Trygg digitalisering

Anbefalte felles kommunale sikkerhetskrav

Sluttrapport
24. juni 2024

Innholdsfortegnelse

Bakgrunn

Med bakgrunn i risikobildet for kommunal sektor besluttet KS vinteren 2022 å utarbeide et kunnskapsgrunnlag 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 sikkerhetsarbeidet.

Rapporten *Styrking av digital robusthet i kommunal sektor*[1] (heretter kalt Rapporten) slår fast 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.

Rapporten inneholder 16 tiltak hvor tiltak 7 omhandler utarbeidelsen av anbefalte felles sikkerhetskrav som bør sammenstilles og tilgjengeliggjøres til hele sektoren. Det er forventet at tiltaket skal vesentlig redusere risiko i anskaffelser, drift og forvaltning, og ikke minst at kommunene kan gjennomføre trygg digital transformasjon for å kunne møte fremtiden på en god måte.

Dagens situasjon, utfordringsbildet i kommunal sektor

Rapporten beskriver dagens situasjon godt og det henvises til denne. Her gis det imidlertid en kort oppsummering av dagens situasjon. Den teknologiske utviklingen og integrerte IT-systemer bidrar til økt samvirke og mer effektive tjenester. Samtidig fører dette med seg avhengigheter mellom konsumenter og tjenestetilbydere, som igjen kan medføre utfordringer knyttet til ivaretakelse av personvernet til ansatte og innbyggere, og igjen øker kompleksiteten i verdikjedene. Det kan derfor være utfordrende å få oversikt over avhengigheter i og mellom tjenesteleveransen(e), og kritikaliteten det representerer for kommunene.

Rapporten viser at det er ulik modenheten på digitaliseringsområdet i kommunal sektor. Ulik modenhetsgrad innen digitalisering gir også følgelig ulik modenhet innen informasjonssikkerhet, digital beredskap og personvern. Ulik modenhet skyldes parametere som:

- Ulik ressurstilgang (kompetanse, personell og økonomi).
- Ulik konsumeringsevne.
- Ulike forvaltningsmodeller.
- Ulik strategisk styringskompetanse (politisk og ledelsesnivå).
- Mangel på felles krav og samstyring.
- Fagområdet er komplekst og i hurtig endring og mange aktører.

Rapporten slå videre fast at på tross av ulikt utgangspunkt for kommunene er det vesentlig at man når ut og løfter samtlige kommuner for å gjøre dem mer robuste for å opprettholde sin funksjonsevne i det digitale skiftet.

[1] https://www.ks.no/contentassets/6394e77225384674b1de93b0203f6825/Digital-robusthet-i-kommunal-sektor-.pdf

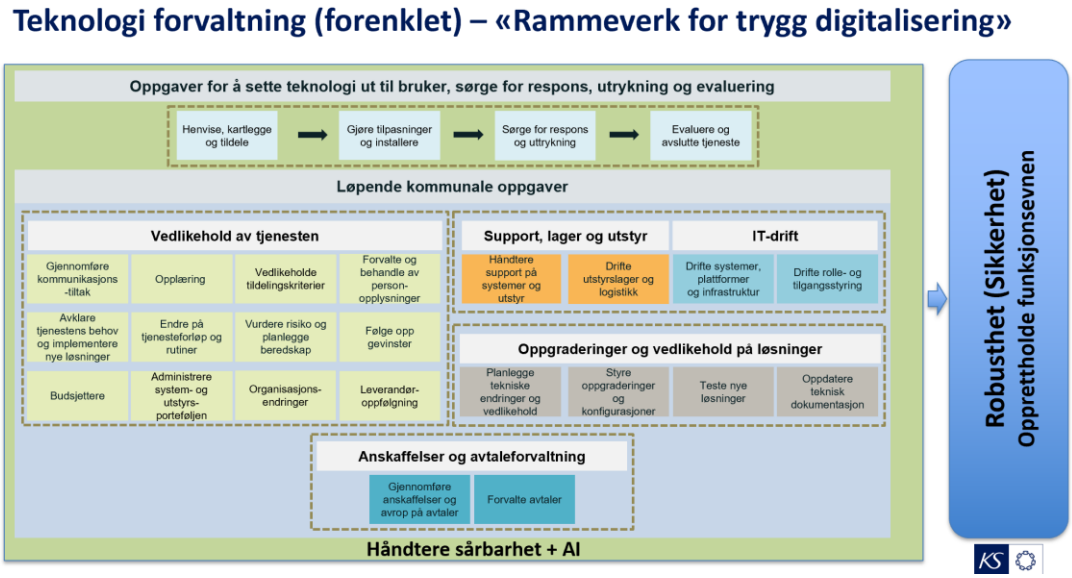
Behovet for anbefalte sikkerhetskrav i kommunal sektor

Den enkelte kommune (behandlingsansvarlig) har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden. I de tilfeller det ikke behandles personopplysninger, har likevel den enkelte kommune eller fylkeskommune et ansvar for at det utarbeides og stilles riktige krav til leverandører med hensyn til risikoen tjenesten representerer.

I leveranser av tjenester, maskinvare eller systemer skal det avtales med leverandører hvilke sikkerhetskrav som skal oppfylles for at den behandlingsansvarlige (kommune og fylkeskommune) skal kunne oppfylle sitt ansvar. Dette ansvaret gjelder også til egen organisasjon, og kravene må derfor stilles til de ansvarlige for implementering, drift og avslutning/avhending av IKT-porteføljen i egen organisasjon.

Kommunal sektor tjenesteutsetter i økende grad hele eller deler av IKT-porteføljen. Tjenesteutsettning benyttes som et virkemiddel for å være med på digitaliseringstakten og teknologiutviklingen, men også fordi det av økonomiske eller forvaltningsmessige årsaker er gunstig og effektivt for kommunal sektor å tjenesteutsette. Med bakgrunn i økende grad av tjenesteutsetting, blir det stadig mer krevende å ha oversikt over allerede komplekse verdikjeder.

Erfaringer fra NSM og andre statlige tilsynsorganer viser at det er lav bevissthet rundt krav til og oppfølging av informasjonssikkerhet ved tjenesteutsetting av IKT-tjenester. Risikovurderinger og konsekvensutredninger som utføres ved tjenesteutsetting er ofte mangelfulle. Funnene i rapporten viser de samme trendene og utfordringene. Kommunal sektor rapporterer også selv at det er utfordrende å utarbeide, forvalte og implementere sikkerhetskrav, ofte begrunnet i manglende kapasitet eller kompetanse. For å illustrere kompleksiteten av kravstilling til alle faser av (digital) tjenesteproduksjon, vises det til figur 1. Til alle elementene som fremvises i figuren, fordrer det at det er etablert og stilt riktige sikkerhetskrav til tjenesten.



Figur 1 Illustrasjon av elementene i digital transformasjon

For at kommunal sektor skal lykkes med tjenesteutsetting, gode teknologiske anskaffelser, og en vellykket og sikker tjenesteutsette, er det viktig at det stilles riktige og gode krav. På grunn av

innvirkningen som teknologien har på organisasjonen og det mulighetsrom og sårbarheten som den representerer, er det fra kommunal sektor etterlyst en felles tilnærming til anskaffelses- og forvaltningsperspektivet gjennom å ha spesifikke og operative anbefalte sikkerhetskrav for å kunne digitalisere trygt.

Tiltak 7 vil kunne ha innvirkning i positiv retning på digitalisering i kommunal sektor ved at:

- Leverandørene vet hvilke krav som gjelder innen informasjonssikkerhet, digital beredskap og personvern. Dermed kan de også lettere implementere kravene inn i sine systemer allerede fra utviklingsfasen. Dette i sum vil gjøre kommunal sektor mer robust ved at systemene blir mer robuste i tillegg til en forutsigbarhet for leverandørene.

- Kommunal sektor effektiviserer tidskrevende arbeid. Det er tidskrevende å utarbeide sikkerhetskrav i forbindelse med anskaffelse og forvaltning. Ofte er systemene som anskaffes i kommunal sektor de samme, men kommunen gjør jobben hver for seg. Det vil være svært tidsbesparende for kommunale sektor å ha «ferdige» anbefalte sikkerhetskrav som kommune kan legge til grunn ved anskaffelser og forvaltning og ikke «finne opp hjulet på nytt hver gang».

- Felles anbefalte sikkerhetskrav vil redusere risiko for anskaffelser av sårbare system. Mange anskaffer systemer som ikke er tilstrekkelige robuste, eller har en lite tilfredsstillende forvaltning. Dette fører igjen til kommune blir unødvendig sårbare.

- I den grad kravene legges til grunn ved anskaffelser, kan forskjeller mellom kommuner begrenses når det gjelder ivaretakelse av informasjonssikkerhet, digital beredskap og personvern.

Eksisterende veiledning

KS har verktøykasse for kommunedirektører[2], veileder for bruk av sosiale media i kommunal sektor[3], og i tillegg til prosjektet SkoleSec[4]. I tillegg finnes det flere rammeverk på overordnede nivåer, f.eks. NSM grunnprinsipper for IKT-sikkerhet[5], ISO27001[6], Digitaliseringsdirektoratet internkontroll[7] og ulike veiledninger fra Datatilsynet, og Digitaliseringsdirektoratet prosjekt «felles sikkerhet i forvaltningen».

Det eksisterer lite spesifikk og operativ veiledning innen området. Det kommunal sektor etterlyser i sterk grad er spesifikke og operative anbefalte sikkerhetskrav til anskaffelse og forvaltning i hele IT-

[2] https://www.ks.no/fagomrader/forskning-og-utvikling-fou/forskning-og-utvikling/slik-sikrer-du-oppfolging-av-personvern-og-informasjonssikkerhet/

[3] https://www.ks.no/fagomrader/digitalisering/kompetanse-og-verktoy/informasjonssikkerhet-og-personvern/ny-veileder-for-bruk-av-sosiale-medier-i-kommunen/

[4] https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/

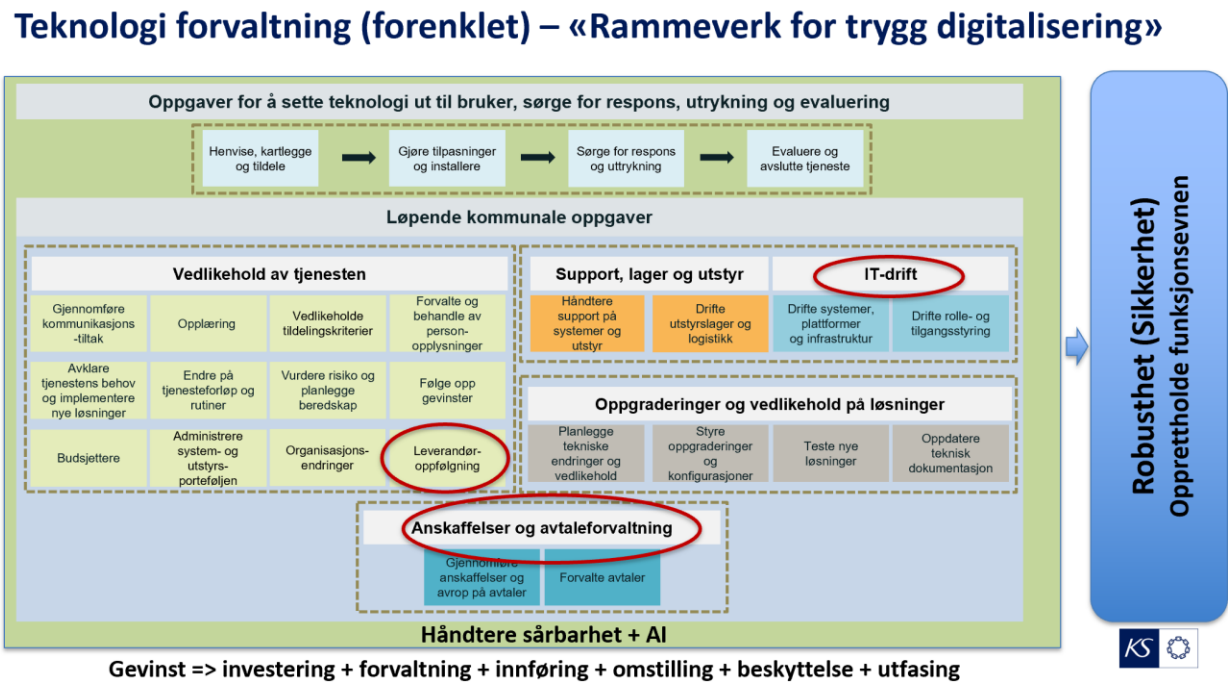
[5] https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

[6] https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/

[7] https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601

systemets livsløp. Videre etterlyses sikkerhetskrav til drifts- og forvaltningsorganisasjonen for å ivareta trygg og sikker digitalisering i hele verdikjeden

Fokuset for tiltak 7 er derfor å utarbeide spesifikke og operative sikkerhetskrav innen anskaffelse, forvaltning og sikker drift i hele livsløpet til IT-tjenesten, se elementene merket i rød figur 2 nedenfor.



Figur 2, fokuset for tiltak 7

Leveranser for tiltak 7

Leveranse	Beskrivelse
Leveranse 1: Anbefalte spesifikke og operative sikkerhetskrav for anskaffelse og forvaltning.	I tillegg til egen drift, tjenesteutsetter kommunal sektor hele eller deler av IKT-porteføljen. Tjenesteutsetting benyttes som et virkemiddel for å være med på digitaliseringstakten, teknologiutviklingen, eller at det av økonomiske eller forvaltningsmessige årsaker er gunstig og effektivt å tjenesteutsette. I noen tilfeller finnes det ikke reelle alternativ til tjenestene eller IT-systemene som leverandørene tilbyr. I tillegg til tjenesteutsetting anskaffer kommunene også teknologi og systemer, f.eks. velferdsteknologi, infrastruktur, maskiner og programvare for å drifte dem selv. Med bakgrunn i bl.a. økende grad av digitalisering på tvers av sektorer, store IT-leverandører og tverrgående mikrotjenester blir det stadig mer krevende å ha oversikt over allerede komplekse verdikjeder. Dette

	bidrar til å øke risikoen ved ytterligere å øke kompleksiteten i verdikjeden. I denne leveransen vil man sette opp anbefalte spesifikke og operative sikkerhetskrav innen informasjonssikkerhet, digital beredskap og personvern for anskaffelser og forvaltning. De anbefalte kravene vil være spesielt rettet mot kommunal sektors behov for å kunne ivareta anskaffelses- og forvaltningsperspektivet.
Leveranse 2: Anbefalte spesifikke sikkerhetskrav til drifts- og forvaltningsorganisasjonen	Kommen har ulike drifts- og forvaltningskonstellasjoner. Noen kommuner drifter selv, andre har et Interkommunalt samarbeid (IKS), atter andre har tjenesteutsatt det meste, og atter andre en kombinasjon av ovennevnte konstellasjoner. Uavhengig av dette har kommunen et behov for å stille spesifikke og operative sikkerhetskrav til drifts- og forvaltningsorganisasjonen. Et slikt krav er f.eks. spesifikt responstid for hendelser eller bruk av lagdelt sikkerhetsteknologi. Kommunal sektor har etterlyst en felles tilnærming til felles sikkerhetskrav til drifts- og forvaltningsorganisasjoner. Dette tiltaket vil ha en positiv innvirkning på digitalisering i kommunal sektor ved at; - Drifts- og forvaltningsorganisasjonene vet hvilke krav som gjelder innen informasjonssikkerhet, digital beredskap og personvern. Dermed kan de også lettere implementere kravene da det ikke vil være utydelighet på hva som gjelder. Dette i sum vil gjøre hele kommunal sektor mer robust ved at drifts- og forvaltningsorganisasjonene for forutsigbarhet i forhold til drift og forvaltning. - Den enkelte kommune bruker veldig mye tid hver for seg å til «lage» sikkerhetskrav i forbindelse med drift og forvaltning og kommunen gjør jobben hver for seg. Det vil være svært tidsbesparende for hele kommunale sektor å ha «ferdige» sikkerhetskrav som kommune kan legge til grunn i forhold til drifts- og forvaltning. På grunn av manglene sikkerhetskrav i forbindelse med drift og forvaltning gjør at flere driftsorganisasjoner ikke har tilstrekkelig

	robusthet. Dette fører igjen til kommune blir unødvendig sårbare.

Prosjektets gjennomføring

Prosjektet ble gjennomført fra 1. oktober 2023 til 31. januar 2024, med noe tid avsatt i februar for utarbeiding av instruksjonsvideo. Tiden frem til slutten av juni er brukt til å kvalitetssikre og skrive sluttrapport.

Deltakere

Prosjektet har involvert en rekke deltakere fra forskjellige sektorer, fra ulike geografiske områder og med variert bakgrunn.

Prosjektets referansegruppe bestod av representanter av følgende kommuner: Asker, Fredrikstad, Vågan, Beiarn, Kristiansand, Hammerfest, Horten, Stjørdal, Bergen og Ålesund. I tillegg besto referansegruppen av representanter fra følgende IKS/felles driftsenheter: ROR-IKT, IKOMM og Region Nordhordland IKS.

Denne referansegruppen møttes ukentlig i hele prosjektperioden, og ga tilbakemeldinger underveis på både metodikk, analyse og de praktiske leveransene.

Prosjektet har også gjennomført månedlige workshops med Nasjonal sikkerhetsmyndighet (NSM), Digitaliseringsdirektoratet (DigDir), e-Helse og Direktoratet for forvaltning og økonomistyring (DFØ), samt Datatilsynet. Disse organisasjonene har bidratt med spesialisert kunnskap og veiledning, særlig i aspekter knyttet til sikkerhet, digitalisering og personvern. Videre har de kommet med mange gode råd og innspill på hvordan løsningene kan komplementere eksisterende prosjekter som for eksempel DFØs markedsplass for skytjenester.

Vi har også fått mye hjelp med test av løsning og innspill fra innkjøpere fra flere kommuner, Innlandskommune (kommuner tilknyttet IKOMM), driftsorganisasjoner og KS.

Mål for prosjektet

Som definert i søknaden om prosjektmidler var de originale målene for prosjektet som følger:

- Å klargjøre krav innen informasjonssikkerhet, digital beredskap og personvern for leverandørene. Dette gjør at de kan integrere disse kravene i sine systemer fra utviklingsfasen, noe som øker robustheten i kommunale systemer og gir forutsigbarhet for leverandørene.

- Å effektivisere tidskrevende arbeid i kommunal sektor. Ved å ha standardiserte anbefalte sikkerhetskrav for anskaffelser og forvaltning unngår kommunene å måtte utarbeide disse kravene hver for seg, noe som sparer tid og ressurser.

- Å redusere risikoen ved anskaffelse av sårbare systemer. Felles anbefalte sikkerhetskrav vil bidra til å forhindre anskaffelse av systemer som ikke er tilstrekkelig robuste, eller hvor leverandørene ikke har tilstrekkelig sikkerhetskompetanse, og dermed redusere kommunenes sårbarhet.

- Å minimere forskjeller mellom kommuner i anskaffelsesprosesser, ved å standardisere kravene som legges til grunn.

I den første fasen av prosjektet ble eksisterende sikkerhetskrav både til leverandører og til egne drift- og forvaltningsorganisasjoner vurdert. Basert på eksisterende krave definerte prosjektet følgende strategiske retningslinjer:

1. Å gå fra en teoretisk "papirsikkerhet" til en mer praktisk og anvendelig sikkerhet. Dette betyr å bytte ut tekstlige besvarelser og vurderinger basert på skjønn med mer direkte og nøyaktige metoder.

2. Som en utvidelse av dette ønsket vi å gjøre sikkerhetsarbeidet mer konkret, presist og målbart, ved å bruke skjemaer som er enkle å forstå og følge. Dette hjelper med å bedre vurdere og forbedre sikkerheten uten at alle parter trenger å ha ekspertkunnskap innen sikkerhet.

3. Alle leveranser i prosjektet ble bestemt tilpasset behovene til spesielt mindre og mellomstore kommuner, som kan mangle spesialistkompetanse innen datasikkerhet. Dette stiller krav til å skrive forståelige beskrivelser, og til å tilpasse kravene kommunenes faktiske situasjon.

4. For å dekke både eksterne leverandører og interne organisasjoner anså vi det som viktig å inkludere sikkerhetskrav tidlig i design- og planleggingsfasen av anskaffelser. Dette bidrar til en mer forebyggende tilnærming til sikkerhet.

Leveranse 1: Spesifikke og operative sikkerhetskrav for eksterne leverandører

Arbeid med leveranse 1 varte i hele prosjektperioden, hvor både den tekniske løsningen og skjema ble utviklet i oktober og november 2023. Desember og januar ble brukt til testing og kvalitetssikring.

Prosjektet har prøvd å adressere følgende utfordringer ved anskaffelser:

- Manglende spesifikke sikkerhetskrav: Det er mange veiledninger og kravlister, men de er oftest av generell karakter, og heller ikke nødvendigvis tilpasset behov og risikoer i kommunal sektor.

- Ressursbegrensninger i kommunal sektor: Det kan være utfordrende å vurdere sikkerhetsaspektene ved anskaffelser, og det er mange manuelle prosesser ved anskaffelser.

- Overholdelse av regelverk: Kommunene har mange regler å forholde seg til.

- Risikovurdering- og håndtering: Det kan ofte være utfordrende å gjennomføre tilstrekkelige risikovurderinger både før og etter anskaffelse.

- Leverandørsikkerhet: Kommunene er ansvarlige for sikkerhet også når tjenestene utføres av leverandør. Tilstrekkelig kontroll kan være omfattende og komplisert.

Den mest brukte prosedyren for anskaffelser i kommunal sektor er presentert i DFØ på anskaffelser.no. For å støtte opp anbefalte krav til sikkerhet og robusthet i denne prosessen utviklet vi en metode delt i fire deler, henholdsvis:

1. Måling av kritikalitet og modenhet for kommunen: Dette skjemaet består av to deler:

a. Kritikalitet: Vurderer hvor kritisk systemet er, for kommunens innbyggere og for kommunens ansatte (12 spørsmål).
b. Modenhet: Vurderer hvor moden kommunen er til å anskaffe et nytt system (23 spørsmål).

2. Evaluering av leverandørens modenhet og sikkerhet: Dette skjemaet brukes for å kartlegge leverandørene og består av tre deler:
    a. Innledende spørsmål: Dette er grunnleggende spørsmål om virksomheten, som antall ansatte og hvor virksomheten er lokalisert (15 spørsmål).
    b. Leverandørmodenhet: Dette er spørsmål som går på organisatorisk modenhet hos leverandøren, som i hvilken grad de har et styringssystem (28 spørsmål).
    c. Leveransesikkerhet: Dette er spørsmål som måler organisatorisk og teknisk sikkerhet hos leverandøren for selve leveransen (110 spørsmål).

3. Analyse og veiledning: Dette skjemaet kan automatisk analysere utfylte utgaver av de to forrige skjemaene mot hverandre, og til å komme med forslag til tekster og aktiviteter, herunder:
    a. Veiledning: En kort beskrivelse av hvordan bruke løsningen.
    b. Analyse kommune: Forslag til utlysningstekst basert på utfylt Kritikalitet og modenhet og forslag til aktiviteter kommunen bør gjøre.
    c. Analyse leverandør: Analyse av leverandørbesvarelser, hvor det blir beregnet skåre for leverandøren, samt vist røde flagg for mulige mangler i leverandørens besvarelse.
    d. Sammenligning av kommune og leverandør: Her tas de utfylte arkene for Kritikalitet og modenhet og sammenligner dette med en leverandørbesvarelse. Det blir også vist hvor det er avvik, og spørsmål som en bør stille leverandøren.
    e. Oppfølging: Dersom leverandøren har sagt seg villig til å dele informasjon med kommunen blir dette vist her.

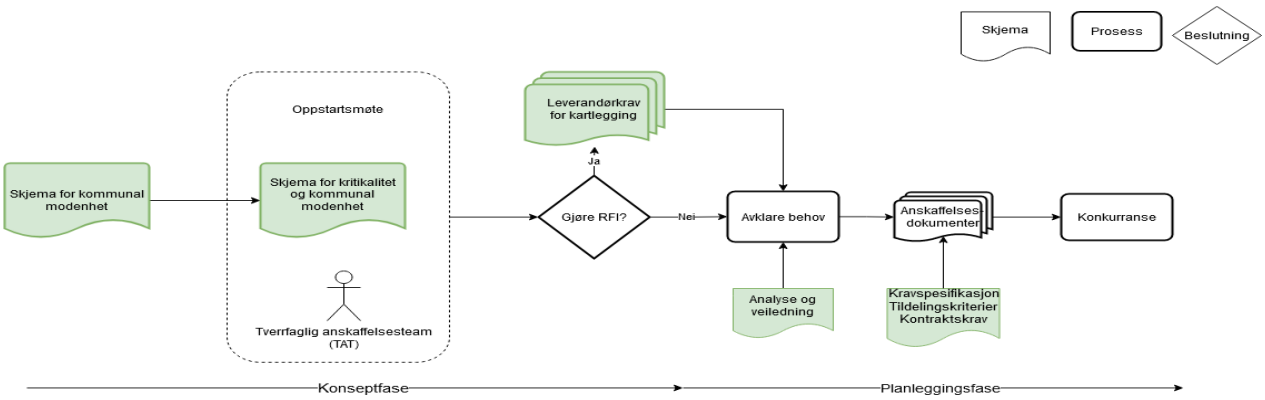
4. Utkast til krav for anbudsdokumenter: Dette arket inneholder utkast til krav som kan stilles i anbudsdokumentene, basert på resultatet av kartleggingen.

Følgende vedlegg er også inkludert:

- Utkast til spørsmål for løsning for kommunens innbyggere: Dette er en oversikt over mulige utfordringer en bør vurdere for anskaffelsen for løsninger planlagt brukt av kommunens innbyggere.

- Utkast til grunnlag for kartlegging av teknisk IT infrastruktur: Dette er en oversikt over ulike kategorier systemer som en kommune typisk har. Om leverandørens løsning skal tilpasses kommunens infrastruktur vil det være praktisk å informere leverandøren om dette som en del av anbudsprosessen, og eventuelt ha det som et tildelingskriteria.

Dette diagrammet viser hvor løsningen støtter opp om DFØs anbefalte anbudsprosess:



Elementer markert i grønt er der løsningen støtter anskaffelsesprosessen for henholdsvis konseptfasen og planleggingsfasen.

Kravene til leverandørene dekker alle ledd av kommunal tjenesteproduksjon og systemers livsløp, fra prosesser rundt anskaffelser og brukerstøtte til utfasing og deponering.

Leveranse 2: Strategiske og spesifikke sikkerhetskrav til egen organisasjon

Arbeid med leveranse 2 startet i desember. Kommunedirektørene står overfor en betydelig utfordring når det gjelder å få en klar oversikt over sikkerheten i kommunens systemer. Ofte blir kommunikasjonen omkring dette emnet teknisk, noe som gjør det vanskelig for ledelsen å holde tritt med alle detaljene. Dette fører til at sikkerhetsaspektet ofte blir oversett, i hvert fall inntil det oppstår et alvorlig sikkerhetsbrudd.

På den andre siden, opplever IT-lederne utfordringer med å bli hørt, spesielt i diskusjoner om budsjetter og ressurser. Det kan også være utfordrende å koble tekniske sikkerhetstiltak til konkrete trusler og risikoer. En annen kompliserende faktor er at det operative ansvaret for sikkerhet ofte ligger hos eksterne leverandører eller interkommunale selskaper (IKS). Til tross for disse utfordringene, er det viktig å erkjenne at det endelige ansvaret for sikkerheten hviler på skuldrene til kommunedirektøren.

Prosjektet har utviklet to skjemaer for å forbedre informasjonssikkerheten i kommunene, hver med sitt spesifikke fokus og målgruppe:

1. Kartlegging av sikkerhet for kommunedirektør: Det første skjemaet består av 26 spørsmål som omhandler informasjonssikkerhet, komplett med beskrivelser og motivasjon for hvert spørsmål. Dette skjemaet er rettet mot kommunedirektøren, som har det formelle, overordnede ansvaret.

2. Kartlegging av sikkerhetstiltak for IT-ledere/sikkerhetsledere: Det andre skjemaet inneholder 22 kategorier og praktiske 104 tiltak presentert i form av spørsmål, som hver har et begrenset antall svaralternativer.

3. Visning av rest-risiko: Når skjemaene er utfylt, kan både kommunedirektøren og IT-direktøren se en detaljert oversikt over restrisiko, i form av 13 aktuelle angreps- og hendelses-scenarioer.

Dette inkluderer konkrete mulige trusler mot kommunen, scenarioer for hvordan disse truslene kan oppstå, og aktuelle tiltak som bidrar til beskyttelse, samt status for disse tiltakene.

Denne tilnærmingen er svært konkret og motiverende for å forbedre sikkerheten. I tillegg gir det kommunene et solid grunnlag for planlegging av videre sikkerhetsarbeid.

Begge skjemaene er utformet for å gi en skåre for kommunen. Denne skåringen gjør det mulig for kommunene å måle endringer og fremskritt i sikkerhetsarbeidet over tid. Skjemaene har samme struktur, slik at en kan sammenligne svarene på tvers av skjema. Tiltakene er ellers knyttet opp til NSMs grunnprinsipper for IKT sikkerhet, men går mer i detalj om hvert inkludert krav.

Leveranser og måloppnåelse

Bedre målbarhet og mindre krav til skjønn og ekspertkompetanse

Tradisjonelle rammeverk for evaluering av leverandører til anskaffelser og evalueringer av driftsorganisasjoner er gjerne basert på en rekke spørsmål av typen:

- Foreligger det oversikt over hvilke roller, tilganger og oppgaver underleverandørene brukt i leveransen har?

I en tradisjonell løsning vil dette være et ja/nei spørsmål, men også gjerne ha en åpning for en tekstlig besvarelse.

I den nye løsningen bruker vi det samme spørsmålet, men med utvidet med forklaring, motivasjon, konkrete alternativer og forklaring av alternativene. Her er et eksempel basert på spørsmålet om tilganger og oppgaver for underleverandørene:

- Forklaring: En slik oversikt må inneholde en liste som inneholder minst 1) navn på underleverandør, 2) deres ansvarsområder og 3) deres oppgaver.

- Motivasjon: Presis og konkret informasjon om underleverandørenes roller, tilganger og oppgaver vil gi leverandøren og kommunen kontroll over tilgangene. Mangler slike oversikter kan tilganger komme på avveie, og rollene og oppgavene deres ikke bli forstått. Ved hendelser kan dette føre til kaos.

- Svaralternativer: (leverandøren kan bare velge ett alternativ):
    - Ja, detaljert og delbart med kommunen: Oversikt over alle underleverandører, inkludert deres navn, ansvarsområder og oppgaver, og denne informasjonen er aktivt delt med kommunen
    - Ja, detaljert for alle underleverandører: Detaljert oversikt finnes, men den er ikke delt med kommunen.
    - Ja, men bare for kritiske underleverandører: Oversikt finnes bare for kritiske underleverandører, dvs de som er mest kritiske for leveransen av tjenesten
    - Delvis: Det er noe oversikt over underleverandører, men ikke komplett

- Nei: Det er ikke noen oversikt over underleverandører

Denne måten å presentere spørsmål og tiltak gjør det mulig å sammenligne besvarelser, måle dem opp mot kommunens krav, og stille oppfølgingsspørsmål, f.eks. om å få en kopi av oversikten nevnt i det første alternativet.

Løsningen for sikkerhetskrav til driftsorganisasjonen er basert på en tilsvarende tankegang, men i tillegg tar den hensyn til restrisiko, ved å knytte tiltak opp mot mulige angrep og så skåre i hvor høy grad skadebegrensende tiltak er utført.

Økt effektivitet og besparelser
De nye løsningene representerer en effektivitetsforbedring sammenlignet med den gamle metoden for å håndtere sikkerhet og robusthet ved anskaffelser og evalueringer av driftsorganisasjoner.

Eksisterende løsninger var typisk basert på mellom 100 og 300 spørsmål som krevde tekstlige besvarelser. Dette er svært tidkrevende både for den som fylte ut skjemaet og den som måtte evaluere svarene. Hvert svar som ikke var rene ja/nei spørsmål krever dessuten tolkning, noe som legger en stor belastning på den som skal evaluere. Dette kan være spesielt utfordrende for mindre kommuner, hvor ressursene ofte er begrensede. Disse prosessene var videre preget av manuelt arbeid og avhengighet av spesialiserte ressurser med erfaring i å håndtere komplekse spørreskjemaer.

I kontrast til dette, tilbyr de nye løsningene, både for anskaffelser og for krav til forvaltningsorganisasjoner, en langt mer effektiv tilnærming. Den består av konkrete og presise beskrivelser av tiltak, hvor den som fyller ut skjemaet velger mellom klart definerte alternativer. Dette gjør det mulig å evaluere besvarelsene automatisk basert på en modell hvor både spørsmål og svaralternativer kan skåres. Spørsmålene og alternativene er forklart i detalj, noe som sikrer at både den som fyller ut skjemaet og den som leser besvarelsen, har tilgang til den samme forståelsen og tolkningen av informasjonen. Dette gjør det langt enklere å forstå og besvare spørsmålene, uten behov for spesialistkompetanse.

Videre er svarene skåret automatisk, slik at det blir lettere å se mangler og utfordringer. For anbefalte sikkerhetskrav til anskaffelser er det dessuten støtte for mye av prosessen beskrevet i Direktoratet for forvaltning og økonomistyring (DFØ) sin anskaffelsesprosess. Denne automatiseringen og standardiseringen av prosessen reduserer tidsbruk og kompleksitet, noe som gjør det mulig for alle typer kommuner, uavhengig av størrelse og ressurser, å håndtere anskaffelsesprosesser mer effektivt.

Utvidede bruksområder

Verktøyene vi har utviklet har vist seg å være nyttige i flere sammenhenger enn opprinnelig antatt. For eksempel er skjemaet for kritikalitet blitt utvidet slik at det også kan brukes for kritikalitets- og verdivurderinger. Når dette skjemaet fylles ut, beregnes det en lokal kritikalitetsskåre. Denne skåren kan være svært nyttig i de tidlige fasene av anskaffelsesprosessen, spesielt i situasjoner der kommunen opererer med ulike prosedyrer basert på forskjellige grader av kritikalitet, eller som en del av kommunens arbeid med verdivurderinger.

I tillegg har målingen av leverandørens modenhet og leveransesikkerhet vist seg å være et fleksibelt verktøy som kan brukes på to forskjellige måter. For det første kan det brukes som en del av en Request for Information (RFI), hvor det bidrar til å kartlegge mulige leverandører. For det andre kan det fungere som et verktøy for å måle sikkerheten til leverandørene som deltar i en konkurranse. Begge disse strategiene er fullt støttet av løsningen, noe som gir en ekstra dimensjon til dens anvendelighet og effektivitet i anskaffelsesprosessen. Denne utvidede bruken av verktøyene understreker deres fleksibilitet og verdi for å styrke anskaffelsesprosedyrer.

Videre åpner løsningen for at verktøyene kan brukes utenfor offentlige sektor. Spesielt kan tilpasningen av «sikkerhetskrav rettet mot egen organisasjon» spille en nøkkelrolle i å forenkle og styrke sikkerhetsarbeidet til private bedrifter, interkommunale selskaper (IKS), og andre private organisasjoner. Ved å implementere tiltakene og kravene som er utviklet i denne løsningen, kan mellomstore og større organisasjoner i Norge ikke bare forbedre sin egen sikkerhetsstyring, men også bidra til en høyere standard for sikkerhet og robusthet innenfor sin bransje og samfunnet som helhet. På sikt kan arbeidet bidra til økt robusthet for hele Norge, ikke bare kommunal sektor.

Teknisk løsning

Nåværende teknisk løsning (Versjon 1)

Versjon 1 av skjemaene for begge løsningene er utviklet i Excel, i hovedsak grunnet den korte prosjektperioden. En Excel basert versjon har ført til at det har vært lett å gjøre endringer, siden krav til programmering er minimalisert. En av de største fordelene med Versjon 1 er muligheten for brukerne til enkelt å redigere og gjøre endringer. Skjemaene er laget uten makroer, noe som eliminerer bekymringer knyttet til sikkerhetsadvarsler.

Den største ulempen med løsningen er at det vil være krevende å vedlikeholde spørsmålene og analysen over tid, siden det ikke er noen sentral lagring av spørsmål. Tilsvarende er det ingen samlet innsamling av resultater, noe som begrenser effektene av informasjonsdeling mellom brukerne.

Alternativer for videre utvikling

For en ny versjon foreslås det en overgang til en web-basert plattform, i alle fall for krav til anskaffelser.

Denne oppgraderingen vil tillate definering av spesifikke brukere og tilgangsnivåer, både for kommunene og for leverandørene. Dette vil forenkle delingen av informasjon og bidra til å bygge et omfattende datagrunnlag om sikkerhetsstatusen i sektoren. En web-basert løsning vil også gjøre vedlikeholdet av skjemaene enklere og mer effektivt. Det blir mulig å tilpasse kravsett basert på typen av system som anskaffes, noe som øker relevansen og presisjonen i skjemaene. I tillegg vil brukervennligheten forbedres betraktelig, med en mer effektiv og sikrere prosess for deling av informasjon, samt enklere vedlikehold av spørsmål og skalaer.

I løpet av prosjektperioden har det også åpnet seg flere nye muligheter:

- Øke bredden på løsningen, ved å omfatte Normen for ehelse og mer av NSMs grunnprinsipper for IKT sikkerhet.

- Øke antall prosesser som støttes, ved å gå dypere inn i anskaffelsesprosesser, verdivurderinger, risikoanalyser og risikovurderinger

- Integrere med eksisterende løsninger, som Prosjektportalen og Fiks-plattformen.

Offentliggjøring

De utviklede løsningene ligger på KS sine nettsider, i tillegg vil man invitere til workshop i de ulike digitaliseringsnettverkene. Løsningen ble også kort presentert på ekommune2024, samt gjennom ulike fora i KS regi.