



Kommunernes Digitaliseringsprogram 2021-2025

Projektbeskrivelse

Delprogram 6 – Kommunalt værn mod cyberkriminalitet

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Side 1 af 7

1. Formål og baggrund

1.1. Baggrund

Væksten i sikkerhedsudfordringer mod offentlige myndigheder er bl.a. en væsentlig stigning i cybertrusler. Hvilket KLs analyser i kommunerne 2018-2022 også klart viser.

Alle lande oplever dette, men i et land som Danmark, der er langt mere digitaliseret end de fleste andre lande, giver det særlig anledning til at finde veje til at gardere sig mod disse.

De professionelle anbefalinger til forebyggelse og håndtering af disse trusler og angreb, er etablering af et landsdækkende analysecenter, der bl.a. via overvågning af trafikken på internettet, skal kunne varsle myndighederne om potentielle angreb, således at disse kan forebygges eller afværges. Et sådan center skal ligeledes kunne hjælpe myndighederne ved advarsler og angreb.

KL indgår sammen med kommunerne i samarbejdet om etablering af fælles overvågnings- og analysefunktioner på tværs stat, regioner og kommuner. Det sker i forlængelse af regeringens strategi for cybersikkerhed, og den strategi for Cyber- og informationssikkerhed i sundhedssektoren, som KL, Danske Regioner og Staten aftalte i januar 2019. Hensigten er at skabe et fælles overordnet samarbejde, for at kunne imødegå de hastigt udviklende cybertrusler mod offentlige myndigheder, her særligt med fokus på sundhedssektoren. Strategien indeholder en række initiativer, som bl.a. har afsæt i fælles varsling og beredskab.

Den nuværende strategi udløber ved årets udgang, hvorfor en ny revideret strategi vil foreligge i 1 kvartal 2023. Der vil ske en videreførelse af samarbejdet af det fælles overvågnings- og analysecenter, hvor det er aftalt at kommunerne skal opkobles fra 2023-2024.

Projektet er en del af det Kommunernes Digitaliseringsprogram 2021-2025, Delprogram 6.

1.2. Formål

Projektet planlægges til at vare til og med 2025. Det er ikke muligt at fastlægge alle formål og indsatser for hele denne periode, de første indsatser og udefrakommende krav til kommunerne kan og vil få betydning for de behovene for aktiviteter i dette projekt.

Projektets formål er:

- at synliggøre behov og konsekvenser for kommunerne ift. tilslutning til det fællesoffentlige analysecenter for cybersikkerhed

- i samarbejde med kommunerne at udarbejde en fælleskommunal analyse om mulige løsningsmodeller for kommunernes deltagelse i det nationale værn mod cyberkriminalitet
- i samarbejde med kommuner at pege på en mulig fælleskommunal løsningsmodel samt sikre opstart af projektet
- Understøtte opbygning af kompetencer til håndtering af cyberkriminalitet i kommunerne
- Understøtte vidensdeling mellem de ansvarlige kommunale ledere og medarbejdere

1.3. Projekt idé

Cybertruslen stiller nye og højere krav til kommunernes arbejde sikkerhed. Dette vil særligt komme til udtryk gennem krav til at indgå i det nationale arbejde med cybersikkerhed. Derfor til etableringen af et nationalt center for overvågning og analyse stille ændrede og øgede krav til kommunernes arbejde med cybersikkerhed. Kommunerne vil skulle samarbejde med det nationale center, og kan i varierende omfang få behov for selv at kunne lave øget overvågning og analyser ift. egne systemer og løsninger.

Udarbejdelse af analyser og anbefalinger om et sådan overvågnings- og analysecenter indgår i sektorstrategien for cyber- og informationssikkerhed i sundhedssektoren. Baggrunden for dette er den stigende digitalisering i den samlede sundhedssektor. Der håndteres store mængder sundhedsoplysninger digitalt og på tværs af mange enheder. Og der arbejdes for stadig mere samarbejde om behandling og pleje med øget digital udveksling af informationer til følge. De store mængder følsomme personoplysninger gør sundhedssektoren sårbar over for cyber- og informationssikkerhedshændelser – som fx et potentielt cyberangreb.

Der er ikke tvivl om, at der brug for et sådant overvågnings- og informationscenter ift. sundhedssektoren. Der ses allerede alvorlige cybertrusler mod sektoren. Det er også flere gange lykkedes cyber-kriminelle at gøre skade. Der er til sammenligning allerede etableret centrale overvågnings- og analysecentre på tele- og finansområdet.

Kommunerne er ikke de største aktører ift. sundhedsdata, og bl.a. ved nationale beredskabsøvelser er det blevet klart, at kommunerne ikke er de mest sårbare her. Men med væksten i kommunernes samarbejde med regionerne om sundhedsopgaverne, vil dette øges. Kommunerne har også andre samfundskritiske aktiviteter, der med tiden må forventes også at skulle indgå i, eller blive underlagt, nationale overvågningsaktiviteter i forlængelse af Statens Cyber- og informationssikkerhedsstrategi. Det er derfor en væsentlig overvejelse, i hvor høj grad der skal etableres overvågning alene for sundhedssektoren, samt hvordan der sikres koordinering med de øvrige samfundskritiske sektorer. Særligt for kommunernes muligheder for at kunne drive sikre og effektive IT-organisationer, er dette et væsentligt hensyn.

Der er en række forhold, som det kan være vanskeligt at få fuldt belyst inden der er brug for at træffe beslutninger. Det er dog helt sikkert, at dette vil få konsekvenser for kommunerne, da der bliver behov for investeringer i ny teknologi, ændrede kompetencer og flere ressourcer til arbejdet med sikkerhed. De lokale behov for analyse kapacitet vil overstige det, som enkelt kommuner kan håndtere, og der vil af den grund blive behov for at udarbejde en model for, hvordan kommunerne kan arbejde sammen om

opbygning af noget af den nødvendige kompetence og teknisk infrastruktur ift. at indgå i cyber-aktiviteter.

KL og repræsentanter fra kommunerne indgår i samarbejde med Sundhedsdatastyrelsen og regionerne i arbejdsgrupper om mulige modeller for etablering af et landsdækkende analysecenter på tværs af sundhedssektorens parter, hvor der også kigges på sammenhængen til øvrige sektorer.

Der blev i ØA21 og ØA22 aftalt og afsat midler til oprettelse og drift af det fælles overvågnings- og analysecenter. I første omgang var det alene midler til Sundhedsdatastyrelsen og regionerne, der er i gang med at implementere opkoblingen af regionerne. Det er hensigten, at kommunerne kobles gradvist på fra 2023–2024. KL fremlagde et oplæg ifb. med ØA22, som ikke blev indfriet. Det er målet, at KL igen fremlægger et oplæg til at indgå en aftale i forbindelse ØA23.

Dvs. der er krav på vej til kommunerne og der er på den baggrund behov for at afdække krav og de afledte konsekvenser for kommunerne både teknologiske, kompetencemæssige og økonomiske.

På EU-fronten er der også nye krav og nye direktiver på vej. EU har vedtaget et nyt NIS-direktiv (Sikkerhed i net- og informationssikkerhedssystemer i samfundskritiske sektorer) kaldet NIS2-direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen. Kommunerne er i dag ikke underlagt NIS-direktivet. Men med nuværende statslige cyber- og informationsikkerhedsstrategi der udover sundhed nu også omfatter affald, drikkevand og spildevand som samfundskritisk infrastruktur, er det forventet at kommunerne bliver omfattet af NIS2-direktivet. Det vil betyde, de bliver pålagt lovkrav, der vil stille nye krav til kompetencer, krav til national rapportering og som følge heraf vil øge omkostningerne. Omfanget af statens ønsker til implementering af NIS2-direktivet kendes p.t. ikke.

Der er på den baggrund udarbejdet et særskilt projekt vedr. NIS2 i regi af Delprogram 6, Digitale Fundamenter.

1.4. Gevinster

Gevinsterne ved projektet er, der skabes et samlet overblik over de økonomiske, teknologiske og kompetencemæssige konsekvenser for kommunerne ift. en tilslutning til overvågnings- og analyseenheden. Samtidig med at det vil være muligt for kommunerne i fællesskab at stille krav til dette, så det sikres, at der er størst mulig god sammenhæng til kommunernes øvrige aktiviteter.

Kommunerne er i størrelse, teknologisk og kompetencemæssigt meget uens. Såfremt kommunerne skal kunne opfylde kravene til øget cybersikkerhed, skal der udarbejdes mulige løsninger ud fra et need-to perspektiv.

1.5. Resultatmål

Sikre, at kommunerne er klar til at indgå i arbejdet mod cyberkriminalitet. Herunder arbejde for, at kommunerne opnår de bedst mulige løsninger, så de kan opfylde kravene om tilslutningen til det centrale overvågnings- og analysecenter.

Sikre kommunerne mulighed for at den nødvendige kompetenceopbygning ift. cybersikkerhed.

I samarbejde med kommunerne udarbejde forslag til et fælleskommunalt samarbejde på området, som kommunerne kan tage beslutninger om deltagelse i.

2. Leverancer og succeskriterier

2.1. Modnings- og analysefasen

Forventes at igangsættes i 1. kvartal 2022.

KL har ansvar for program- og projektledelsen fra start til slut. Herunder opbygning af en kommunal referencegruppe primært bestående af it-chefer og it-driftschefer, kommunikation til kommunerne og det politiske niveau.

Oplæg til et fælleskommunalt samarbejde kræver juridiske kompetencer samt teknologiske kompetencer inden for cybersikkerhed, hvor der er brug for at indkøbe ekstern konsulentassistance.

Leverancer
<ul style="list-style-type: none">• Opbygning af en kommunal referencegruppe• Opbygning af en adgangssikret digitalplatform til gavn for videndeling i projektet og kommunerne imellem• Oplæg til et fælleskommunalt samarbejde på cybersikkerhedsområdet.
Succeskriterier
<ul style="list-style-type: none">• Kommunerne forstår vigtigheden af projektet, og derfor deltager aktivt med videndeling og hårdt arbejde• Oplægget til et fælleskommunalt samarbejde får en kvalitet og afgrænsning, der sikrer, at kommunerne får et overblik over konsekvenserne ved tilslutningen ift. økonomi, jura og den værdi et fælleskommunalt samarbejde vil tilføre kommunerne.

2.2. Gennemførelses- og implementeringsfasen

Indholdet i denne fase vil afhænge af resultaterne i den første fase.

Såfremt der er fundet en brugbar fælleskommunal model, hvor kommunerne ønsker at indgå i et formelt samarbejde, oprettes et program/organisation til håndtering af opbygningen af det fælleskommunale samarbejde på cybersikkerhedsområdet.

Implementeringen af det fælleskommunale samarbejde og kommunernes opkobling afstemmes med det landsdækkende analysecenter i Sundhedsdatastyrelsen, DCISSund

Leverancer

- Oprettelse af program/organisation, der på kommunernes vegne får ansvaret for at udarbejde aftalegrundlag inkl. juridiske forhold samt betalingsmodel til et fælleskommunalt samarbejde på cybersikkerhedsområdet
- Involvering af de væsentlige interessenter

Succeskriterier

- Konsekvenser for kommunerne kendes ift. tilslutningen til det fælleskommunale samarbejde.
- Den kommunale topledelse og det politiske niveau er bekendt med konsekvenserne for kommunerne, og bakker op om vigtigheden af et øget cyber-forsvar i kommunerne

2.3. Gevinstrealiseringsfasen

Cybersikkerhed får den fornødne opmærksomhed i kommunerne, og bliver en integreret del af kommunernes fokusområder til gavn for borgere og ansatte.

Tilslutningen fra kommunerne til et fælleskommunalt samarbejde på cyberområdet er stor nok til, at der kan opbygges en organisation, der kan varetage og drifte, de aftalte leverancer.

Leverancer

- Det er ikke muligt at beskrive denne fase, før resultaterne af de første faser kendes

Succeskriterier

- Det er ikke muligt at beskrive denne fase, før resultaterne af de første faser kendes

3. Budget

Aktivitet/år	2021	2022	2023	2024	2025
Lønmidler	0	800.000	450.000	-	-
Øvrige omkostninger	0	900.000	400.000	-	-
Konsulentydelse – forplejning mv.					
Samlet finansiering	0	1.7 mio.	850.000	-	-

4. Tidshorisont

Vurdering af konsekvenser for kommunerne ift. tilslutningen til det centrale overvågnings- og analysecenter hos DCISSund foreligger i 2022.

For en fælleskommunal model, hvor kommunerne kan at indgå i et formelt samarbejde, til håndtering af samarbejde på cybersikkerhedsområdet foreligger senest i 3. kvartal 2023

5. Risikovurdering af projektet

Cyber-sikkerhed er i sin natur teknisk funderet, derfor er kommunikation og formidling til ledelse og politisk niveau svært og dermed forståelsen for nødvendigheden af investeringer i en risiko. Skal kommunerne have succes ift. at indgå i et fælleskommunalt samarbejde, er det nødvendigt med forståelse for, at cyber-angreb er komplekst og bliver mere og mere avanceret, så de fleste kommuner ikke vil kunne håndtere de udfordringer, det giver, og at der skal handles på det. Den største risiko for projektet er således, at det ikke lykkes at få opbakning i kommunerne hos topledelse og politisk niveau til et fælleskommunalt samarbejde.

6. Interessentvurdering

It-chefer og it-drifts-chefer er de primære interessenter. Det er vigtigt at denne målgruppe bakker op om løsningsforslagene og selv tager initiativ i egen kommune.

Kitas (Kommunale IT-chefer) bestyrelse er en vigtig kanal til at få adgang til de primære interessenter.

KLs ledelse, Kommunaldirektørerne og politisk niveau, skal involveres løbende og klædes på med de væsentligste budskaber og beslutninger fra projektet.

Tæt og løbende samarbejde med Sundhedsdatastyrelsen.

Styregruppen for delprogram 6 – Digitale fundament er væsentlige interessenter, da de skal træffe afgørende beslutninger, og som også står på mål for projektet.

7. Organisering

Projektleder Christian Christensen, Center og Digitalisering og Teknologi i KL er programleder på opgaven. Der udpeges en referencegruppe bestående af it-ledelse og teknisk kyndige fra kommunerne, som er repræsentativ for store, mellem store og små kommuner.

De teknologiske platforme til håndtering af Cyber-angreb er komplekse ligesom området er præget af hurtig teknologisk udvikling. Der er derfor brug for indkøb af eksterne ressourcer til projektet, der har indsigt i området.

Beslutninger og resultater i projektet skal koordineres og kommunikeres med de væsentligste parter i Cyber- og informationssikkerhedsstrategien for Sundhedsområdet, da kommunerne er part i denne strategi. De primære samarbejdspartnere er DCIS i Sundhedsdatastyrelsen og regionerne.



Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Side 7 af 7