet om innføring av nasjonale e-helseløsninger i 2023. Målet er å legge til rette for innføring av nasjonale e-helseløsninger i kommunene og legge til rette for bedre journal- og samhandlingsløsninger. Innføring av kjernejournal vil bidra til at helseopplysninger følger pasienten på tvers av helse- og omsorgstjenesten og er høyt prioritert. Kjernejournal er også en forutsetning for innføring av pasientens legemiddelliste, som vil gi bedre tilgang til legemiddelinformasjon.

Digital samhandling
Det er allerede etablert flere nasjonale e-helseløsninger for digital samhandling. For å nå målene om helhetlig og effektiv digital samhandling og få realisert gevinstene, er det behov for å videreutvikle dagens nasjonale e-helseløsninger og etablere nye tjenester og ny funksjonalitet.

En felles legemiddeloversikt er høyt prioritert av aktørene i helse- og omsorgstjenesten og vil realisere nytte hos både spesialisthelsetjenesten, kommunal helse- og omsorgstjeneste, pasient og innbygger, gjennom økt effektivitet og økt pasientsikkerhet. Kommunenes deltagelse er en forutsetning for å lykkes med en felles legemiddeloversikt. Arbeidet med å realisere felles komponenter som er nødvendige for å håndtere informasjonssikkerhet og personvern knyttet til mer utstrakt bruk av digital samhandling, skal fortsette i 2023. I 2022 har innsatsen vært rettet mot å etablere løsningen *pasientens prøvesvar* samt tilhørende tjenester for deling av kritisk informasjon og dokumenter via kjernejournal. Dette skal sikre at rett helsepersonell får tilgang på relevant pasientinformasjon når behovet er til stede. Tjenesten pasientens prøvesvar skal gi helsepersonell og pasienter tilgang til prøvesvar uavhengig av hvem som har bestilt og utført undersøkelsen. Målet er å gjøre laboratorie- og radiologisvar tilgjengelige for helsepersonell og for innbyggerne via helsenorge.no.

Velferdsteknologisk knutepunkt er etablert som en nasjonal tjeneste for å utveksle journalføringspliktige helseopplysninger mellom kommunens velferdsteknologiske løsninger og virksomhetens journalsystem. Det skal understøtte arbeidet med digital hjemmeoppfølging og bidra til å øke trygghet og mestring hos innbygger, og øke omsorgskapasiteten i kommunene.

Nasjonal rådsmodell for e-helse

Den nasjonale rådsmodellen for e-helse er en videreutvikling av den nasjonale styringsmodellen for e-helse og endringene ble gjennomført 1. juli 2022. Formålet med rådsmodellen er å styrke gjennomføringsevnen på e-helseområdet gjennom å samle de sentrale aktørene i helse- og omsorgssektoren om felles behov, utviklingsretning, innsats og måloppnåelse. Modellen består i dag av tre utvalg, Nasjonalt e-helseråd, Prioriteringsutvalget (NUIT) og Fagutvalget (NUFA) med medlemmer fra helsesektoren, inklusive KS og utvalgte kommuner. Saker fra den nasjonale rådsmodellen for e-helse løftes til konsultasjonsordningen mellom staten ved regjeringen og KS ved behov.

Innføringsaktiviteter
I arbeidet med digitalisering i helse- og omsorgssektoren er det viktig med helhet og sammenheng. Skal vi lykkes er det viktig at innføringen av de nasjonale e-helseløsningene prioriteres og koordineres i fellesskap, og at kommunesektoren settes i stand til å understøtte felles planer. Det er avgjørende at det er tilstrekkelig kapasitet i tjenesten til å ta imot løsningene.

Flere av de nasjonale e-helseløsningene krever innføringsaktiviteter i kommunene de nærmeste årene. Flere av løsningene vil kreve tilpasninger i kommunenes IKT-systemer, etablering av nødvendig infrastruktur og sikkerhetsløsninger, og endring av arbeidsprosesser. Kompetansenettverk for innføring, i regi av KS, skal understøtte kommunenes arbeid med innføring av nasjonale e-helseløsninger og bidra til at innføringen følger nasjonale planer. Det er i statsbudsjettet for 2023 bevilget 20,4 millioner kroner til nettverk for innføring av e-helseløsninger i kommunene. Kommunal sektors ambisjoner på e-helseområdet, et felles plan og rammeverk utarbeidet av KS i samarbeid med kommuner og fylkeskommuner, danner grunnlaget for nasjonale portefølje for innføring og kunnskapsutvikling innen e-helse, og vil være et grunnlag for arbeidet som gjennomføres i kompetansenettverket for innføring og kommunenettverk for velferdsteknologi og digital hjemmeoppfølging.

Velferdsteknologiprogrammet er videreført i perioden 2022 - 2024. Formålet med videreføringen av programmet er å understøtte kommunene i deres arbeid med å integrere velferdsteknologi i de kommune helse- og omsorgstjenestene. Nasjonale myndigheter støtter først og fremst kommunene gjennom nettverk og prosessveiledning. Det er et mål å etablere varige strukturer for å sikre at velferdsteknologi integreres i det ordinære tjenestetilbudet også etter 2024. Økt bruk av velferdsteknologi kan føre til økt kvalitet i form av bl.a. økt mestring for tjenestemottakere i den kommunale helse- og omsorgstjenesten og økt omsorgskapasitet. Nasjonale myndigheter støtter også kommunene gjennom prosessveiledning av kommunene i innføring av velferdsteknologi, og faglig rådgivning, kunnskapsutvikling, utvikling av retningslinjer og opplæringsverktøy mv i velferdsteknologi.

Helseplattformen
Helseplattformen er en felles pasientjournal for hele helsetjenesten i Midt-Norge. Helseplattformen er tatt i bruk i syv kommuner, inkludert Trondheim kommune, St. Olavs hospital og alle laboratoriene i Midt-Norge. Alle midt-norske kommuner har opsjonsavtaler

med Helseplattformen, og kan fatte vedtak i kommunestyret for å slutte seg til den felles journalløsningen.

Bedre journalløsninger i kommunene
Arbeidet med felles kommunal journal har fra 2021 vært organisert som et samarbeidsprosjekt mellom staten, KS og samarbeidskommuner. Arbeidet med å oppdatere styringsdokumentet og utforme en gjennomføringsstrategi i tråd med anbefalingen fra den eksterne kvalitetssikringen (KS2) av forprosjektet har pågått siden 2021, jf. Prop. 1 S (2020–2021) og Prop. 1 S (2021–2022). Staten har i 2021 og 2022 finansiert programaktiviteter til arbeidet med felles kommunal journal gjennom en tilskuddsordning. Jf Prop 1 S (2022-2023) avvikles den statlige finansieringen av programaktiviteter fra 2023, og det vil ikke være aktuelt for staten å være medeier i et ev. felleseid selskap med kommunesektoren. Jf Innst. 11 (2022-2023) vedtak 263, har Stortinget bedt regjeringen sørge for at opp mot 20 millioner kroner innvilget for 2022 overføres til 2023 med formål om å sluttføre pågående aktiviteter knyttet til å ferdigstille, kvalitetssikre og forankre styringsdokumentet for felles kommunal journal i kommunesektoren.

Regjeringen vil støtte kommunenes arbeid med bedre journalløsninger gjennom regulering av standarder og krav til funksjonalitet, og gjennom virkemidler som stimulerer til at kommunene kan foreta investeringer og forenkler kommunenes anskaffelse og modernisering av journalsystemene.

Regjeringen har i Hurdalsplattformen varslet at den vil etablere en helseteknologiordning som støtter innføring av ny teknologi i helse- og omsorgstjenesten. På oppdrag fra regjeringen har Direktoratet for e-helse, i samarbeid med Helsedirektoratet og KS, utredet en mengde tiltak for både velferdsteknologiområdet og journalområdet, for hva en helseteknologiordning kan inneholde. Helseteknologiordningen er planlagt innført i 2024 og vil bygges ut trinnvis.

Pålegg om bruk av og betaling for forvaltning og drift av nasjonale e-helseløsninger
Stortinget vedtok 17. desember 2021 endringer i pasientjournalloven §§ 8 og 21 som gir Helse- og omsorgsdepartementet hjemmel til å gi forskrifter som pålegger virksomheter som yter helse- og omsorgstjenester å gjøre tilgjengelig og ta i bruk elektroniske resepter (e-resept), Nasjonal kjernejournal, helsenorge.no og helsenettet. Loven gir videre departementet hjemmel til å gi forskrifter som pålegger virksomhetene å betale for forvaltning og drift av disse løsningene. Departementet har fastsatt betalingen for 2023 gjennom endring i forskrift om standarder og nasjonale e-helseløsninger. Kommunenes andel av betalingen fordeles mellom kommunene etter delkostnadsnøkkel kommunehelse. Kommunene er over statsbudsjettet kompensert for eksisterende kostnader til forvaltning og drift av løsningene, og for deler av kostnadsveksten siden betalingsordningen ble innført i 2022. Prismodellene for de nasjonale e-helseløsningene er nå under evaluering og vil fra 2024 bli justert basert på erfaringer med ordningen.
Helse- og omsorgsdepartementet har etablert et teknisk beregningsutvalg for nasjonale e-helseløsninger som skal vurdere tallgrunnlaget for beregnede kostnader til forvaltning og drift

av de nasjonale e-helseløsningene. Utvalget inkluderer medlemmer som er foreslått av KS, regionale helseforetak, Legeforeningen og Apotekforeningen. Beregningsutvalget gjennomfører hver vår en overordnet gjennomgang av tallmaterialet, basert på prognoser fra Norsk helsenett SF. På høsten behandler utvalget Norsk helsenett SFs beregninger av priser og avgiftsatser på et mer detaljert nivå. Kostnader til forvaltning og drift som er en konsekvens av investeringsbeslutninger og tiltak i nasjonal e-helseportefølje, skal synliggjøres og behandles i den nasjonale rådsmodellen for e-helse. I tillegg drøftes årlige endringer i betalingen for forvaltning og drift av de nasjonale e-helseløsningene i konsultasjonsordningen mellom regjeringen og KS.

DigiUng-programmet
I juni 2022 besluttet regjeringen at ung.no skal være statens primære tverrsektorielle kanal for digital informasjon, dialog og digitale tjenester til barn og unge på tvers av tjenestenivåer gjennom realisering av DigiUng-programmet. BFD, HOD, KD, KUD, KDD, AID og JD med relevante underliggende etater samarbeider om ung.no og DigiUng-programmet.

Det er lagt opp til tre nivåer av interaksjon med forvaltningen på ung.no som avhenger av hvilke behov ungdommen har. Det er lagt opp til et økosystem, der tjenestene fortsatt skal driftes på de plattformer hvor de eksisterer i dag, og det arbeides for å få ulike plattformer, databaser og tjenester til å henge sammen og fungere helhetlig for brukeren. Målet er at barn og unge får riktig hjelp til riktig tid, og at de skal veiledes inn til riktig tjeneste fra ung.no. DigiUng-programmet er også knyttet opp mot livshendelsen *Alvorlig sykt barn*.

Reklameskolen
Reklameskolen er et digitalt interaktivt opplæringsverktøy om reklame laget primært for elever på ungdomsskolen. Her får elevene lære om hvordan reklame påvirker oss gjennom video, tekst og interaktive oppgaver. Målet er at elevene skal bli flinkere til å kjenne igjen reklame, skjønne hvem som står bak og hvordan reklamen påvirker oss. Reklameskolen er utviklet av Forbrukertilsynet. Reklameskolen

Digitalisering i barnevernet
DigiBarnevern består av to prosjekter, et kommunalt og et statlig prosjekt. Sammen har de som mål å øke kvaliteten i det kommunale barnevernet, blant annet ved å sørge for bedre IT-løsninger. Bedre digitale løsninger skal gi kommunene bedre forutsetninger for å gi god og effektiv hjelp til barn og unge, samt legge til rette for bedre styringsinformasjon for ledere i barnevernet og i kommuneledelsen. Det statlige prosjektet har ansvaret for tre leveranser som kommunene kan ta i bruk:
Nasjonal portal for bekymringsmeldinger ble lansert i april 2020 og er et samarbeid mellom Bufdir og KS. Portalen gjør det mulig for både privatpersoner og offentlige meldere å sende bekymringsmeldinger digitalt. Dette gjør det enklere og sikrere å melde bekymring, og barnevernstjenesten i ulike kommuner kan raskere gi hjelp til barn som trenger det. Løsningen er overført fra prosjekt til forvaltning.

Barnevernsfaglig kvalitetssystem (BFK) skal gi barnevernsfaglig og juridisk kvalitetsstøtte til det kommunale barnevernets arbeid med barnevernssaker. Et av målene med BFK er å bidra til likere og mer kvalitetssikret utøvelse av barnevernsfaglig praksis i alle landets barnevernstjenester. BFKs innholdselementer kan implementeres i nye fagsystemer, og dermed bli en integrert del av det kommunale barnevernets arbeidsverktøy. Saksbehandlerne vil på den måten få støtte i det daglige arbeidet, direkte tilgjengelig i fagsystemet. BFKs innhold gjøres tilgjengelig på data.bufdir.no, primært for systemleverandører som utvikler nye fagsystemer. Løsningen er overført fra prosjekt til forvaltning.

Rapporteringsløsning og Nasjonalt barnevernregister er en ny måte for kommunene å rapportere til staten, og skjer fortløpende og automatisk fra nye fagsystemer. Den nye rapporteringsløsningen ivaretar kravene i KOSTRA-rapporteringen og rapportering til Statsforvalter, og overtar for de årlige og halvårlige rapporteringene. På Bufdir sine nettsider beskrives hvordan overgangen fra gammel til ny løsning skal håndteres. Løsningen overføres fra prosjekt til forvaltning i løpet av 2023.

Koordineringsansvar for en tryggere digital oppvekst for barn og unge
Regjeringen besluttet i 2022 at det skal legges fram en stortingsmelding om trygg digital oppvekst, og Barne- og familiedepartementet koordinerer dette arbeidet. Stortingsmeldingen følger opp *Nasjonal strategi for trygg digital oppvekst*, Rett på nett, og skal gå dypere inn i problemstillingene og målene i denne strategien. Medietilsynet har en koordinerende rolle på direktoratsnivå og skal etter planen lansere en handlingsplan som følger opp strategien *Rett på nett* høsten 2023.

DigiHoT – digitalisering i formidling av hjelpemidler og tilrettelegging
NAV startet i 2020 utviklingen av løsninger for innbygger, kommune og hjelpemiddelsentral om formidling av hjelpemidler. Leveransene til nå lar kommunene sende bestillinger og søknader på utvalgte hjelpemidler til hjelpemiddelsentralen, etter fullmakt fra bruker. Bruker får også enkel oversikt over status i sak, og det er gjort et betydelig arbeid for å forenkle og effektivisere saksbehandlingen i NAV. Prosjektet vil fremover også se på forbedringer i lager- og logistikkhåndtering. Prosjektet er et samarbeid mellom NAV og KS, og vil gå ut 2024.

Digitalisering i barnehager og grunnopplæringen
Samarbeid om digitalisering i skolen og barnehage er forankret i en samarbeidsavtale mellom Kunnskapsdepartementet og KS om kvalitetsutvikling i sektoren. Fra 2022 har samarbeidet også vært operasjonalisert gjennom samstyringsråd for digitalisering i grunnopplæringen mellom staten og KS.
I tråd med dette utvikler regjeringen i samarbeid med KS, en ny strategi for digital kompetanse og infrastruktur i barnehage og skole. Som del av arbeidet med den nye strategien har det i 2022 vært innspillsmøter med kommunal sektor, bransjeorganisasjoner og andre fag -og interesseorganisasjoner. Strategien planlegges å ha en varighet fra 2023 til 2030, og vil favne om barnehage, grunnskolen og videregående opplæring. Sammen har Kunnskapsdepartementet og KS vurdert ulike kartlegginger av behov og forslag til tiltak i

kommunal sektor. Innspillene viste til både store felles utfordringer og viktige gevinster ved digitalisering og at det er store forskjeller i kommunenes digitale infrastruktur og kompetanse disse sektorene. Aktuelle innsatsområder i strategien er digital praksis i barnehage og skole, digitale læremidler og tjenester, universell utforming og inkludering, og personvern og informasjonssikkerhet. Regjeringen og KS planlegger å legge frem den nye strategien vinteren 2023. Videre samordning og samarbeid om digitalisering på nasjonalt og regionalt nivå sees på som en forutsetning for å nå viktige målsetninger om barnehage- og skoleutvikling.

Miljødirektoratet.no
Miljødirektoratet.no gir kommunene og andre myndigheter oppdatert digital veiledning og kommentarer til miljøregelverket. På Miljødirektoratet.no finner kommunene også nyttige tjenester, verktøy og data innen forurensning, naturforvaltning, friluftsliv, arealplanlegging, klima og luftkvalitet.

Ny IT-løsning for luftkvalitetsmåledata: "Luftkvalitet i Norge: Målinger"
Miljødirektoratet startet høsten 2022 utviklingen av et nytt IT-system for luftkvalitetsmåledata. Plikten til å måle luftkvalitet er nedfelt i forurensningsforskriften kapittel 7.
Systemet vil både være

- en database hvor det vil være mulig å se hva som har vært målt av luftforurensning for eksempel svevestøv på Norges målestasjoner.
    - tilbake i tid
    - i "nær sanntid" som vil si fram til forrige time, som vist her: Luftkvalitet i Norge (miljodirektoratet.no)
- et arbeidsverktøy for de som utfører målingene, de som sjekker kvaliteten til dataene og de som rapporterer dataene inn til det europeiske miljøbyrået.

Et godt IT-system for måledata gjør det mulig å følge med på status og utvikling av nivåene av luftforurensning. Det er et viktig grunnlag for å vurdere og iverksette tiltak. Systemet skal være brukervennlig, bruke moderne teknologi og være fleksibelt.
Hovedbrukergruppene er:

- Kommunen
- Fylkeskommunen
- Statens vegvesen
- Industribedrifter
- Miljødirektoratet
- Nasjonalt referanselaboratorium for luftkvalitetsmålinger (NRL)

Kommunen er både myndighet for lokal luftkvalitet etter forurensingsforskriften kapittel 7 og anleggseier (vedfyring, kommunale veier og havner). Fylkeskommunen og Statens vegvesen har ansvar for luftforurensning fra sine veier, mens industribedrifter har ansvar for luftforurensning fra sine anlegg. Alle disse er også eiere av eller medansvarlige for målestasjonene i Norge.

Miljødirektoratet har blant annet ansvar for bakgrunnsmålinger i spredtbygde strøk og rapportering av data til det europeiske miljøbyrået. NRL skal sikre at kvaliteten på måledataene er i tråd med det europeiske kvalitetssystemet.

IT-systemet vil også være nyttig for andre i forvaltningen som statsforvalteren, forskningsmiljøer, befolkningen og journalister.

Hjorteviltregisteret
Miljødirektoratet har de siste årene tilrettelagt for en effektiv kommunal saksbehandling i Hjorteviltregisteret. For eksempel kan kommunene nå sende ut digitalt godkjente fellingstillatelser med ev. vedlegg direkte fra registeret til alle valdansvarlige i kommunen samtidig. Kommunen kan også motta digitale fellingsrapporter etter endt jakt, og sende påminnelse om manglende rapportering via Hjorteviltregisteret.

NaturOppdrag - bestille og utføre oppgaver i felt knytta til verneområder
NaturOppdrag er et digitalt verktøy for å bestille og gjennomføre oppdrag i felt, følge opp installasjoner i felt og å notere viktige feltobservasjoner. Det skal særlig støtte en bedre dialog og samhandling mellom forvaltningsmyndighet og naturoppsyn. Verktøyet blir tilgjengelig for alle kommuner med forvaltningsmyndighet for verneområder, på lik linje med andre forvaltningsmyndigheter (Statsforvalteren, Sysselmesteren, Nasjonalpark- og verneområdestyrer). I dag har ca. 60 kommuner forvaltningsmyndighet for ett eller flere verneområder. Det omfatter ca. 300 områder - se verneområder med kommunal myndighet. På nettsiden Forvaltningsmyndighetens ansvar for verneområder er dette forklart nærmere.

Vann-Nett
Vann-Nett er inngangsportalen til informasjon om vann i Norge. Vann-Nett sikrer tilgang på miljøinformasjon for kommuner, faglige institusjoner, interessegrupper, alle myndigheter og allmennheten. Målet er å gi en enkel og rask tilgang til data i forskjellige format. Her kan du finne hvordan det står til i vannet (miljøtilstand, miljømål, tiltak, påvirkninger osv.) og få ut data i forskjellige formater (faktaark og kart). Faktaarkene vil kunne brukes for å formidle informasjon om miljøtilstanden og hvordan vannet påvirkes av ulik menneskelig aktivitet. Dette vil gi en samlet oversikt til bruk i jobben med å ta gode og helhetlige beslutninger for å bedre miljøet i vannet. Kommunen er myndighet på flere områder som påvirker vann: landbruk, miljø, avløp, forurensning, arealbruk med mer. Her har kommunen virkemidler i vannforvaltningen blant annet gjennom plan- og bygnings-loven, forurensingsloven og vannressursloven.

Jegerprøveeksamen
Jegerprøveeksamen med gebyr ble 1. januar 2023 oppdatert med en digital løsning som gjør at kandidatene kan ta eksamen på sin egen mobile enhet. Det er kommunene som er ansvarlig for å gjennomføre kurs med eksamen, og dette forenkles nå ved at de ikke lenger trenger å stille med klassesett med PCer på eksamen.

Tilskudd.no - digital oversikt over statlige tilskudd til frivillig sektor
I Meld. St. 10 (2018-2019) *Frivilligheita - sterk, sjølvstendig, mangfaldig* ble det varslet en forenklingsreform for frivillig sektor. Forenklingsreformen er forankret i målet om at det skal være enkelt å engasjere seg som frivillig, det skal være enkelt å drive frivillig organisasjon og det skal være enkelt for frivilligheten å søke og rapportere på statlige tilskudd. Digitaliseringsstrategien for offentlig sektor (2019-2025) peker ut syv prioriterte livshendelser. Starte og drive en frivillig organisasjon er én av de prioriterte livshendelsene. Kultur- og likestillingsdepartementet (KUD) har overordnet ansvar for oppfølging av livshendelsen, og har sammen med Direktoratet for forvaltning og økonomistyring (DFØ) laget en digital løsning som gjør det mulig å få oversikt over statlige tilskuddsordninger, tildelinger, mottakere og enkeltstående tilskudd til frivillig sektor. Tilskudd.no ble lansert 5. desember 2022, og kan også være nyttig for kommunene for å vurdere egne virkemidler og tiltak. Rapporten om videreutvikling av Frivillighetsregisteret ble ferdigstilt i mai 2022. Som en oppfølging av rapporten vil Kultur- og likestillingsdepartementet igangsette arbeidet med å gjennomgå lov om register for frivillig virksomhet. Lovarbeidet vil særlig fokusere på registreringsrett i Frivillighetsregisteret og hvordan registeret kan bidra til forenkling og samordning.

Nye digitaliseringstiltak i 2023
Digitalisering er både en driver og et viktig virkemiddel for å effektivisere ressursbruken og tilby bedre tjenester til innbyggere, næringsliv og frivillig sektor. Digitalisering, bruk av ny teknologi og bedre utnyttelse av data kan bidra til økt innovasjon, bedre offentlige tjenester og nye arbeidsplasser. Noen av de nye digitaliseringstiltakene i 2023 med relevans for kommunal sektor er listet opp nedenfor.

- Et prioritert digitaliseringstiltak i 2023 som vil ha betydning for kommunal sektor er økt bevilgning på om lag 58 millioner kroner til bredbåndsutbygging i områder uten kommersielt grunnlag for utbygging, dette gir totalt 362,7 millioner kroner.
- Gjennom økning av kommunerammen kompenseres kommuner og fylkeskommuner for kostnader ved å innføre krav om synstolking av innhold på offentlige nettsider.
- Regjeringen vil prioritere arbeid knyttet til utvikling av matrikkelen. Matrikkelen er en viktig felleskomponent som gjør det lettere å lage gode løsninger. Dette arbeidet vil styrke deling og bruk av data på tvers av offentlig og privat sektor og bidra til videreutvikling av den nasjonale infrastrukturen for geografisk informasjon. En matrikkel med høyere kvalitet og bedre tekniske løsninger er viktig for arbeidet med forenklinger og innsparinger i staten, kommunene og næringslivet.
- Den regulatoriske sandkassen for personvernvennlig innovasjon og digitalisering hos Datatilsynet videreføres. Sandkassen er et tiltak for å stimulere til utvikling av

personvernvennlige tekniske løsninger, og både offentlig og privat sektor kan få veiledning i arbeidet med å ivareta personvernet i nye og innovative løsninger.

Medfinansieringsordningen, som forvaltes av Digitaliseringsdirektoratet, har siden oppstarten i 2016 bidratt til at 81 tiltak med samlede prosjektkostnader på over 1,7 mrd. kroner er igangsatt. Prosjektene i 2016–2022 oppgir samlede netto gevinster i offentlig sektor på over 1,2 mrd. kroner per år. Dette fordeler seg på statlig sektor med 335 mill. kroner per år og kommunal sektor med 839 mill. kroner per år.
I 2021 fikk 12 prosjekter tilsagn fra medfinansieringsordningen, med en samlet tilsagnsramme på 129 mill. kroner. I 2022 har 8 prosjekter fått tilsagn om til sammen 128,1 mill. kroner i medfinansiering. Disse prosjektene har en beregnet netto nåverdi på 2,2 mrd. kroner over 10 år, med vesentlige gevinster hos innbyggere og næringsliv. Mulig innsparingspotensial i offentlig sektor er beregnet til om lag 152 mill. kroner per år. Av dette er om lag 142 mill. kroner i kommunesektoren.
I 2022 er om lag 57 pst. av gitte tilsagn til prosjekter som gjelder strategisk prioriterte fellesløsninger eller tverrgående tiltak (sammenhengende tjenester). Resterende tilsagn er gitt til små og mellomstore lønnsomme digitaliseringstiltak, slike som ordningen har støttet siden 2016. Ordningen har blitt evaluert og det er vedtatt reviderte retningslinjer for den i 2022.

Digitaliseringsrundskrivet for statlige virksomheter
Digitaliseringsrundskrivet gjelder for statlig sektor, og er en helhetlig sammenstilling av pålegg, føringer og anbefalinger for staten. Siden rundskrivet viser til regjeringsbeslutninger og en rekke krav som er hjemlet i lover som også gjelder for kommunal sektor, kan deler av rundskrivet være relevant for kommuner og fylkeskommuner. Departementet oppfordrer kommuner og fylkeskommuner til å gjøre seg kjent med kravene som stilles og anbefalingene som gis til statlige virksomheter på digitaliseringsområdet, og vurdere om noen av disse kan være relevante for digitaliseringsarbeidet i kommunal sektor.

Rundskrivet stiller også krav til involvering av kommunal sektor i nasjonalt digitaliseringsarbeid. Regjeringens digitaliseringsstrategi stadfester felles prinsipper for samarbeid mellom stat og kommune i det statlige digitaliseringsarbeidet, beskrevet som «samordning med og involvering av kommunal sektor». Prinsippene inngår i rundskrivet og gjelder for «strategisk digitaliseringsarbeid av betydning for offentlig sektor, og som skjer i råd og utvalg der aktører fra kommunal og statlig sektor er representert». Det stilles krav til statlige virksomheter om å følge prinsippene. I tillegg stilles krav om involvering av KS ved forberedelse av digitaliseringstiltak. En sjekkliste for hvordan kommunal sektor bør involveres i statlige digitaliseringstiltak, er utarbeidet av Digitaliseringsdirektoratet og KS. Sjekklisten retter seg mot statlig sektor, men er også relevant å kjenne til for kommunal sektor.

Med hilsen

Jan Hjelle
ekspedisjonssjef

Katarina de Brisis
avdelingsdirektør

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer

Referansearkitektur for informasjonssikkerhet, digital beredskap og personvern for kommunal sektor (RSB)

Konseptuell beskrivelse
Versjon 1.0
18. august 2020

Overlevert Aksjon prosjektet, 18. august 2020

Innholdsfortegnelse

1. Innledning 3
2. Bakgrunn for utarbeidelse av RSB 4
3. RSB i et nøtteskall 6
3.1 Dagens utfordringer 6
3.2 Hva er RSB 6
3.2.1 RSB sett fra konsumentens side 8
3.2.2 RSB sett fra tjenesteyters side 8
3.3 Hva baserer RSB seg på 8
3.4 Oversikt over RSB 9
4. Gjennomgang av elementene i RSB 10
4.1 RSB modellen 10
4.2 Grunnprinsipper 10
4.2.1 Tjenesteleveranseprinsippet 10
4.2.2 Verdikjedeprinsippet 10
4.2.3 Den menneskelig utgangspunkt 10
4.2.4 Prinsippet om innebygd sikkerhet, beredskap, og personvern 11
4.3 Styringsprinsipper 11
4.3.1 Risikostyring 11
4.3.2 Innovasjon og evolusjon 11
4.3.3 Læring 12
4.3.4 Målbarhet 12
4.4 Tjenesteleveranse (lag 1) 12
4.5 Perspektiver (lag 2) 13
4.5.1 Virksomhetsperspektivet 13
4.5.2 Samfunnsperspektivet 14
4.5.3 Konsumentperspektivet 14
4.5.4 Oppsummering perspektivene 14
4.6 Tjenestekritikalitet (lag 3) 14
4.7 Sikkerhets-, beredskaps-, og personvernprinsipper (lag 4) 17
4.7.1 Begreper i RSB 17
4.7.2 Sikkerhets-, beredskaps-, og personvernprinsipper 22
7.6 Oppsummering RSB 27
7.7 Konsekvenser for Akson 27

1. Innledning

Direktoratet for e-helse har fått i oppdrag å gjennomføre et forprosjekt for felles kommunal journal og samhandling mellom aktørene innen helse- og omsorgssektoren. Tiltaket har fått navnet Akson. Tiltaket Akson inneholder to deler. En samhandlingsløsning og en felles kommunal journalløsning. Samhandlingsløsningen skal leveres av Norsk Helsenett SF (NHN), mens felles kommunal journal leveres som tjeneste av Akson Journal AS[1].

Når det refereres til begrepet Akson i dette dokumentet refereres det til felles kommunal journalløsning med tilhørende undersystemer. Når det refereres til Akson journal AS referer det til virksomheten som skal levere journalløsningen som en tjeneste til kommunal sektor.

Tiltaket Akson innebærer økt samling og deling av helseopplysninger og anses som et kritisk system for helsebehandling i kommunal sektor[2]. Informasjonssikkerhet[3] (henter kalt sikkerhet), digital beredskap[4] (heretter kalt beredskap), og personvern har av den grunn høy prioritet for å bidra til god og trygg helsebehandling som oppleves tillitsskapende av den enkelte, og samfunnet generelt.

Det finnes ingen helhetlig tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor for digitale tjenester. Dette dokumentet er utarbeidet i den hensikt å bistå kommunal sektor med referansearkitektur innen områdene sikkerhet, beredskap og personvern i et digitalt tjenesteperspektiv. Forkortet som RSB.

Formålet med RSB er å sikre at Akson journal AS og kommunal sektor har tilstrekkelig sikkerhet, beredskap, og personvern for å levere og konsumere trygge og sikre digitale tjenester.

RSB versjon 1.0 er en konseptuell beskrivelse, det vil si en introduksjon til hvordan og hva man bør tenke på innen sikkerhet, beredskap og personvern i et digitalt tjenesteperspektiv. RSB versjon 1.0 er rettet mot tiltaket Akson, og har en helhetlig tilnærming til sikkerhet, beredskap og personvern i tjenesteperspektiv. RSB versjon 1.0 kan ses på som et kravsett som kommunal sektor stiller til Akson.

I fremstillingen benyttes også begrepene tjenesteyter om Akson journal AS, og konsument om kommunene. I denne konteksten vil konsumentene (kommuner) gjennom RSB stille krav til tjenesteyter (Akson journal AS) på hva som bør oppfylles av krav for å kunne motta tjenesten. Tjenesteyter (Akson AS) vil sin side bruke RSB for å sikre tilstrekkelig sikkerhets- og beredskapsevne for å være i stand til å levere trygge og sikre digitale tjenester.

Dokumentet er inndelt i følgende struktur:

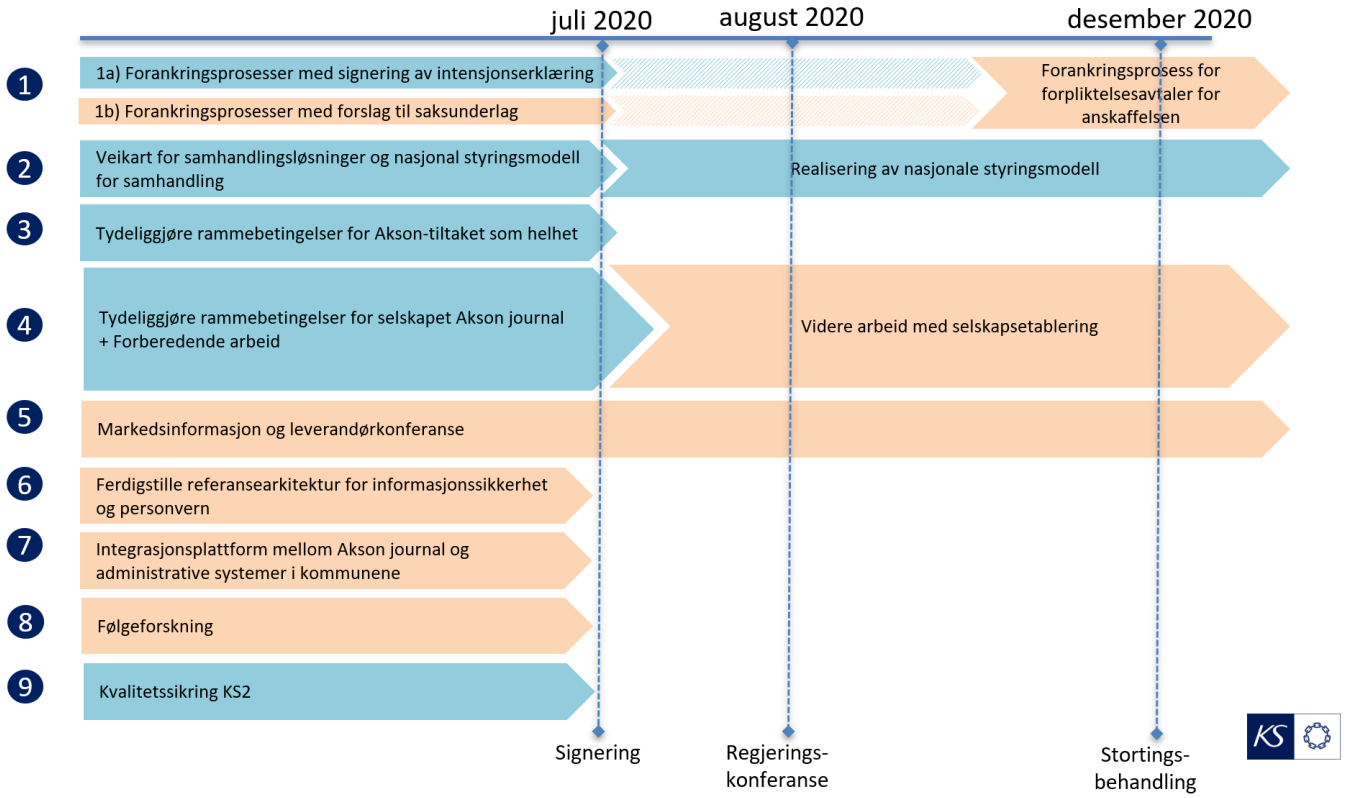
- Bakgrunn for utarbeidelse av RSB.
- RSB i et nøkkeskall.
- Gjennomgang av elementene i RSB.
- Konsekvenser for Akson journal AS og RSB

[1] For mer informasjon om Akson se: https://www.ks.no/fagomrader/digitalisering/utviklingsprosjekter/akson/
[2] Begrepet kommunal sektor benyttes både om kommunene og fylkeskommunene.
[3] Begrepet informasjonssikkerhet inkluderer også teknologisikkerhet.
[4] Begrepet digital beredskap benyttes i forhold informasjonsbehandling.

2. Bakgrunn for utarbeidelse av RSB

Det har vært en dialog mellom Direktoratet for e-helse og kommunal sektor angående hvilke sikkerhetsprinsipper som bør legges til grunn i forbindelse med tiltaket Akson. Ettersom det ikke finnes en helhetlig og metodisk tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor i et tjeneste- og verdikjedeperspektiv, utarbeidet Oslo kommune og KS i februar 2020 et utkastet til en sådan referansearkitektur.

I diskusjonene etter februar 2020 mellom Direktoratet for e-helse, KS, og kommunene er det satt opp 9 tiltak for videre fremdrift av Akson, se figur 1, *Videre fremdrift Akson*.



Figur 1, Videre fremdrift Akson.

Et av tiltakene i videre fremdrift er tiltak nummer 6, «*Ferdigstille referansearkitektur for informasjonssikkerhet og personvern*» med følgende oppdragsformulering.

Oppdraget
«Utarbeide en referansearkitektur for informasjonssikkerhet, beredskap og personvern som premisser for Akson journal AS og felles kommunale journal sin integrasjon med kommunale administrative systemer, inklusive løsninger for identitets- og tilgangsstyring.»

Leveranser
«*Rapport med beskrivelse av referansearkitektur for kommunesektoren og med tydelig angivelse av premisser for felles kommunal journal og for virksomheten Akson journal AS, inklusive konsekvenser for styringssystem for informasjonssikkerhet og personvern*».

Avgrensninger
«*Referansearkitekturen vil være på strategisk [konseptuelt] nivå med et sett med prinsipper for kommunenes utøvelse av informasjonssikkerhet, beredskap og personvern. Behandlingsansvar er ikke en del av oppdraget*».

Tiltak nummer 6 innebærer å sluttføre det arbeidet som Oslo kommune og KS startet sammen med kommuner og andre aktører i kommunal sektor. Med dette som utgangspunkt har kommunal sektor utarbeidet versjon 1.0 av referansearkitektur for sikkerhet, beredskap og personvern for kommunal sektor (RSB).

Dataeierskapet i Akson er kompleks og det bør nedsettes en egen arbeidsgruppe som bør se på problematikken rundt behandlingsansvaret. Behandlingsansvaret ligger derfor utenfor utforming av RSB.

I forbindelse med utarbeidelsen av RSB er følgende vektlagt:

1) Arbeidsgruppen skal være bredt sammensatt. Hele spekteret av kommunal sektor med kommuner, fylkeskommuner, og skal interkommunale selskaper (IKS) innen IKT skal være representert.
2) Arbeidsgruppen skal være sammensatt av dyktig fagpersonell innen sine respektive fagområder.
3) Legge samstyringsmodellen for kommunal sektor til grunn. Det betyr at RSB behandles i Fagrådet for informasjonssikkerhet og personvern, Digitaliseringsutvalget, og KommIT-rådet for forankring av RSB i kommunal sektor.

Med utgangspunkt i det ovennevnte har arbeidsgruppen for utarbeidelsen av RSB bestått av 11 kommuner, 3 fylkeskommuner, 5 IKS, KINS og KS. Følgende personer har deltatt i arbeidsgruppen:

Type	Navn	Kommune/Fylkeskommune/IKS mv.
Kommuner	Anette Skogstad	Bodø kommune
	Hans Christian Sander	Fredrikstad kommune
	Jørn Hanssen	Harstad kommune
	Marianne Bjønness	Hamar kommune
	Per Jakobsen	Narvik kommune
	Roy Håland	Stavanger kommune
	Rune Nilsen	Tromsø kommune
	Rune Schumann	Oslo kommune
	Sigurd Strand	Larvik kommune
	Thomas Wullun	Horten kommune
	Vilhelm Einen	Larvik kommune
	Øyvind Erikstein	Midt-Telemark kommune
Fylkeskommuner	Egon Nybo Skaar	Viken fylkeskommune
	Espen Solheim	Trøndelag fylkeskommune
	John A. Solstad	Troms og Finnmark fylkeskommune
IKS	Espen Lund	Digitale Gardermoen
	John Horve	LMT Setesdal
	Lars Erik Domaas	Setesdal IKT
	Olve Sveen	IKT Agder
	Stian Jordet	IKT Valdres
Forening	Harald Torbjørnsen	KINS
KS, ledelse	Suhail Mushtaq	KS

I tråd med samstyringsmodellen har RSB vært presentert og diskutert i Fagrådet for informasjonssikkerhet og personvern forløpende. Videre er det gitt en kort orientering om RSB i digitaliseringsutvalget (14. april 2020) og i KommIT-rådet (7. februar 2020). Det er gitt orientering til Fagråd for arkitektur 19. juni 2020. Det blitt gjennomført mer enn 25 møter i perioden januar – juni 2020, både gruppen samlet og bilateralt. Det har blitt også avholdt møter med flere aktører og fagmyndigheter for rådføring og kommentarer. Tilbakemeldinger fra andre aktører og fagmyndighetene er blitt innarbeidet og bidratt til at RSB har blitt enda bedre.

RSB versjon 1.0, fikk faglig tilslutning i Fagrådet for informasjonssikkerhet og personvern den 24. juni 2020.

3. RSB i et nøtteskall

3.1 Dagens utfordringer

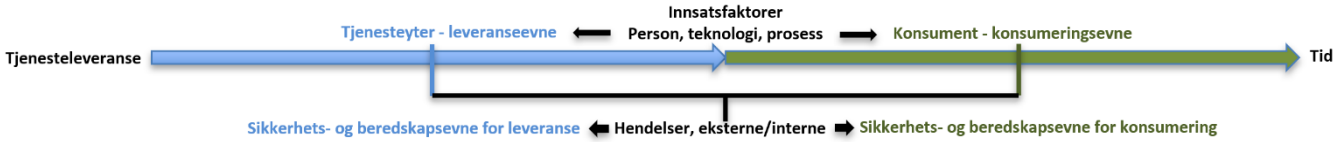
I KS' FoU-prosjekt "Kartlegging av digital modenhet i kommunesektoren"[5] oppgis flere utfordringer knyttet til arbeid med informasjonssikkerhet. Utfordringer er gjerne knyttet til etterlevelse og prioritering og forståelse fra ledelsen. Ofte blir rapporteringer, risikovurderinger, kurs i informasjonssikkerhet og personvern med videre veldig omfattende og med et vanskelig språk. Videre strever mange med å etterleve og gjennomføre alle kravene i en travel hverdag, hvor man har mer enn nok med å gjennomføre de daglige faglige arbeidsoppgaver.

Dagens personvern, sikkerhets- og beredskapsbilde kan fremstå som komplisert, uoversiktlig og utfordrende. For eksempel har man ulik språkbruk om samme teama i ulike lover, standarder og normer. Det virker også å være lite fokus på den menneskelige faktoren. I tillegg til at tjenesteperspektivet virker å være noe fraværende, noe som er primærmålet med enhver virksomhet. Det finnes heller ikke en helhetlig tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor. Dette i sum gir uheldige ringvirkninger når man skal levere eller konsumenere digitale tjenester i kommunal sektor.

3.2 Hva er RSB

Primærformålet for enhver virksomhet er å levere en eller flere tjenester som enten har et samfunnsøkonomisk[6] eller bedriftsøkonomisk[7] formål. Siden virksomhetens formål er å levere en eller flere tjenester, må disse sikres slik at virksomheten faktisk er i stand til å levere disse tjenestene. Videre, at konsumenten er i stand til å konsumere de. En virksomhet vil ikke operere lenge hvis den ikke er i stand til å levere stabile og gode tjenester til konsumentene over tid.

Tjenesteyter må derfor ha leveranseevne til å levere tjenesten, og sikkerhets- og beredskapsevne til å håndtere hendelser som kan påvirke leveranseevnen. Konsument må ha en konsumeringsevne til å konsumere tjenesten, og sikkerhets- og beredskapsevne til å håndtere hendelser som kan påvirke konsumeringsevnen. Konsumeringsevnen er viktig, ettersom konsumenten som regel er avhengig av denne for å kunne levere sine tjenester. Dette kan uttrykkes som figur 2, *sikkerhets- og beredskapsevne*, nedenfor.



Figur 2, sikkerhets- og beredskapsevne

En tjenesteleveranse kan deles inn i to deler. Del en er tjenesteproduksjon fra tjenesteyter. Tjenesteyter må ha leveringsevne for å kunne levere tjenesten. Del to er konsumeringsevne for konsument til å konsumere tjenesten. Konsumering og leveranse skje ved hjelp av innsatsfaktorer innen dimensjonene person, teknologi, og prosess.

I en optimal verden vil det ikke skje hendelser, og både leveransen og konsumering kan skje uten avbrytelser eller hindringer. Den digitale verden er imidlertid kompleks, ustabil, ukjent, og uforutsigbar. Derfor vil det uavhengig av hvor god sikkerhet, beredskap, og personvern man har, og uavhengig av hvor mange risikoreduserende tiltak som gjennomføres, skje uønskede hendelser. Hendelser som har sitt utspring i interne eller eksterne forhold. Derfor vil

[5] https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf

[6] Samfunnsøkonomisk gjelder spesielt offentlige virksomheter. Formålet her er ikke nødvendigvis å tjene penger, men at tjenesten totalt sett gir samfunnet en merverdi. I samfunnsøkonomisk ligger også ideelle organisasjoner med videre.

[7] Bedriftsøkonomisk gjelder spesielt private virksomheter. Poenget med privat virksomheter er ofte å levere tjenester som virksomheten kan tjente penger på. Selv om de er non-profit virksomheter, må også denne type virksomheter tjene penger på sin virksomhet for å kunne videreføres. Unntak kan tenkes i de rene stiftelsesvirksomheter som gir penger til veldedighet og gaver.

evnen til å kunne sikre innsatsfaktorene og håndtere hendelser være avgjørende for å kunne levere kontinuerlig, trygge og sikre tjenester. Det er dette som benevnes som sikkerhets- og beredskapsevne i RSB.

Det er viktig at både tjenesteyter og konsument har tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere gode, trygge, og sikre digitale tjenester. Fokuset i RSB er derfor rettet mot digitale tjenesteleveranser, tjenesteyters evne til å levere tjenesten på en trygg og sikker måte, og konsumentens mulighet til å konsumere tjenesten som forutsatt.

RSB har derfor følgende målsetting:

- Ha tjeneste og konsumentfokus – det vil si å sikre tilstrekkelig sikkerhets- og beredskapsevne.
- Redusere risiko langs naturlig arbeidsstrøm ved å ta hensyn til det menneskelig aspekt.
- Legge til rette for Innovasjon, evolusjon og prosessendringer.
- Legge til rette for kontinuerlig utvikling og forbedring.
- Være pragmatisk og ha helhetlig tilnærming til digitale tjenester.

For å finne tilstrekkelig sikkerhets- og beredskapsevne må man kjenne til tjenestekritikaliteten. Dette både fra tjenesteyterens og konsumentens side. For konsumenten er det viktig å vite hvilke kritikalitet og innvirkninger tjenesten vil utgjøre for konsumentens virke. Basert på dette, stille krav til tjenesteyter eller foreta risikoreduserende tiltak slik at tjenesten kan konsumeneres på en trygg og sikker måte. For tjenesteyter vil tjenestekritikaliteten gi en retning på hvilke krav tjenesteyter må oppfylle for å kunne levere tjenesten på en trygg og sikker måte.

Kjernen i RSB er at den skal være pragmatisk og ha en helhetlig tilnærming til å finne tjenestekritikalitet for digitale tjenester. Tjenestekritikaliteten er avgjørende for å kunne dimensjonere tilstrekkelig sikkerhets- og beredskapsevne. Og i en forlengelse av dette, hvilke sikkerhets-, beredskaps-, og personvernprinsipper som bør legges til grunn for å oppnå tilstrekkelig sikkerhets- og beredskapsevne i tråd med tjenestekritikaliteten.

For å finne tjenestekritikalitet, og med hvilken styrke de ulike sikkerhets, beredskaps, og personvernprinsippene skal implementeres for tjenesten, baserer RSB seg på fem grunnprinsipper og fire styringsprinsipper. Disse gir en veiledning på hvilke hensyn som bør vektlegges når man skal finnes tjenestekritikalitet og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres.

Basert på det ovennevnte kan man uttrykke RSB som en modell med fire lag, og grunn- og styringsprinsipper, se figur 3, *RSB i tjenesteperspektiv*, nedenfor. Modellen leses nedenifra og opp, og hvert lag baserer seg på det underliggende laget. I lag 4 er noen av prinsippene felles for konsument og tjenesteyter, mens andre er kun for konsument, og atter andre er kun for tjenesteyter. Grunn- og styringsprinsippene er gjennomgående i de fire lagene.

Figur 3, RSB i tjenesteperspektiv

Oppsummert kan det sies at jo mer kritisk en tjeneste anses å være, jo sterkere grad må sikkerhets- og beredskapsevnen være til stede både fra tjenesteyter og konsument. Dette for at tjenesten skal kunne leveres og konsumeneres på en trygg og sikker måte som forutsatt. Dette er også kjernen i RSB. Å finne tjenestekritikalitet, og basert på denne, finne hvordan man kan oppnå tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester.

Med dette som utgangspunkt kan RSB anses som en veiledning/kravsett på hvordan man kan oppnå nødvendig og tilstrekkelig sikkerhets- og beredskapsmessig evne både for tjenesteyter og konsument for å levere eller konsumere sikre og trygge digitale tjenester.

3.2.1 RSB sett fra konsumentens side

Det sentrale i RSB er leveranse og konsumering av digitale tjenester på en trygg og sikker måte. For konsumenten er det viktig å finne ut hvilke kritikalitet og innvirkninger tjenesten vil utgjøre for konsumentens virke. RSB bistår konsumenten med å finne kritikaliteten på tjenesten.

Videre må konsumenten ha tilstrekkelig sikkerhets- og beredskapsevne for å konsumenere tjenesten på en trygg og sikker måte. Basert på tjenestekritikalitet, må konsumenten derfor implementere ulike sikkerhets-, beredskaps-, og personvernprinsipper for å oppnå tilstrekkelig sikkerhets- og beredskapsevne. Disse vil sikre at konsumenten evner å konsumenere tjenesten på en trygg og sikker måte.

For konsumenten er lag 1, 2 og 3 viktig for å finne tjenestekritikalitet for tjenesten som skal konsumenere, samt prinsippene som gjelder for konsument i lag 4 for å oppnå tilstrekkelig sikkerhets- og beredskapsevne.

3.2.2 RSB sett fra tjenesteyters side

Basert på tjenestekritikalitet vil konsumenten stille krav innen sikkerhet, beredskap, og personvern til tjenesteyter slik at tjenesten leveres i forhold til avtale, lov, og forventning. Disse kravene vil tjenesteyter finne igjen som prinsipper i lag 4 basert på tjenestens kritikalitet.

Tjenesteyter må også gi input til konsument i forhold lag 1, 2, og 3. Dette for å komme frem til en felles konsensus om tjenestens innhold, kritikalitet og leveransekvalitet.

Tjenesteyter kan bruke RSB som konsument når tjenesteyter selv skal konsumenere digitale tjenester for sin egen tjenesteproduksjon fra andre underleverandører.

3.3 Hva baserer RSB seg på

Kommuner og fylkeskommuner er fortrolig/familiære med at det skal etableres styringssystem for informasjonssikkerhet og personvern. Det finnes allerede veiledere og standarder for etablering av slike systemer, eksempelvis ISO/IEC 27001/2. Det er derfor viktig å relatere regelverket og forklaringen av regelverket til noe som er praktisk knyttet til egen hverdag. Erfaringen fra kommunal sektor er at man vil følge retningslinjer, rutiner og lovverk, men at de komplekse og ressurskrevende å følge i en hektisk hverdag.

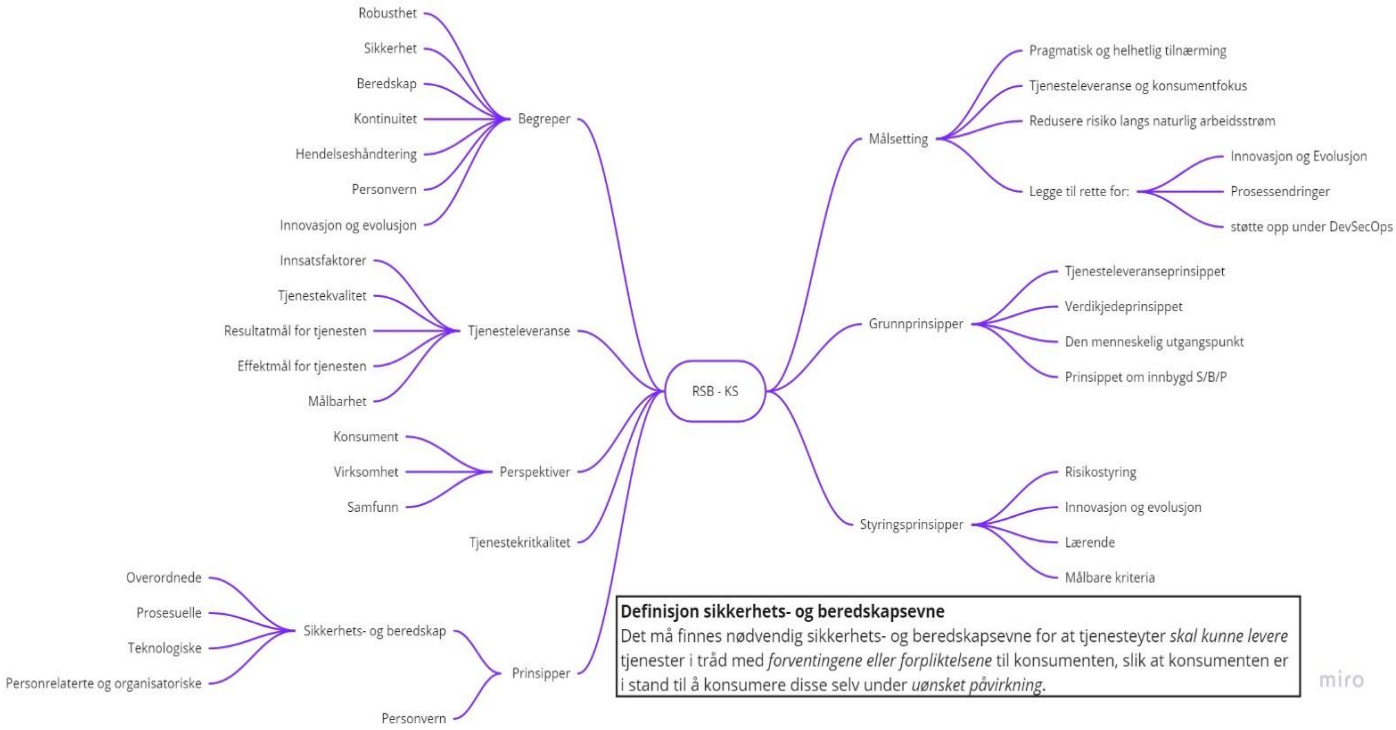
RSB prøver å forenkle et komplekst og krevende tema slik at det blir lettere og oppnå tilstrekkelig sikkerhets- og beredskapsevne for å kunne levere og konsumenere trygge og sikre digitale tjenester. RSB tar utgangspunkt i de strategiske føringene i en rekke standarder, lover, og prinsipper for å systematisere disse på slik måte at de kan følges og etterleves i en hektisk hverdag. RSB kombinerer teorier om forretnings- og leveranseprosesser med sikkerhets-, beredskaps-, og personvern prosesser.

RSB har tatt utgangspunkt i strategiske føringer fra en rekke standarder og prinsipper så som for eksempel:

- ISO27001 / ISO27002 / ISO27005 / ISO270031 / ISO270034 / ISO27035 / NS 5830
- ISO27701 - Security techniques for privacy information management.
- NSM sine grunnprinsipper.
- Nasjonale arkitekturprinsipper (Digitaliseringsdirektoratet), spesielt prinsipp 7.

- Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen).
- Krav til informasjonssikkerhet for skytjenester i offentlige anskaffelser[8].
- NIST.
- CIS Controls.
- Sabsa.
- HRO.
- Six Sigma.
- Lean.
- Med flere.

3.4 Oversikt over RSB



[8] https://www.anskaffelser.no/hva-skal-du-kjope/it/skytjenester-cloud/krav-til-informasjonssikkerhet.

4. Gjennomgang av elementene i RSB

4.1 RSB modellen

Som tidligere nevnt er kjernen i RSB å finne tjenestekritikalitet for å kunne dimensjonere tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester.

Nedenfor gjennomgås de enkelte elementene i RSB.

4.2 Grunnprinsipper

RSB basere seg på fire grunnprinsipper som gir veiledning på hvilke hensyn som bør vektlegges når man skal finne tjenestekritikalitet, og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres for å oppnå tilstrekkelig sikkerhets- og beredskapsevne:

- Tjenesteleveranseprinsippet.
- Verdikjedeprinsippet.
- Den menneskelig utgangspunkt – lov om minst mulig anstrengelse i tråd med innovasjon og evolusjon.
- Prinsippet om innbygd personvern, sikkerhet, og beredskap.

Grunnprinsippene som er skissert overfor inngår i ulike lag i RSB modellen og vil bli belyst ytterligere når de ulike lagene gjennomgås. Nedenfor gås det kort gjennom grunnprinsippene.

4.2.1 Tjenesteleveranseprinsippet

Tjenesteleveranseprinsippet handler om evnen til å levere og konsumenere tjenester i tråd med avtale, lov, eller forventninger. Det vil si om virksomheten og konsumenten har nødvendig sikkerhets- og beredskapsmessig evne til å levere og konsumenere sikre og trygge digitale tjenester. I den forbindelse er det avgjørende og finne tjenestekritikalitet. Tjenestekritikaliteten vil avgjøre hvilke sikkerhets- og beredskapsmessig evner som trengs for å kunne levere tjenesten på en trygg og sikker måte.

RSB legger til grunn at ansatte i Akson journal AS og kommunene har en felles forståelse av formålet, innholdet, og viktigheten av de tjenester som skal ytes av Akson journal AS. Dette vil være avgjørende for å kunne levere sikre og trygge tjenesteleveranser.

4.2.2 Verdikjedeprinsippet

Verdikjedeprinsippet handler om tjenesten inngår i en eller flere verdikjeder. Verdikjede[9] kan ses på som en sammenhengende «forsyningskjede» fra ulike virksomheter for å oppfylle en konsumentforespørsel. En verdikjede vil for eksempel kunne spenne over mange sektorer og flere land. En tjeneste vil dermed være en delmengde i en verdikjede.

Verdikjedeprinsippet ser på tjenestens betydning i ulike verdikjeder. Det må derfor komme tydelig frem hvilke kaskadevirkninger tjenesten vil få for konsumentene, det vil si kommunene og innbyggerne, hvis tjenesten blir utilgjengelig eller mister tillitt.

4.2.3 Den menneskelig utgangspunkt

Det menneskelig utgangspunkt tar utgangspunkt i adferdsøkonomi (Behavioral economics), beslutningstaking (Decision making), psykologi og kommunikasjon. RSB legger til grunn at Akson journal AS og kommunene har en klar formening om hvordan tjenesten vil påvirke den daglige arbeidsutførelsen til brukerne. Og i en forlengelse av dette, legger opp arbeidsflyten i tjenesten på en slik måte at den blir en naturlig del i arbeidsutførelsen.

[9] Se NOU 2015: 13 15, *Digital sårbarhet – sikkert samfunn* for mer informasjon om verdikjeder.

4.2.4 Prinsippet om innebygd sikkerhet, beredskap, og personvern

Prinsippet om innebygd sikkerhet, beredskap, og personvern innebærer at tjenesten skal ha innebygde mekanismer for å bistå brukerne med å ivareta sikkerhet, beredskap og personvern. Dette er spesielt viktig i forbindelse for å gjøre tjenesten mer robust, fjerne feilkilder, og redusere risiko for kompromittering av tjenesten eller arbeidsflyten.

4.3 Styringsprinsipper

En kritikalitetsvurdering av tjenesten vil gi en indikasjon på hvor kritisk tjenesten er.

Selv om tjenesten anses som svært kritisk er det ikke dermed sagt at samtlige av sikkerhets, beredskap, og personvern prinsipper skal implementeres for å oppnå god sikkerhets- og beredskapsmessig evne. Det må foretas en avveining i forhold til kost/nytte på hvilke sikkerhets, beredskaps-, og personvern prinsipper som bør implementeres. RSB inneholder styringsprinsipper som gir veiledning til hva som bør vektlegges ved implementering av sikkerhets-, beredskap, og personvernprinsippene.

RSB inneholder følgende styringsprinsipper:

- Risikostyring
- Innovasjon og evolusjon
- Læring
- Målbarhet

4.3.1 Risikostyring

Når det gjelder personvernprinsippene angir artikkel 35 i personvernforordningen når det skal foretas en personvernkonsekvensvurdering. Personvernforordningen er risikobasert. Det må derfor gjøres gode risikoanalyser i tråd med lovgivningen for å ivareta personvernet. For Akson innebærer det at kommunal sektor og Akson journal AS gjør gode risikoanalyser sammen slik at personvernet blir ivaretatt for å skape nødvendig tillitt hos innbyggerne.

Når det gjelder sikkerhets- og beredskapsprinsippene er ikke gitt at alle prinsippene vil være aktuelle. Det må gjennomføres en kost- og kvalitetsanalyse som munner ut i en risikoanalyse med en risikoaksept og restrisiko.

Naturligvis jo høyere kritikalitet på tjenesten, jo sterke styrke vil de ulike prinsippene slå inn. Som eksempel her kan nevnes at hvis man antar at systemet er svært kritisk, bør man gjennomføre kontinuerlige automatiske sikkerhetstester. Er systemer derimot ikke kritisk, trenger man ikke å gjennomføre denne type tester. På den annen side, selv om systemet er svært kritisk, betyr det ikke at man må gjennomføre kontinuerlige automatiske sikkerhetstester. Det kan hende at risikoappetitten er høy eller at det gjennomføres andre risikoreduserende tiltak, at det ikke er nødvendig å gjennomføre denne type tester.

Prinsippet ligger imidlertid fast, tjenestekritikalitet sett opp mot en kost-, kvalitet-, og risikoanalyse vil gi en retning på hvilke prinsipper som bør implementeres.

4.3.2 Innovasjon og evolusjon

Det vil komme ny teknologi på markedet, behovene, arbeidsprosessene, og organisering i kommunale helse- og omsorgstjenesten vil endre seg, og ikke minst vil det skje helsefaglig tjenesteutvikling og samfunnsendringer. Derfor det helt vesentlig at sikkerhet og beredskap ikke legger hindre for innovasjon og evolusjon, men heller søker å øke forenklings- og effektivitetsevne for helsepersonell.

Tjenesten, samt sikkerhets- og beredskapsprinsippene, må derfor designes og gjennomføres på en slik måte at de ikke hindrer innovasjon og evolusjon for tjenesteyter og konsument. De må tvert imot legge til rette og støtte opp under innovasjon og evolusjon.

RSB setter som styringskrav at innovasjon og evolusjon er vurdert i kost-, kvalitets-, og risikoanalyser og for hvert prinsipp som ønskes implementert.

4.3.3 Læring

RSB legger til grunn at den digitale verden er kompleks, ustabil, og uforutsigbar. RSB forutsetter derfor at både tjenesteyter og konsument har gode læringsprosesser spesielt rundt hendelseshåndtering, og av de ulike elementene i leveranse- og konsumentkjeden.

4.3.4 Målbarhet

RSB setter som styringskrav at effektene av sikkerhets-, beredskaps-, og personvern prinsippene som implementeres kan måles. Kost-, kvalitets-, og risikoanalyser sett opp mot tjenestekritikalitet vil gi indikasjoner på hvilke prinsipper innen sikkerhet, beredskap, og personvern som bør implementeres for å oppnå tilstrekkelig sikkerhets- og beredskapsevne.

Styringsprinsippet om målbarhet er gjennomsyret i hele RSB og ikke bare for prinsippene innen sikkerhet, beredskap, og personvern. RSB forutsetter at hvert tiltak eller handling som er av betydning har målbarhetsparametere for å forsikre at tjenestene leveres i tråd med avtale, lov, eller forventning.

4.4 Tjenesteleveranse (lag 1)

Første steg i RSB er å definere hvilke tjeneste(r) som skal leveres og konsumeres. I RSB defineres tjeneste som en leveranse en tjenesteytende virksomhet leverer, og som en konsument konsumerer. Tjenestebegrepet benyttes både om produkter og tjenester.

Tjenesten vil være satt sammen av innsatsfaktorer (innen dimensjonene mennesker, teknologi, og prosesser) hos tjenesteyteren for å oppfylle en konsumentforespørsel. Tjeneste i RSB er definert som et sluttprodukt som leveres av tjenesteyteren til konsumenten. I forbindelse med produksjon av en tjeneste kan denne bestå av mindre delleveranser fra ulike enheter internt/eksternt hos tjenesteyter. Delleveranser anses ikke tjenester i RSB sammenheng, men som en «komponent» inn i tjenesten.

Begrunnelsen for dette er at RSB har konsument- og samfunnsperspektiv. For en konsument er det irrelevant hvordan tjenesteyteren produserer, eller om det inngår delleveranser i tjenesten. For konsument er det viktigst å få sluttproduktet som konsument kan konsumere i tråd med avtale, lov, eller forventning. For tjenesteyteren er det imidlertid viktig å ha oversikt og kontroll over innsatsfaktorene og delleveransene. Dette er helt nødvendig for å sikre gode og robuste tjenesteleveranser. Ved å ha oversikt og kontroll over innsatsfaktorer og delleveranser vil man også kunne finne «enkelt feilpunkter» (single points of failure), avhengigheter, og andre faktorer som kan forstyrre tjenesteleveransen. Et annet aspekt er at det er viktig for tjenesteyteren å ha kunnskap om hva som skal til av innsatsfaktorer for å kunne levere robuste tjenester i tråd med avtale, lov, eller forventning.

I forbindelse med tjenesteleveranser i RSB gjør følgende to aspekter seg gjeldende:

- Innsatsfaktor.
- Tjenestekvalitet (kvalitetsnivå).

For å kunne levere en tjeneste av en viss kvalitet (tjenestekvalitet), må det finnes innsatsfaktorer som gjør det mulig å levere tjenesteleveransen. Tjenestekvalitet innebærer hvilken kvalitet tjenestene skal leveres til konsumenten. Det kan være en eller flere kvalitetsnivåer. Hva som ligger i de forskjellige kvalitetsnivåene vil kunne variere i henhold til avtale, lov eller forventning mellom partene.

Sammenheng mellom innsatsfaktorer og tjenestekvalitet vises i figur 5 nedenfor (kvalitetsnivåene bronse, sølv og gull er kun navneeksempler på tjenestekvalitet).

Tjeneste-leveranse	Tjenestekvalitet		
	Bronse	Sølv	Gull
	Innsatsfaktor 1		
	Innsatsfaktor 2	Innsatsfaktor 4	
	Innsatsfaktor 3	Innsatsfaktor 5	Innsatsfaktor 7
		Innsatsfaktor 6	Innsatsfaktor 8
			Innsatsfaktor 9

Figur 5, sammenheng mellom innsatsfaktorer og tjenestekritikalitet

I elementet tjenesteleveranse er fem faktorer som gjør seg gjeldene for konsument og tre for tjenesteyter.

For konsument gjelder følgende fire faktorer som må kartlegges:

1) Hvilke tjenester skal mottas og i hvilke kvalitet, hva de skal utrette, og hvilke gevinster tjenesten skal gi (resultat- og effektmål).
2) Om tjenesten støtter opp under naturlig arbeidsflyt.
3) Om tjenesten vil bidra til forenkling, automatisering, forbedring, og en god brukeropplevelse.
4) Avhengigheter og andre kritiske faktorer som kan medføre at tjenesten kompromitteres eller mister tillitt.
5) Målbare indikatorer for å bekrefte om tjenesten utretter det den skal, gir antatt gevinst, og understøtter konsumentens virke.

For tjenesteyter gjelder følgende tre faktorer som må kartlegges:

1) Hvilke innsatsfaktorer som skal til å kunne levere tjenesten med en gitt kvalitet.
2) Avhengigheter og andre kritiske faktorer som kan medføre at tjenesten kompromitteres eller mister tillitt.
3) Målbare indikatorer for å bekrefte om leveransen er i tråd avtale, lov, eller konsumentens forventning.

Det er viktig at konsumenten og tjenesteyteren har en felles forståelse av hva tjenesteleveransen innebærer, hvilke kvalitet denne skal leveres i, hvilke robusthet tjenesten skal ha, og ikke minst hvordan den skal leveres. Det er derfor viktig at kommunal sektor og Akson Journal AS har en felles forståelse og konsensus på hva som er tjenesteleveransen og innholdet i denne.

4.5 Perspektiver (lag 2)

Første steg i RSB handler om at konsumenten og tjenesteyteren har en felles forståelse og konsensus om tjenesten, og hva tjenesteleveransen innebærer. Steg to i RSB handler om å vurdere føringene som ligger i virksomhets-, konsument- og samfunnsperspektivet. Perspektivene gir input til kritikalitetsvurderingen, og i neste omgang sikkerhets-, beredskaps-, og personvernprinsippene.

Nedenfor gjennomgås disse perspektivene.

4.5.1 Virksomhetsperspektivet

Virksomhetsperspektivet handler om tjenesteyter. Tjenesteyter må ha en robust virksomhet som evner å levere avtalte tjenester. Det innebærer blant annet at tjenesteyter må pålitelighet ved utførelse av komplekse oppgaver under tidspress, samt ha lav forekomst av ulykker, avbrudd og feiltoleranse gjennom flere år. Jo høyere kritikalitet på tjenesten, jo høyre krav til robusthet for tjenesteyter og pålitelighet for tjenesten.

I virksomhetsperspektivet ligger det vurdering av leveranse- og modenhetsevne til tjenesteyter:

- Om tjenesteyter og dens ansatte forstår tjenesteleveransen og verdikjeden og har nødvendig modenhet for å levere tjenesten.
- Om tjenesteyter har en organisasjonskultur som legger til rette for læring, samhandling og korreksjon.
- Om nødvendige kommunikasjonslinjer mellom tjenesteyter og samarbeidspartnere er opprettet.

- Om det er felles konsensus om tjenesteleveransens viktighet for konsumenten mellom tjenesteyter og tjenesteyters samarbeidspartnerne.
- At tjenesteyter forutsetter at feil vil skje, men forstår verdikjeden og tjenesteleveransen og kan derfor håndtere selv det uventede. Dette for å påse at tjenesten leveres kontinuerlig i tråd med avtale, lov og forventning.

4.5.2 Samfunnsperspektivet

Den teknologiske utviklingen og integrerte informasjonssystemer bidrar til økt samvirke og mer effektive tjenester. Samtidig fører dette med seg avhengigheter mellom konsumenter og tjenesteytere, mellom tjenesteytere, mellom konsumenter, og samfunnet med det resultat at man i praksis kan se på mange delsystemene som et stort hele med innbyrdes varierende grad av kritikalitet.

Den overordnet målsetting for Akson er å tilrettelegge for bedre samvirke i helsesektoren, med mer tidseffektive og tidsriktige løsninger for å løse de utfordringer som helsesektoren står ovenfor. Det underliggende spørsmålet er derfor hvilke kaskadeeffekter det vil få for konsument, samfunnet, tjenesteyter, samarbeidspartnere, og innbyggerne hvis man for eksempel tenker seg at tjenesten blir kompromittert (for eksempel integriteten, tilgjengeligheten, konfidensialiteten, eller kvalitet), eller at tillitt til systemet bortfaller i ulik grad.

I samfunnsperspektivet ligger det vurdering av kaskadevirkninger og kost/gevinstberegninger:

- Hvilke kaskadeeffekter det vil få for konsument, samfunnet, samarbeidspartnere, innbyggerne og verdikjedene hvis tjenesten blir kompromittert eller at tillitt til tjenesten bortfaller i ulik grad.
- Om det finnes alternative tjenester eller prosesser (og på hvilket nivå), for å opprettholde konsumentens virke i den perioden tjenesten er bortfalt eller tillitten til tjenesten er lav.
- Om tjenesten lar seg reetablere og i hvilken grad hvis kompromitteringen er fatal.

4.5.3 Konsumentperspektivet

Konsumentperspektivet (for Akson vil dette både være kommunene og innbyggerne) handler om konsumentens mulighet til å konsumere tjenesten i forhold til avtale, lov, og forventning.

Selv om kritikaliteten og sensitiviteten til informasjonen vil variere, må konsumenten forvente at informasjon håndteres i tråd med avtale, lov, og forventing. I tillegg er det viktig at konsumenten selv evner å levere sine tjenester ved å konsumere tjenesteyters tjenester. Poenget er at tjenesten må leveres og bygges på en slik måte at konsumenten faktisk er i stand til å konsumere disse med positivt utfall, og ikke bare få «levert» tjenesten.

I konsumentperspektivet ligger hvilken grad konsumenten kan nyttiggjøre seg av tjenesten:

- Om tjenesten er bygd og levert slik at konsumenten evner å konsumere tjenesten med positivt utfall.
- At informasjonen håndteres på en trygg måte både i forhold til informasjonsbehandlingen og ivaretakelse.
- At tjenesten er endringsdyktig i tråd med konsumentsbehov, følger teknologi- og samfunnsutviklingen, og legger til rette for innovasjon og evolusjon for konsumenten.
- At konsumenten forstår tjenesteleveransen og har nødvendig modenhet for å nyttiggjøre seg av denne.

4.5.4 Oppsummering perspektivene

Formålet med perspektivene er å gi generell input for å finne kritikalitet til en tjeneste. Perspektivene er ikke uttømmende, og det vil være andre vurderingskriteria avhengig av tjenestetype.

4.6 Tjenestekritikalitet (lag 3)

Første steg i RSB er å kartlegge tjenester. Andre steg er å gå gjennom perspektivene for å gi input til kritikalitetsvurderingen. Tredje steg i RSB er å finne ut hvilken kritikalitet en tjeneste har. Dette er helt nødvendig å finne ut hvilken kritikalitet tjenesten representerer for konsument, tjenesteyter, og samfunnet som sådan.

Fra konsumentens ståsted er viktig og finne ut hva tjenesten betyr for konsumentens virke og oppdragsutførelse, samt hvilke prosessøkonomiske konsekvenser tjenesten representerer hvis tjenesten blir utilgjengelig eller at tillitten til den bortfaller (for eksempel på grunn av at integriteten i systemet er brutt). I forhold til Akson betyr det å finne ut hvor viktig felles kommunal journal er for kommunen(e), og hvilke prosessøkonomiske konsekvenser dette vil gi kommunen(e) hvis løsningen er utilgjengelig eller mister tillitt.

For tjenesteyter blir det viktig å finne ut hva det vil innebære hvis tjenesteyter ikke evner å levere tjenesten, eller at tillitt til tjenesten bortfaller. For Akson journal AS betyr det å finne ut hvilke innsatsfaktorer er nødvendig for å oppfylle tjenesteleveransen, avhengigheter, og andre kritiske faktorer. Og videre, hvordan innsatsfaktorene skal beskyttes for å opprettholde nødvendig robusthet i kontinuerlig tjenesteleveranse.

Fra et samfunnsperspektiv blir det også viktig å kartlegge kaskadevirkningene av at tjenesten blir utilgjengelig, eller at den mister tillitt. For eksempel at persondata kommer på avveie. Eller at personene som skal inn til behandling ikke får nødvendig behandling fordi tjenesten er utilgjengelig. Eller at integritet til data er brutt og man ikke lenger kan stole på innholdet. For Akson journal AS og kommunene betyr det å finne ut hva det innebærer for samfunnet og innbyggerne at felles journalløsning ikke er tilgjengelig eller har mistet tillitt. Og i forlengelse av dette, om det finnes alternativer (for eksempel gjennom manuelle rutiner) som fortsatt kan bidra til å opprettholde en viss grad av kommunenes virke og forpliktelser.

Å finne kritikalitet på tjenesten er en viktig del av RSB. Hvis man ikke har en fellesforståelse og konsensus av kritikalitet mellom konsument og tjenesteyter, da vil det være vanskelig å dimensjonere robusthet og leveransekrav til tjenesten. For at tjenesteyter og konsument skal ha samme forståelse til tjenestekritikalitet bidrar RSB med en veiledning på hvordan man kan regne ut kritikalitet til en tjeneste. Dette gjøres ved å sette score fra 0 – 5 på 20 elementer av konsumenten og tjenesteyter i samarbeid, se tabellene nedenfor.

Kategori	Kritikalitetselement	Beskrivelse
Vurderes av konsument		
Informasjon	**Tilgjengelighet**	Maksimal utilgjengelighet. Jo kortere tid som aksepteres, jo høyere score.
	Integritet	Om man kan stole på de data som ligger i systemet. Jo mindre avvik som aksepteres, jo høyere score.
	Konfidensialitet	Andel av data som kan komme på avveie eller blir tilgjengeliggjort for uvedkommende. Jo mindre avvik som aksepteres, jo høyere score.
	Autentisitet (identifikasjon)	Ektheten til data og tjenester samt opprinnelse. Jo mindre avvik som aksepteres, jo høyere score.
	Kvalitet	Om data skal brukes som beslutningsdata. Jo større krav til at data skal være beslutningsdata, jo høyere score.
	Tillitt (pålitelighet)	Grad av tillitt til tjenesten. Jo høyre grad av tillitt som kreves, jo høyere score.
	Sporbarhet	Krav til sporbarhet for data og transaksjoner. Jo større krav til sporbarhet, jo høyere score.
	Persondata	Krav til behandling av personopplysninger. Jo større krav til sikring av personopplysninger, jo høyere score.
Leveranse	**Funksjon**	Om hvor viktig eller avgjørende tjenesten er for konsumentens arbeidsutførelse. Jo mer viktig/avgjørende tjenesten anses å være, jo høyere score.
	Alternativer	Om det finnes alternativer til å opprettholde konsumentens virke og forpliktelser ved bortfall av tjenesten. Jo færre alternativer, jo høyere score.
	Avtaleverk	Om avtalen oppfyller tjenesteleveransens formål og krav. Jo dårligere oppfyllelse, jo høyere score.

	Leveringsevne	Om benyttede leverandører/tjenesteyter har tilstrekkelig overlevelsesevne. Jo mindre overlevelsesevne, jo høyere score.
	Modenhet tjenesteyter	Om tjenesteyter er moden til å levere tjenesten. Jo større krav til modenhet, jo høyere score.
	Modenhet konsument	Om konsument er moden til å konsumenere tjenesten. Jo større krav til modenhet, jo høyere score.
Teknologi og ressurser	**Teknologisk modenhet**	Om teknologien som er tenkt valgt er agil, skalerbar, åpen, utskiftbar, fremtidsrettet og levedyktig. Jo mindre teknologisk modenhet, eller større krav til teknologisk modenhet, jo høyere score.
	Kompetanse	Om det finnes mye kompetanse/ressurser på produkter/tjenester. Jo mindre tilgjengelig kompetanse, jo høyere score.
Økonomi	**Kostberegning**	Det gjennomføres en kostnadsutregning for bortfall av tjenesten (økonomi, liv/helse, kaskadeeffekt mv) for konsument og samfunn. Jo høyere kost, jo høyere score.
Vurderes av tjenesteyter i samarbeid konsument		
Prosess	**Kontrollerbarhet**	Om hvor kontrollerbar tjenesteleveransen er fra produksjon til konsum. Jo mer krav til kontroll, jo høyere score.
	Avhengigheter	Om tjenesten har avhengigheter og andre kritiske faktorer som er en forutsetning for leveransen. Jo flere avhengigheter/kritiske faktorer, jo høyere score.
	Økonomisk tilfang	Om tjenesten vil få økonomisk tilfang slik at den at den kan leveres med ønsket resultat og funksjonsevne i tjenestens livsløp. Jo større usikkerhet til økonomisk tilfang, jo høyere score.

Når det gjelder elementet økonomisk tilfang er det viktig å understreke at hvis tjenesten ikke sikres økonomisk tilfang i tjenestens livsløp, anses dette til å være så kritisk for tjenesten at det bør revurderes om den bør igangsettes.

Etter at man har satt score mellom 0 – 5 på hvert enkelt element vil man få en totalscore mellom 0 – 100 for tjenesten. Hva det betyr kan man lese ut av veiledningstabellen for kritikalitetsskala nedenfor.

Kritikalitetsskala		**Beskrivelse**
For elementene	**For tjenesten**	
5	81 – 100	Svært kritisk
4	61 – 80	Kritisk
3	41 – 60	Mindre kritisk
2	21 – 40	Noe kritisk
1	1 – 20	Ikke kritisk
0	0	Ikke relevant

Kritikalitetsmetodikken i RSB benyttes både av konsumenten og tjenesteyter. For konsumenten å finne ut hvor kritisk tjenesten er for konsumentens funksjonsevne. For tjenesteyter å finne ut hvor robuste innsatsfaktorene må være for å kunne levere kontinuerlig trygge og sikre tjenester.

Det er derfor vesentlig at kommunal sektor og Akson Journal AS har en felles forståelse og konsensus av kritikalitet til tjenester som skal leveres. Kritikalitetsvurderingen kan anses som et grunnleggende kravsett på hvor robust tjenesten må være i forhold til leveranse og konsum.

4.7 Sikkerhets-, beredskaps-, og personvernprinsipper (lag 4)

Fjerde steg i RSB er å avgjøre hvilke av sikkerhets-, beredskaps, og personvernprinsipper som bør innføres for å gi tilstrekkelig sikkerhets- og beredskapsevne for å levere tjenesten på en trygg og sikker måte.

For å ivareta informasjonssikkerhet må sikkerhetsdimensjonene fysisk sikkerhet, logisk sikkerhet (herunder psykologisk sikkerhet), og teknologisk sikkerhet være til stede. I RSV versjon 1.0 fokuseres det hovedsakelig på logisk og teknologisk sikkerhet.

4.7.1 Begreper i RSB

RSB bruker flere begrep for å beskrive innholdet i prinsippene for sikkerhet, beredskap, og personvern. I den videre fremstillingen går man først gjennom begrepsapparatet som blir brukt i prinsippene, deretter forholdet mellom begrepene, og til slutt selve prinsippene. Denne tilnærmingen er gjort da det gir en bedre bakgrunn for å forstå prinsippene og formålet med RSB. Prinsippene må leses med bakgrunn i begrepsapparatet.

RSB benytter følgene begreper:

- Robusthet.
- Sikkerhet.
- Beredskap.
- Kontinuitet.
- Hendelseshåndtering.
- Personvern.

Nedenfor gjennomgås de ulike begrepene i RSB.

7.5.1.1 Robusthet i tjenesteleveransen

RSB skal bidra til å oppnå tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester. RSB har fokus på tjenesteleveranser. RSB handler derfor ikke om sikkerhetsstyring på virksomhetsnivå eller operativ sikkerhetshåndtering.

Sikkerhetsstyring på virksomhetsnivå handler om hvordan man skal arbeide med informasjonssikkerhet i et virksomhetsperspektiv. Det vil si styringssystemer, ledelsens gjennomgang, og sikkerhetsorganisering med videre. Operativ sikkerhetshåndtering handler om hvordan man operasjonaliserer og effektuerer ulike tiltak. For eksempel være patching, overvåking av systemer, teknisk sikkerhetsarkitektur med videre. Selv om RSB først og fremst har fokus på tjenesteleveranser, vil RSB kunne være dimensjonerende for sikkerhetsstyring og sikkerhetshåndtering. eller sikkerhetshåndteringen. Dette fordi kritikaliteten til tjenesten kan gi utslag i dimensjonering av sikkerhetsstyring og sikkerhetshåndtering.

I RSB defineres sikkerhets- og beredskapsevne på denne måten:

Det må finnes nødvendig sikkerhets- og beredskapsevne for at tjenesteyter *skal kunne levere* tjenester i tråd med *forventingene eller forpliktelsene* til konsumenten, slik at konsumenten er i stand til å konsumere disse selv under *uønsket påvirkning*.

Med utgangspunkt i den ovennevnte definisjonen inneholder den tre perspektiver og fire grunnelementer. Disse kan man lese ut av det som er skrevet i kursiv.

De tre perspektivene er (for mer informasjon om perspektivene se kapittel 4.5):

- Virksomhetsperspektivet
- Samfunnsperspektivet
- Konsumentperspektivet

De fire grunnelementene er:

- Sikkerhet
- Beredskap og kontinuitet
- Personvern
- Innovasjon og evolusjon

I ordene *skal kunne levere* ligger virksomhetsperspektivet og grunnelementet sikkerhet. I ordene *forventingene eller forpliktelsene* ligger konsumentperspektivet og grunnelementene personvern, innovasjon og evolusjon. I ordene *uønsket påvirkning* ligger samfunnsperspektivet og grunnelementene beredskap og kontinuitet. Det er viktig å understreke at grunnelementene og perspektivene er uavhengig av hverandre og flere grunnelementer kan inngå i et perspektiv.

I perspektivene og grunnelementene ligger det implisitt et viktig grunnelement som går gjennom alle perspektivene og grunnelementene – hendelseshåndtering. Det vil før eller siden skje hendelser uavhengig av hvor god sikkerhet, beredskap og personvern man har. Det er derfor helt avgjørende at man evner å håndtere hendelser for å opprettholde gode, trygge og sikre tjenesteleveranser. Hendelseshåndtering er derfor en viktig del av RSB.

7.5.1.2 Begrepet sikkerhet

Tjenesteleveranseperspektiv i RSB har både en konsument- og tjenesteytendeside. Konsumenten forutsetter at tjenesten leveres som avtalt eller forventet fordi konsumenten selv er avhengig av tjenesten for å gjennomføre sitt virke. Tjenesteyteren på sin side må forholde seg til alle typer avvik som kan forstyrre tjenesteleveransen, uavhengig hvilke merkelapper man ønsker å sette på hendelsene.

Med utgangspunkt i det ovennevnte kan man oppsummer leveranseevnen på følgende måte:

1) Tjenesteyters evne til å kunne levere tjenesten.
2) Tjenesteyters evne til å skape tillit til tjenesteleveransen og mellom partene.
3) Konsumentens evne til å konsumere tjenesten i en positiv kontekst. Det vil si om det er knyttet positivitet til bruk av tjenesten for konsumenten. Det vi si at tjenesten ikke oppleves som en hinder i konsumentens naturlige arbeidsflyt, innovasjon og evolusjon.

En tjenesteleveranse vil kunne forstyrres av mange typer avvik. Tjenesteyter må derfor ha en evne til å håndtere ulike hendelser, herunder sikkerhetshendelser. Det vi si at en tjenesteyter må ha nødvendig og tilstrekkelig sikkerhetsmessig evne til å levere tjenesten ved å beskytte innsatsfaktorene, tiltak mot avbrudd, samt ha nødvendig kapasitet for å håndtere hendelser.

I en slik kontekst defineres begrepet sikkerhet i RSB som ulike risikoreduserende tiltak for å oppnå en tilstrekkelig sikkerhetsevne for å kunne levere digitale tjenester kontinuerlig i henhold til avtale, lov, eller en forventning.

7.5.1.3 Begrepene beredskap og kontinuitet

7.5.1.3.1 Beredskap

Beredskap[10] betyr i utgangspunktet «å være beredt». Beredskap betyr at man har dimensjonert seg på slik måte at hvis en uønsket hendelse inntreffer og som krever ressurser utover normal drift skal man kunne håndtere denne på en effektiv måte. Dette for å redusere risikoen for tjenestens utilgjengelighet, og opprettholdes av funksjonsevnen.

God beredskap er avgjørende for å opprettholde trygge og sikre tjenesteleveranser. Kvalitet, læringsevne, evne til kontinuerlig forbedring av organisasjon, teknologi, prosesser, og kompetent personell på alle nivå i organisasjonen er derfor nøkkelfaktorer for å kunne lykkes med god beredskap. Robuste

[10] DSB sin veileder til forskrift for kommunal beredskapsplikt, jf også NOU 2000:24 Et sårbart samfunn, NOU 2006:6 Når sikkerheten er viktigst.

beredskapsorganisasjoner har gode prosesser og kompetent personell for å håndtere krevende og kompliserte situasjoner som kan strekke seg over lengre tidsperioder.

RSB baserer seg på de nasjonale beredskapsprinsippene om ansvars, likhet, nærhet og samvirke. Prinsippene innebærer at det er den ordinære linjen som er fundamentet i beredskapsarbeidet, og at risikodempende tiltak i størst mulig grad skal håndteres som linjeaktiviteter. Samtidig har alle i virksomheten et selvstendig ansvar for å sikre best mulig samvirke med andre interne og eksterne relevante aktører, organisatoriske enheter og virksomheter. Innen beredskap vil det finnes ulike beredskapsnivåer, f.eks. grønn (nivå 0), gul (nivå 1), oransje (nivå 2), og rød (nivå 3) og så videre avhengig av hendelseskritikalitet.

7.5.1.3.2 Kontinuitet

Med kontinuitet menes en uavbrutt sammenheng. En virksomhet eller dets konsumenter er i stor grad avhengig av IKT-systemer, og i mange tilfeller er det IKT-systemene som muliggjør virksomhetens eksistens.

Kontinuitetsstyring i RSB har to dimensjoner. Den ene dimensjonen er hvordan man benytter sikkerhet for å opprettholde kontinuitet i normal tjenesteproduksjon.

Det andre dimensjonen er hvordan man hurtigst mulig gjenopptar tjenesteleveranser etter en større feil eller katastrofe. Dette for at tjenesteyter raskest mulig skal være i stand til å gjenoppta sin normale virksomhet og leveranse av tjenester. Kontinuitetsstyring skal bidra til å sikre virksomhetens funksjonsevne, og i forlengelse av dette, omdømme, merkevare, interesser og tjenester. Kontinuitetsstyring skal også bidra til at konsumenten får gjennomført sine leveranser slik at kaskadevirkningen blir minst mulige.

I RSB refereres kontinuitetsstyring til den andre dimensjonen. Det vil si gjenoppretting. Det innebærer at man gjennom kontinuitetsstyringen skal gjenopprette tjenesteleveransen raskest mulig for å kunne tilby kontinuerlige trygge, sikre og pålitelige digitale tjenester til konsumenten.

7.5.1.4 Kort om hendelseshåndtering

Uavhengig av hvor god sikkerhet, beredskap, og personvern man har, og uavhengig av hvor mange risikoreduserende tiltaks som gjennomføres, vil det skje uønskede hendelser.

Det er ikke praktisk mulig å forhindre alle hendelser. Som en del av risikohåndteringen etableres det derfor tiltak som har til hensikt å oppdage uønskede hendelser (enten tilsiktede eller utilsiktede), og for å håndtere og redusere konsekvensene av disse. Hendelseshåndtering handler om evnen til å kunne oppdage og håndtere hendelsen ved hjelp av teknologiske, organisatoriske, og personelle tiltak.

I RSB anses hendelseshåndtering som en svært viktig komponent for å kunne opprettholde tjenesteyterens og konsumentens funksjonsevne. RSB legger videre systematikken rundt hendelseshåndtering tett opp til drifts-, forvaltnings-, sikkerhets-, og beredskapsplanverk, slik at man benytter samme begrepsapparat for alle dimensjoner av tjeneleveransen for å fjerne eventuelle misforståelser i leveransekjeden.

7.5.1.5 Begrepet personvern

Personvern[11],[12] anses som en ivaretakelse av personlig integritet. Det vil si ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. Personvern blir knyttet til retten til å ha en egen private sfære som man selv kontrollerer, ytringsfrihet, og det å kunne operer som et selvstendig individ.

Personopplysningsvern har ivaretakelse av personvern som hovedmål, og handler om å ha regler og standarder for behandling og oppbevaring av persondata. Regelens formål er å sikre enkeltindividers oversikt

[11] https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/
[12] https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/id1373/

og kontroll over behandling av opplysninger om dem selv. Personopplysningsvern blir knyttet til muligheten til selv å kontrollere hvordan, når, hvor mye, og hvilken informasjon om seg selv kan spres til andre aktører/entiteter. I hverdagen brukes gjerne personvern om personopplysningsvern, og da spesielt i forhold til General Data Protection Regulation (GDPR).

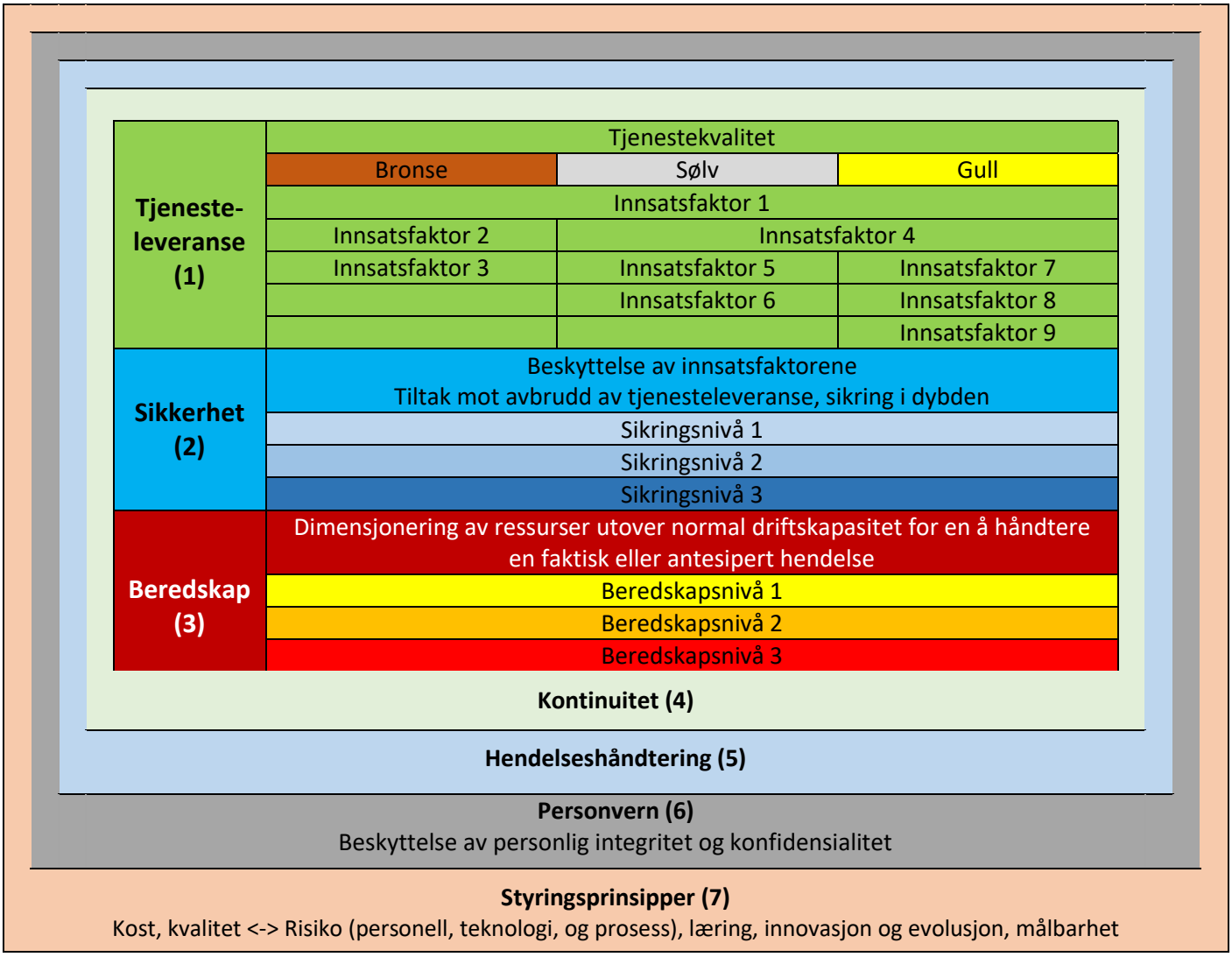
Akson kommer til å samle store mengder av persondata, herunder sensitiv helsedata. Personvernet skal sikre behandlingen av persondata, slik at individers integritet og privatliv ikke krenkes. Derfor er registrertes tillitt til tjenesten helt avhengig av at persondata data håndteres i tråd med lov og registrertes forventninger.

For å forenkle fremstillingen bruker RSB begrepet personvern som et samlebegrep om beskyttelse av personlig integritet og konfidensialitet i tråd med personvernlovgivningen.

Med personlig konfidensialitet menes at informasjonen til registrerte behandles fortrolig, lovlig, og riktig med et klart definert formål. I dette ligger det også at det er åpenhet om formålet og hvordan registrertes informasjon håndteres. Med personlig integritet mens ansvarlighet og ivaretakelse av registrertes rettigheter slik at rettsikkerheten og den personlige sfæren til registrerte er ivaretatt.

7.5.1.6 Sammenhengen mellom tjenesteleveranse og begrepene i RSB

Ovenfor har vi gått gjennom sentrale begreper i RSB. Sammenhengen mellom begrepene illustreres med figur 6, *sammenheng mellom begreper*, nedenfor. Figuren leses innen ifra og ut med tjenesteleveranse som startpunkt.



Figur 6, RSB, sammenhengen mellom begreper

Nedenfor følger en forklaring på sammenheng mellom begreper i RSB.

(1) Tjenesteleveranse:

1) En tjenesteleveranse er ofte inndelt i ulike tjenestekvaliteter. Navnet på tjenestekvalitetene vil variere avhengig av sektor og bransje. For å kunne levere en tjeneste i en viss kvalitet må det finnes ulike personelle, teknologiske, og prosessuelle innsatsfaktorer.
2) Innsatsfaktorene må dimensjoneres slik at tjenesteyter evner og levere sammenhengende digital tjeneste i tråd med avtale, lov, eller forventning til konsumenten.

(2) Sikkerhet:

3) Det må finnes nødvendig sikkerhet (risikoreduserende tiltak) for å beskytte innsatsfaktorene, og mot avbrudd i tjenesteleveransen.
4) Sikkerhet gjennomføres ved sikring i dybden gjennom ulike sikringsnivåer, slik som f.eks. sikringsnivå 1, 2 og 3 osv. Innholdet i sikringsnivåene vil avhenge av tjenestekritikalitet sett opp imot tjenestekvalitet og risiko.

(3) Beredskap:

5) I noen situasjoner vil ikke sikkerhet eller innsatsfaktorene være nok til å opprettholde tjenesteleveransen. Man må derfor gjennom beredskap dimensjonere seg på slik måte at hvis en uønsket hendelse inntreffer (enten faktisk eller antesipert) og som krever ressurser utover normal drift/forvaltning, kan håndteres på en effektiv måte.
6) Beredskapen vil inneholde ulike beredskapsnivåer avhengig av tjenestekritikalitet sett opp imot tjenestekvalitet og risiko.

(4) Kontinuitet:

7) Uansett hvor mye man sikrer seg vil det inntreffe større feil av «katastrofal» art.
8) Man må derfor ha en kontinuitetsstyring for å sikre og funksjonsevne både for seg selv og de som er avhengig av tjenesten. Dette for å være i stand til å gjenoppta normal drift og leveranser av tjenester raskest mulig.

(5) Hendelseshåndtering:

9) Hendelseshåndtering handler om hvordan man skal oppdage og håndtere hendelser.
10) Uavhengig av hvor god sikkerhet, beredskap, og antall risikoreduserende tiltaks som gjennomføres, vil det skje uønskede hendelser som driftsavbrudd, sikkerhetsbrudd og andre avvik. Derfor må det finnes metoder for varsling, analyse/mobilisering, sikring/respondering, gjenoppretting og normalisering innen samtlige dimensjoner av tjenesteleveransen.

(6) Personvern:

11) Innen dimensjonene tjenesteleveranse, sikkerhet, beredskap, kontinuitet og hendelseshåndtering vil det behandles persondata av ulik karakter og sensitivitet.
12) Personvern må sørge for beskyttelse av personlig integritet og konfidensialitet. Det må derfor finnes metodikk som ivaretar behandling av personrelatert data i tråd med lov og forventning.

(7) Styringsprinsipper:

13) Se kapitel 4.3, *Styringsprinsipper*, for mer informasjon.

RSB tar utgangspunkt i ovennevnte modell som et bakteppe når man skal vurdere ulike sikkerhets-, beredskaps- og personvern prinsipper i tråd med tjenestens kritikalitet.

4.7.2 Sikkerhets-, beredskaps-, og personvernprinsipper

Når kritikalitetsvurdering av tjenesten er foretatt vil det gi en indikasjon på hvor kritisk tjenesten er. Tjenestekritikaliteten sett opp mot en kost-, kvalitets-, og risikoanalyse vil gi en retning på hvilke sikkerhets-, beredskaps-, og personvern prinsipper bør implementeres.

Når det gjelder personvernprinsippene er disse direkte lovhjemlet gjennom personvernlovgivningen. Lovgivningen gir også anvisning på hva som ligger i de ulike personvern prinsippene og hvordan de skal forstås.

Når det gjelder sikkerhets-, beredskaps-, og kontinuitetsprinsipper må det i stor grad søkes i faglitraturen, standarder, og ulik lovgivning.

Ved utvikling, forvaltning, og bruk skal det være helhetlig tilnærming til både personvern (brukersiden/registrerte), sikkerhet (redusere risikoen for hendelser), og beredskap (evne til å gjenopprette eller alternativ oppgave gjennomføring). RSB skal bidra til at kommunale virksomheter og Akson journal AS gjennom implementering av prinsippene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på en forsvarlig og trygg måte.

Noen av sikkerhets-, beredskaps, og personvern prinsippene vil kun gjelde for konsument, andre for tjenesteyter, og atter andre for begge. Selv om et prinsipp gjelder for begge, betyr ikke det at begge skal oppfylle det i samme grad eller på samme måte. Det kan hende at konsumenten skal kun gi input til tjenesteyter og visa versa. Eller at konsumenten skal se prinsippet i forhold til sin funksjonsevne, mens tjenesteyter skal se prinsippet i forhold til sikring av den digitale plattformen. Hvilken styrke prinsippene skal implementeres med vil avhenge av kost-, kvalitets-, og risikovurderingene sett opp mot kritikalitet for tjenesten.

Nedenfor gjennomgås de ulike sikkerhets-, beredskaps-, og personvern prinsippene på et overordnet nivå.

7.5.2.1 Personvernprinsipper

EUs personvernforordning artikkel fem oppstiller personvernprinsipper. All behandling av persondata må skje i samsvar med disse. Prinsippene er basert på tanken om at behandling av persondata skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltpersoner. For ytterligere informasjon henvises det til personvernforordningen.

Som tidligere nevnt er dataeierskapet i Akson er kompleks og det bør nedsettes en egen arbeidsgruppe som bør se på problematikken rundt behandlingsansvaret. På det stadiet som prosjektet er i nå, vil personvernprinsippene både gjelder for Aksjon journal AS og kommunene. Nedenfor gjennomgås personvernprinsippene, og de må leses med dette som bakteppe.

Lovlighet, rettferdighet og åpenhet: Prinsippet om lovlighet innebærer at behandlingen av personopplysninger må ha et rettslig grunnlag etter EUs personvernforordningen eller eventuelt særlovgivningen. Prinsippet om rettferdig behandling innebærer bl.a. at den registrerte ikke må forskjellsbehandles. Prinsippet om at behandlingen skal være åpen, betyr at den skal være oversiktlig og forutsigbar for den registrerte, slik at vedkommende er i stand til å ivareta sine egne interesser og rettigheter. I åpenhet ligger det også at det må være enkelt for den registrerte å ta kontakt for å få mer informasjon om løsningen, dette skal bidra til tillit og at den registrerte lettere kan ivareta sine rettigheter.

Formålsbegrensning: I formålsbegrensning ligger at persondata bare kan behandles for spesifikke, uttrykkelig angitte og berettigede formål.

Dataminimering: Prinsippet om dataminimering henger tett sammen med formålsbegrensningsprinsippet. I dette ligger at den dataansvarlige skal begrense mengden av persondata til det som er relevant og nødvendig for å oppnå det konkrete formålet.

Riktighet: Prinsippet om at persondata som behandles skal være korrekte. Det skal treffes ethvert rimelig tiltak for å sikre at persondata som er uriktige med hensyn til formålene de behandles for, uten opphold slettes, eller rettes.

Lagringsbegrensning: Prinsippet om at persondata skal slettes når formålet de ble samlet inn for er oppnådd.

Integritet og konfidensialitet: Prinsippet om integritet betyr at persondata som behandles må være korrekte, gyldige, fullstendige, og sikres mot utilsiktet eller uautorisert endring eller sletting. Prinsippet om konfidensialitet handler om å sikre at persondata bare er tilgjengelige for de som rettmessig skal ha tilgang til dem.

Ansvarlighet: Prinsippet om ansvarlighet understreker at den dataansvarlige er den ansvarlige for at behandlingen oppfyller personvernprinsippene, og at den registrertes rettigheter og friheter blir ivaretatt.

Ivaretakelse av den registrertes rettigheter: EUs personvernforordning kapittel III oppstiller de rettigheter den registrerte har etter personvernregelverket når persondata samles inn og behandles om enkeltpersoner. Den registrertes rettigheter står sentralt i forordningen, og en av hovedbegrunnelsene for reguleringen er å sikre at den enkelte får bedre kontroll med behandlingen av persondata om seg selv.

7.5.2.2 Sikkerhets- og beredskapsprinsipper

Nedenfor gjennomgås sikkerhets- og beredskapsprinsippene. Noen av sikkerhets- og beredskapsbegrepene vil kun gjelde for konsument, andre for tjenesteyter og atter andre for begge.

7.5.2.2.1 Overordnede sikkerhets- og beredskapsprinsipper

Tjenestemobilitet (gjelder tjenesteyter): Handler om tjenesten lett kan flyttes fra en leverandør til en annen, eller fra en plattform til en annen. Mobilitet for tjenesten bør vurderes.

F.A.F.B (gjelder tjenesteyter og konsument): Forenkling, automatisering, forbedring, og en god brukeropplevelse. Innebærer at man må ha søkelys på forenkling, automatisering, forbedring, og brukeropplevelse og at tjenesten har et positivt utfall for konsument. F.A.F.B for tjenesten bør vurderes.

Proaktivitet: (gjelder tjenesteyter og konsument): Innebærer å prøve å forutse begivenheter eller problemer, snarere enn bare å reagere når de er oppstått. Begrunnelsen for dette er at kostnaden ved å handle reaktivt er lagt høyere enn å handle proaktiv. Proaktivitet for tjenesten bør vurderes.

7.5.2.2.2 Prosessuelle sikkerhets- og beredskapsprinsipper

Passiv sikkerhet (gjelder tjenesteyter og konsument): Med passiv sikkerhet menes innretninger som hjelper bruker uten nevneverdig innvirkning/interaksjon fra bruker. Passiv sikkerhet kan best forklares med å sammenligne bilens utvikling innen passiv sikkerhet så som radarsystemer, anti-skrens, airbag med videre. Det betyr at naturlige menneskelig adferd skal legges til grunn og hjelpe brukeren til å gjennomføre oppgaven på en trygg måte. Passive sikkerhetsmekanismer bør bygges inn slik at brukeren trygt kan gjennomføre ulike oppgaver uten å bli kompromittert i sin arbeidsutførelse.

Fail safe prinsippet (gjelder tjenesteyter og konsument): Fail safe er en egenskap som gjør at systemet ved feil går til en sikker tilstand. Det vil si at ingen sikkerhetskritisk situasjon skal oppstå som følge av feil i systemet. Det

betyr ikke at et system som er Fail safe ikke kan svikte, men snarere at systemets design forhindrer eller demper utrygge konsekvenser av systemets feil. Det vil si at hvis et fail system feiler, forblir det minst like trygt som det var før feilen. Fail safe prinsippet bør legges til grunn for tjenesten.

Self healing prinsippet (gjelder tjenesteyter og konsument): Self healing prinsippet går ut på at et system har en innebygd evne til å oppdage og rette feil uten å ha hjelp utenfra. For eksempel at et nettverket skal kunne diagnostisere og ordne nettverksproblemene automatisk. Self healing prinsippet bør legges til grunn for tjenesten.

Sikker utviklingssyklus (gjelder tjenesteyter) og anskaffelse (gjelder tjenesteyter og konsument): Det finnes ulike rammeverk for sikker utviklingssyklus, for eksempel Microsoft Security Development Lifecycle (SDL). For å ha en sikker og agil leveransemodell bør DevSecOps prinsipper legges til grunn. SDL eller tilsvarende rammeverk vil være en delmengde av DevSecOps. Sikkerutviklingssyklus varer gjennom hele livssyklusen til produktet. Datatilsynets veileder for programvareutvikling med innebygd personvern legges til grunn[13]. Ved anskaffelse legges hele livssyklusen til systemet til grunn. Brukerinvolvering og interaksjonsdesign bør være sentrale elementer i DevSecOps.

Agilt og skalerbarhet (gjelder tjenesteyter og konsument): Funksjonene i tjenesten bør være skalerbare og agile for hele livsløpet. Dette for å legge til rette for innovasjon og evolusjon.

Dynamisk risikostyring (gjelder tjenesteyter og konsument): På de mest kritiske funksjonene bør det gjøres dynamisk (kontinuerlig) risiko- og sårbarhetsvurdering slik at man evner å levere tjenestene selv under uønsket påvirkning, eller redusere risikoen for bortfall av tjenestene uavhengig om handlingen er tilsiktet eller utilsiktet.

Enkelhetsprinsippet (gjelder tjenesteyter og konsument): Systemet bør baseres seg på enkelthetsprinsippet. Det gjelder både i forhold til brukerinteraksjon og ved oppbygning av løsningen. Løsningsdesign bør være transparent og enkel slik at feilkilder kan oppdages raskt og nye funksjoner kan implementer «on the fly», uten at dette går utover løsningens leveranseevne. I enkelhetsprinsippet ligger også at konsumenten skal være i stand til å konsumere løsningen.

Avhending (gjelder tjenesteyter og konsument): Avhending må gjennomføres på en slik måte at det ikke kommer i konflikt med lov eller de andre sikkerhetsprinsippene.

Åpenhet og åpne standarder (gjelder tjenesteyter): Sårbarheten ved å utvikle selv kontra bruk «off the shell produkter», åpne APIer og tekniske standarder må vurderes. Om det finnes åpne APIer, tekniske standarder som er anerkjent, eller «off the shell produkter» bør disse benyttes.

Transparent og ansvarlighet (gjelder tjenesteyter og konsument): Tjenesten bør være transparent slik at man har oversikt over hele tjenesteleveransen (og verdikjeden) med dets sårbarheter og enkelt feil (singel point of failure). Ansvarsforholdene for tjenesten mellom partene bør være avklart og konsensus om dette bør være oppnådd.

7.5.2.2.3 Teknologiske sikkerhets- og beredskapsprinsipper

Tilgangsstyring (gjelder tjenesteyter og konsument): En zero-trust-tilnærming bør ligge til grunn for autentisering og autorisering samt prinsippet om tjenstlig tilgang. Det vil si at tilgang kun skal gis ved tjenstlig behov og kun til personell og digitale enheter som er autentisert og autorisert. Dette gjelder alle moduler og komponenter i løsningen(e). Samtidig må ikke løsning kompliseres unødvendig. En kost/kvalitetsanalyse munnet ut i risikoaksept vil gi en indikasjon på nivået på fullstendig tillitsprinsippet i en ytterkant, kontra zero-trust tilnærming i andre ytterkant.

[13] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Seperasjon av data og applikasjon (gjelder tjenesteyter): Fleksibilitet, skalerbarhet, innovasjon og næringsutvikling bør legges til grunn for tjenesten. Data skal derfor være adskilt og være tilgjengelige gjennom APIer. Dette for å understøtte utvikling av tilleggsfunksjonalitet og integrasjon med andre løsninger, herunder endring av organisasjonsstrukturer, prosesser og applikasjoner, f.eks. bruk av maskin læring og på sikt kunstig intelligens (KI).

Kommunikasjonssikkerhet (gjelder tjenesteyter): All data krypteres ved overføring i henhold til kritikalitet og nasjonale anbefalinger. All informasjon som kommer fra en part utenfor løsningen(e) bør signeres slik at avsender kan verifiseres. Det bør vurderes kryptering på data som er i bero.

Sporbarhet, preventive, detekterende og korrigerende mekanismer samt kontinuerlig sikkerhetstesting (gjelder tjenesteyter og konsument): Det vil alltid være sårbarheter i tjenesteleveranse og det må tas høyde for at sikkerhetsmekanismer svikter. Det bør finnes mekanismer for å oppdage og hvordan man skal reagere for å gjenopprette normal situasjon og minimere skadeomfang. Komponenter som håndterer kritiske/sensitiv informasjon bør i størst mulig grad beskytte seg selv, og ha minst mulig tillit til omkringliggende komponenter. Det bør gjennomføres kontinuerlige sikkerhetstester av kritiske systemer. Dette både i forhold til gjennomgang av kode, inntrengningstesting, og sårbarhetsskanning.

Seperasjon av kritiske komponenter (gjelder tjenesteyter og konsument): Komponenter som inneholder sikkerhetsfunksjoner/behandler kritisk/sensitiv funksjoner (informasjon) bør separeres i størst mulig grad fra komponenter som utfører andre funksjoner. Dette for å hindre at sikkerhetskomponentene ikke blir påvirket av feil eller sikkerhetsbrudd i de andre komponentene. Separasjon bør praktiserer på alle lag. Diversitet bør praktiseres så langt det lar seg gjøre.

Minst mulig privilegium (gjelder tjenesteyter og konsument): Funksjonene bør har mist mulig privilegium (rettigheter) for å utføre sin funksjon.

Lagdelt sikkerhetsarkitektur og sikring i dybden (gjelder tjenesteyter og konsument): En utfordring med operasjonelle kontroller kan være at de ikke nødvendigvis hindrer feil fra å skje. Sikringstiltak kan gjøre at feil sjeldnere oppstår, eller gjøre det mulig å oppdage de innen rimelig tid i etterkant, men kan ikke garantere tilstrekkelig sikring. Det bør derfor implementeres flere lag av sikkerhet og derav ha tilstrekkelig sikring og oppdagelsesmulighet i dybden hvor diversitet bør være et av flere målparametere.

Tjenesteplattform (gjelder tjenesteyter): Innebærer at tjenesteplattformen må ha nødvendig robusthet i forhold til tjenestekritikalitet med hensyn til flyttbarhet, redundans, skalerbarhet, reverserbarhet, modulærbarhet og stabilitet i tråd med prinsippene om kost, kvalitet og risiko.

Sikker kode (gjelder tjenesteyter): Kildekode, og spesielt åpen kildekode, eller logikk bør testes og sikres gjennom automatiske og manuelle kilde- og logikkrevisjoner, og sårbarhetstester.

7.5.2.2.4 Personrelaterte og organisatoriske sikkerhets- og beredskapsprinsipper

High Reliability Organization (HRO) (gjelder tjenesteyter og konsument): HRO-teorien tar utgangspunkt i at verden er kompleks, ustabil, ukjent og uforutsigbar. Kjernen i teorien er årvåkenhet som gjør det mulig å se betydningen av svake signaler og respondere enhetlig på disse. Utgangspunktet er å håndtere det uventede ved årvåkenhet og oppdage problemer mens de er under utvikling. Om en hendelse ikke kan stanses, bør den demmes opp. Hvis problemet klarer å bryte igjennom oppdemning, må det være robusthet i systemet som gjør det mulig å hurtig reetablere systemfunksjonalitet. HRO-systemer er ikke feilfrie, men samtidig fører ikke feil til at organisasjonen eller funksjonene bryter sammen. Poenget med å benytte HRO er tjenesteyter og konsument utvikler en god evne til å kontrollere komplekse teknologier uten å forårsake individuelle eller organisatoriske ulykker. HRO prinsippet bør legges til grunn for tjenesten.

Kontinuitet (gjelder tjenesteyter og konsument): Det bør etableres en strukturert tilnærming til kontinuitet og gjenoppretting. Virksomhetskontinuitet skal ivareta at de kritiske virksomhetsprosessene vil fortsette innenfor akseptable nivåer når uønskede hendelser inntreffer. Virksomhetskontinuitet omfatter virksomhet som helhet, det vil si også de tilknyttede kommunene i tillegg til Akson Journal AS.

Beredskaps- og drift (gjelder tjenesteyter og konsument): Beredskap og drift skal basere i tråd med nasjonale prinsipper om ansvar, likhet, nærhet og samvirke. Virksomheten bør dimensjonere beredskap i tråd med tjenestekritikalitet og kost-, kvalitets-, og risikovurdering.

Opplæring av personell innen sikkerhet, beredskap og personvern (gjelder tjenesteyter og konsument): Personell bør gis tilstrekkelig opplæring i løsningen(e) og tjenesteleveransen slik at hver enkelt kan ivareta sitt ansvar for sikkerhet, beredskap og personvern. Personell bør også gis opplæring innen kontra psykologiske virkemidler, herunder typiske virkemidler innen sosial manipulering. Årlig sertifiseringsordning for bruk av systemet bør innføres.

Kontrollbarhet personell (gjelder tjenesteyter og konsument): Det må gjennomføres egnet bakgrunnssjekk av personell som skal ha tilgang til kritiske komponenter eller kritiske deler av tjenesten. For annet personell bør det gjennomføres en risikovurdering.

Varslingssystem (gjelder tjenesteyter og konsument): Det bør finnes varsling og koordineringssystem i forhold til leverandører, konsumenter og andre aktuelle entiteter for å minimere kaskadevirkningene minst mulig og for å kunne håndtere en «situasjonen» raskest mulig.

Øvelser (gjelder tjenesteyter og konsument): Det bør gjennomføres øvelser både i forhold til kontinuitets-, sikkerhets- og beredskapsstyring.

Seperasjon av ansvar (gjelder tjenesteyter og konsument): Seperasjon av ansvar bør være avklart i forhold til tjenestens kritikalitet.

Dokumentasjon og tilgang (gjelder tjenesteyter og konsument): Kritisk tjenestedokumentasjon bør være oppdatert og befinne seg på et område som lar seg aksessere når alt feiler.

Leverandør og leveranser (gjelder tjenesteyter og konsument): Anskaffelsene bør støtte oppunder tjenestekritikalitet. Prinsippet om innovative anskaffelser bør vurderes.

Nasjonale krav (gjelder tjenesteyter og konsument): Tjenesten må oppfylle avtalemessige, lovmessige, eller nasjonale krav til sikkerhet, beredskap og personvern.

Organisasjonens modenhet (gjelder tjenesteyter og konsument): Organisasjonen (både tjenesteyter og konsument) bør legge til rette for systematisk forståelse av tjenestekritikalitet, tjenesteleveranser, og øvelser som muliggjør en god tjenesteleveranse i tråd med sikkerhets-, beredskap, og personvernprinsippene.

Revisjonsbarhet (gjelder tjenesteyter og konsument): Tjenesten bør enkelt kunne underkastes revisjon. Det bør legges til rette for eksterne revisjoner for å skape økt tillitt til systemet. Revisjoner bør gjøres på innenfor personvern, sikkerhet, beredskap, kontinuitet, og hendelseshåndtering. Automatiske revisjoner bør vurderes.

7.6 Oppsummering RSB

Kjernen i RSB er at den skal være pragmatisk og ha en helhetlig tilnærming til å finne tjenestekritikalitet for tjenestene. Tjenestekritikaliteten er avgjørende for å kunne dimensjonere rett og tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre tjenester. Og i en forlengelse av dette, hvilke sikkerhets-, beredskaps-, og personvernprinsipper som bør legges til grunn for å oppnå tilstrekkelig sikkerhets- og beredskapsevne i tråd med tjenestekritikaliteten.

For å finne tjenestekritikalitet, og hvilke sikkerhets, beredskaps, og personvernprinsippene som skal implementeres, baserer RSB seg på fire grunnprinsipper og fire styringsprinsipper. Disse gir en veiledning på hvilke hensyn som bør vektlegges når man skal finnes tjenestekritikalitet og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres.

RSB kan anses som en veiledning/kravsett på hvordan man kan oppnå en sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester. RSB handler ikke om sikkerhetsstyring på virksomhets- eller på operativnivå, men vil være styrede for dimensjonering av sikkerhetsstyring, operativ sikkerhet, og teknisk sikkerhetsarkitektur.

Det finnes allerede gode ulike rammeverk som gir god veiledning sikkerhetsstyring på virksomhetsnivå og teknisk sikkerhetsarkitektur som kan benyttes. Som eksempler her kan nevnes Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen), ISO27001 (ISO27002) med flere, NIST Cyber Security Framework, CIS Center for Internett Security (CIS) kontroller, Nasjonal sikkerhetsmyndighets grunnprinsipper, og Nasjonal sikkerhetsmyndighets rammeverk for håndtering av IKT-hendelser, og SABSA (Sherwood Applied Business Security Architecture) for å nevne noen.

7.7 Konsekvenser for Akson

Slik RSB er designet vil det gjøre kommunal sektor bedre rustet til å vurdere tjenestekritikalitet og oppnå nødvendig sikkerhets- og beredskapsevne for å kunne konsumenere digitale tjenester levert av Akson journal AS (og NHN) på trygg og sikker måte.

RSB er kost, kvalitet, og risikobasert slik at i hvilken styrke den enkelte personvern, sikkerhets- og beredskapsprinsipp skal implementeres i vil avhenge av tjenestekritikalitet og tjenestetype. RSB vil gi en felles plattform for å skape nødvendig tillit mellom Akson Journal AS og kommunal sektor for behandling av dataene i Aksons økosystem. En felles plattform og tillitt er helt nødvendig for å legges til rette for innovasjon, kontinuerlig utvikling, og prosessendringer i en verden som endrer seg raskt i forhold til teknologi, økonomi og arbeidsprosesser.

Slik RSB er designet, vil ikke dette medføre noen ekstra kostnader eller dreining av prosjektet i forhold til den planlagte leveransen. Tvert imot vil RSB gjøre leveransen fra Akson Journal AS mer robust, og legge til rette for innovasjon, forenkling, og forbedring.