

Kommunernes Digitaliseringsprogram 2021-2025

Projektbeskrivelse

6.12 Vidensdeling og analyser af status på Cyber- og informationssikkerhed i kommunerne

Formål og baggrund

1.1. Baggrund

Sammenlægning af to projekter

Dette projekt er en sammenlægning og videreførelse af to hidtidige projekter. De to projekter er: 6.5 - Analyser af status på Cyber- og informationssikkerhed i kommunerne og 6.6 - Fælleskommunal videndeling om cyber- og informationssikkerhed.

De to projekter samles i et for at få en forenklet og mere gennemskuelig styring. Projekterne var en lidt kunstig opdeling, da analyserne af status, er grundlaget for samarbejdet mellem KL og kommunerne om cyber- og informationssikkerhed. Projektbeskrivelsen er i forbindelse med sammenlægningen revideret for at tage højde for ændrede krav og forventninger.

Baggrund

Der er stor interesse for og fokus på offentlige myndigheders evner til at tage godt og sikkert vare på borgernes data. Der er som følge heraf stort fokus på, om kommunerne kan leve op til dette og sikre undgåelse af sikkerhedsbrister, når kommunen er udsat for hacking mv.

KL har siden 2016 gennemført baseline analyser af kommunernes indsats for øget cyber- og informationssikkerhed med det formål at øge sikkerheden i kommunerne gennem fælleskommunale indsatser. Årlige målinger var også en aftale med regeringen frem til 2020. KL's bestyrelse besluttede i juni 2020, at disse målinger er nyttige for kommunerne, og at KL skal fortsætte med målingerne.

Resultaterne fra seneste og sidste analyse viser, at der fortsat er behov for, at kommunerne arbejder med den samlede opgave med at sikre borgernes data mv., både i forhold til informationssikkerhed og cybersikkerhed.

Informationssikkerhed er en opgave, der kontinuerligt skal løses i hele organisationen. Der er fortsat behov for, at en kommune sikrer, at de omfattende lovkrav til informationssikkerhed bliver håndteret i såvel administrationen, hjemmeplejen, folkeskoler osv.

I forhold til cybersikkerhed kom der et øget fokus på området i 2022 analysen. I den seneste analyse i 2023 er der blevet fokuseret yderligere på cyber-sikkerhedsområdet og på de hændelser, kommunerne oplever.

Samtidig med opstarten på baselineanalysen i 2016, udpegede den enkelte kommune via kommunaldirektøren en kontaktperson ift. Cyber- og informationssikkerhed. Disse 98 kontaktpersoner indgår i et KL faciliteret fælleskommunalt netværk, hvor der via en videndelings- og kommunikationsplatform på Yammer samarbejdes om at højne cyber- og informationssikkerheden.

1.2. Formål

Formålet med projektet er at understøtte kommunernes arbejde med at sikre tilstrækkelig fokus og niveau i arbejdet med cyber- og informationssikkerhed samt at understøtte vidensdeling og kompetenceopbygning på tværs af kommunerne.

Kommunernes arbejde med at sikre det nødvendige niveau i arbejdet med cyber- og informationssikkerhed sker bl.a. gennem de årlige målinger. Her kan kommunerne se eget niveau og benchmarke sig med andre kommuner. Desuden giver målingerne et fælles grundlag for at kunne drøfte og samarbejde om læringspunkter i netværket. Gennem fysiske netværksmøder mødes KL med de kommunale informationssikkerhedsmedarbejdere, med det formål at drøfte resultaterne fra de gennemførte baselines, vidensdele samt skabe tætte relationer mellem kommunernes informationssikkerhedsmedarbejdere og KL.

Projektet har desuden til formål at udbygge og udvikle det gode samarbejde, der er etableret mellem kommunerne og KL på sikkerhedsområdet. I samarbejdet sikres mulighed for at udveksle gode og dårlige erfaringer. KL faciliterer og sikrer, at der tages hånd om de udfordringer og behov, som de kommunale informationssikkerhedsmedarbejdere giver udtryk for.

1.3. Projekt idé

Ud fra resultaterne af baseline analyserne, samarbejdes på tværs af kommuner og KL med de områder, hvor der er udfordringer eller behov for øget indsigt mv. og de årlige analyser tilpasses løbende, bl.a. tilføjes nye aktuelle analyser, som det f.eks. er sket med cybersikkerhed og cyberhændelser.

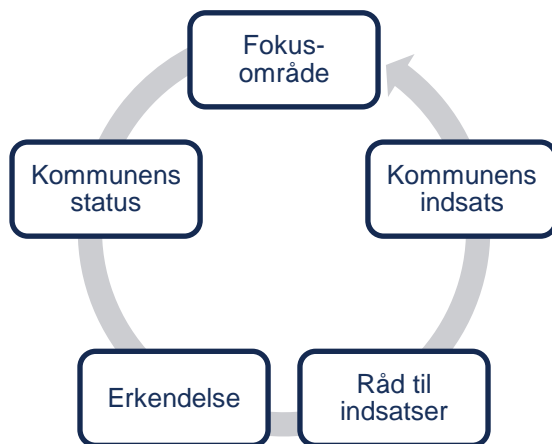
I de seneste år har antallet af kommuner der har deltaget i analysen været nedadgående. Fra deltagelse af 94-98 kommuner i de første år, til 66 kommuner i sidste runde.

Resultaterne af analyserne gennem årene har vist, at 25% af de deltagende kommuner ligger højt i forhold til efterlevelse af kravene til cyber- og informationssikkerhed, 50% ligger på et godt gennemsnitligt niveau, mens op mod 25% af kommunerne ligger under niveau. Det ser dermed ud til at 25% af kommunerne har svært ved at omsætte krav til cyber- og informationssikkerhed i systematiske og dækkende tiltag.

Projektet skal have særligt fokus på at afdække årsagerne til den faldende deltagelse samt på hvorfor, der er en større gruppe kommuner, der fortsat ligger lavt i målingerne og hvad der er udfordringerne her. Det skal dels ske gennem dialog med kommunerne om årsagerne samt drøftelse af, hvad der skal til for få deltagerantallet op og ikke mindst højne niveauet for de lavest liggende 25%. I den forbindelse skal det også vurderes, om det kan være nødvendigt, ikke længere at arbejde med anonymitet i de landsdækkende opgørelser.

1.4. Gevinster

Gevinsterne ved projektet skal falde i kommunerne, hvor samarbejdet om informationssikkerhed via Baseline spørgerammen skal skabe bevidsthed og modne organisationerne ud fra en risikobaseret tilgang. Her har der de seneste år været fokus på den decentrale sikkerhedsorganisation i forvaltningerne, hvor der fortsat er behov for modning.



Anbefalinger til indsatser drøftes både på fysiske netværksmøder samt gennem det kommunale samarbejde om sikkerhed via Sikkerhedsprogrammets netværk, der faciliteres af KL. Netværket bidrager dermed til at øge kompetencerne hos de kommunale informationssikkerhedsmedarbejdere.

1.5. Resultatmål

På tværs af alle kommuner at udpege de områder, der bør have opmærksomhed og iværksætte fælleskommunale indsatser, hvor det skaber værdi for den enkelte kommune.

2. Leverancer og succeskriterier

Kommunernes Baseline værktøjskasse

I baseline undersøgelserne samles informationer om kommunernes status på informationssikkerhed, og det er et tilbud til kommunerne om værktøjer til at bearbejde egne resultater og indsatser.

Hvordan kan resultaterne anvendes i kommunerne

Undersøgelsen gennemføres på en digital platform, der giver kommunerne adgang til at følge egen udvikling og løbende benchmarke sig med andre kommuner. Hver kommune kan se sin egen score ift. de kommunale indsatsområder og kan derfor arbejde med egne udfordringer og prioritere indsatser derefter. KL har hidtil ikke kunnet se den enkelte kommunes besvarelser, da kommunernes data er anonymiserede. KL kan således alene se de samlede resultater, men opfordrer kommunerne

til at sammenholde egne resultater med landsresultatet eller andet de måtte finde bedst.

I platformen har kommunerne adgang til følgende værktøjer:

Digital platform med egen login og adgang til egne historiske data, som kan anvendes hele året

Analytiske værktøjer til at vurdere egen indsats – både historik og ved benchmark med andre kommuner

Understøttelse af kommunens besvarelse ved blandt andet mulighed for delegering af spørgsmål til andre i organisationen og ved oprettelse af organisationsenheder med ansvar for besvarelse

Samlet rapport på kommuneniveau.

Ledelsesrapport på forvaltningsniveau, hvor systemejere kan få egen status i forhold til resten af organisationen samt anbefalinger til indsatser.

Vidensdeling gennem fælleskommunalt netværk

Gevinsterne ved at facilitere det kommunale samarbejde om sikkerhed på en struktureret måde er, at kommunerne lærer af hinandens fejl og succeser og får kendskab til og mulighed for at benytte eksempelvis de rigtige leverandører og værktøjer til sikkerhedsarbejdet, fordi andre kommuner allerede har afprøvet dem. Der er med netværket god mulighed for at nå relevante medarbejdere med information.

Kommunerne vil ved at bruge netværket kunne spare mange ressourcer på at genbruge materialer vedrørende sikkerhedsarbejdet udviklet i andre kommuner. Fagområdet er præget af informationer med stor følsomhed, f.eks. når der samarbejdes om beredskabsplaner, risikovurderinger etc. Det er også her, vi opbygger og deler udvikling af fælleskommunale tiltag, og hvor KL og kommunerne kan kommunikere om følsomme informationer ift. konkrete sager og it-kriminalitet. Derfor sker samarbejdet i et lukket forum på platformen Microsoft Yammer. KL modererer Yammer-netværket tæt, så der ikke er uvedkommende med i netværket. KL administrerer derfor deltagerne enkeltvis, og fjerner og tilføjer adgang til kommunale medarbejdere efter direkte aftale med kommunernes kontaktpersoner.

De kommunale deltagere har udtrykt stor nytte af og stort behov for, at KL forsat samler, understøtter og stiller Yammer platformen til rådighed, da netværket bidrager til at øge kompetencerne hos de kommunale sikkerhedsfolk.

2.1. Modnings- og analysefasen

Da projektet er en videreføring, er modnings- og analysefasen allerede gennemført i forrige programperiode.

2.2. Gennemførelses- og implementeringsfasen

Kommunerne har adgang til deres egne baseline besvarelser på portalen på den digitale platform året rundt, og selve baseline analysen trækkes ud én gang årligt.

Undersøgelsens spørgeramme er udformet, så den afspejler organisationens samlede fokus på cyber- og informationssikkerhed – fra den øverste ledelse til de enkelte forvaltninger, medarbejderne og eksterne samarbejdspartnere. I kommunerne er besvarelser oftest koordineret og sikret af kommunens koordinator for informationssikkerhed og it-chefer.

En vigtig del af arbejdet med at øge informationssikkerheds niveauet i kommunerne er dels analysen, men også muligheden for at dele viden og sparring i det fælleskommunale netværk.

For at netværket fortsat er relevant for de kommunale informationssikkerhedsmedarbejdere skal det kontinuerligt evalueres, hvorvidt netværket opfylder deres behov, eller om noget skal justeres.

Dette kan ses gennem de indlæg, der skrives på Yammer-netværket, men KL får en mere nær evaluering gennem Sikkerhedsprogrammets fysiske netværksmøder. Her har kommunerne bl.a. mulighed for at påpege behov for yderligere eller ændrede tiltag fra KL på sikkerhedsområdet.

Leverancer

- KL baseline rapport med en samlet status og udvikling i kommunerne
- *Afrapportering til:*
 - Styregruppen
 - KL's direktion
 - KL's Arbejdsmarked- og Borgerserviceudvalg og bestyrelse
 - K98
- Informationssikkerhedsnetværket inkl. fysiske kommedage i nov. med workshop.
- Evaluering med skriftlig opsamling under Sikkerhedsprogrammets fysiske netværksmøder med kommunale kontaktpersoner.
- Løbende evaluering og moderation af Sikkerhedsprogrammets Yammer-netværk.

Succeskriterier

- Øget cyber- og informationssikkerhed i kommunerne
- Udbytte af de fælleskommunale initiativer, så sikkerhed øges
- KL forstår de kommunale informationssikkerheds medarbejderes behov for tiltag på sikkerhedsområdet.
- KL ved hvilke tiltag, der skal til for at netværket fortsat er aktuelt, aktivt og har de relevante medlemmer.

2.3. Gevinstrealiseringsfasen

Sker årligt i form af Baseline målingerne hvor der er fokus på øget modenhed i kommuner og igangsættelse af fælles initiativer, hvor det giver værdi.

Sikkerhedsprogrammet modererer og evaluerer på Yammer-netværket og gennemfører de kommunale fysiske rundrejser, hvor kommunerne orienteres og deres behov høres.

Kompetencer øges, og de kender deres kommunale kolleger bedre, så de har mulighed for at sparre om komplekse problemstillinger.

3. Budget

Budgettet er en sammenlægning af budgetterne for projekt 6.5 Analyser af status på Cyber- og informationssikkerhed i kommunerne og 6.6 Fælleskommunal videndeling om cyber- og informationssikkerhed. Desuden er budgettet for øvrige omkostninger (baseline værktøj) opskrevet med 200.000kr. Dette skyldes behovet for fortsat at analysere og følge cybersikkerhed og hændelser i 2024

Aktivitet/år	2021	2022	2023	2024	2025
Lønmidler				800.000	-
Øvrige omkostninger (Baseline værktøj)				200.000 700.000	-
Samlet finansiering				1.700.000	-

4. Tidshorisont

Projektet løber til udgangen af 2025. Men skal i overensstemmelse med governance for det fælles kommunale digitaliseringsprogram, årligt godkendes i styregruppe og KL's bestyrelse.

5. Risikovurdering af projektet

Projektets mulighed for at analysere niveauet for cyber- og informationssikkerhed og støtte kommunerne i at højne niveauet, kræver at kommunerne også fremadrettet ønsker at deltage i analyserne. Den faldende deltagelse gennem årene udgør en risiko ift. fortsat at have et korrekt billede af status på kommunerne cyber- og informationssikkerhed, og dermed at kunne arbejde med de rette områder, hvor der er behov for fælles kommunal understøttelse. For at imødekomme nedgangen, skal årsagen til frafald afdækkes og projektet skal gennem dialog med kommunerne undersøge deres behov for støtte og imødekomme det, hvor det er muligt.

En anden risiko kan være, hvis kommunerne ikke oplever fortrolighed på Yammer-netværket, hvilket kan føre til dalende aktivitet eller mindre mulighed for at vidensdele. Dette imødekommes ved kun at lukke medlemmer ind, som kontaktpersonerne selv har bedt om.

6. Interessentvurdering

De vigtigste interessenter i projektet er først og fremmest de kommunale kontaktpersoner til KL ift. cyber- og informationssikkerhed, de kommunale ledelser, KL's politiske udvalg og bestyrelse. Men også omverdenen i form af ministerier og regering.

7. Organisering

Jette Larsson, KL er projektleder på nærværende projekt. Projektet drives i Center for Digitalisering og Teknologi i regi af KL's Sikkerhedsprogram. Projektet drives i tæt samarbejde med kommunernes informationssikkerhedsansvarlige.