Kommunernes Digitaliseringsprogram 2021-2025

Projektbeskrivelse

Delprogram 6 – Kommunalt værn mod cyberkriminalitet

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

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 2018-2021 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 i drøftelser 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.

Projektet bliver en del af det fælleskommunale program for informationssikkerhed.

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

- at analysere konsekvenserne for kommuner, da det forventes, at de bliver omfattet af NIS2-direktivet som følge af de kommende EU-krav på området og dermed indeholdt i den reviderede statslige cyber- og informationssikkerhedsstrategi.
- 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 ny cyberstrategi fra regeringen) . 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 kan overstige det, som enkelt kommuner kan håndtere, og der vil af den grund blive behov for at se på, hvordan kommunerne kan arbejde sammen om opbygning af noget af

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

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 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 tilrettelæggelse af tilkobling til centeret og beskrivelse af gensidige forventninger, krav mv. Det er hensigten, at kommunerne kobles gradvist på fra 2022 – 2023/24. KL forventer, at der vil være oplæg til at indgå aftale om dette i forbindelse med ØA22 – eller ØA 23.

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 bådeteknologiske, kompetencemæssige og økonomiske.

På EU-fronten er der også nye krav og nye direktiver på vej. EU ønsker gennemførelse af forslag til nyt NIS-direktiv (Net- og informationssikkerhed)- – kaldet NIS2-direktivet - om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen. Kommunerne er i dag ikke underlagt NIS-direktivet i den nuværende statslige cyber- og informationssikkerheds-strategi. Men med den kommende reviderede statslige cyber- og informationssikkerheds-strategi, der forventeligt lanceres ultimo 2021, vil inkludering af drikkevand og spildevand bevirke, at kommunerne bliver omfattet af NIS2-direktivet og pålagt krav, der vil stille nye krav til kompetencer, krav til national rapportering og øge omkostningerne.

1.4. Gevinster

Gevinsterne ved projektet er, der skabes et samlet overbliver 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-have perspektiv.

Kende konsekvenserne af det kommende NIS2-direktiv og dermed undgå overimplementering af direktivet.

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.

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

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

På baggrund af de første analyser, evt. udarbejde forslag til et fælleskommunalt samarbejde på området, som kommunerne kan tage beslutninger om.

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.

Analysefasen kræver teknologiske kompetencer inden for cybersikkerhed, hvor der er brug for at indkøbe ekstern konsulentassistance.

Leverancer
• Opbygning af en kommunal referencegruppe • Opbygning af en adgangssikret digitalplatform til gavn for videndeling i projektet og kommunerne imellem • Opbygning af analysekoncept, der skal sikre opfyldelse af projektets formål, gevinster og resultatmål
Succeskriterier
• Kommunerne forstår vigtigheden af projektet, og derfor deltager aktivt med videndeling og hårdt arbejde • Analysekonceptet får en kvalitet, der sikrer, at kommunerne får et brugbart værktøj ift. at indgå i forberedelse og planlægning af cyberakktiviteter

2.2. Gennemførelses- og implementeringsfasen

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

Kommunerne skal medvirke til besvarelse af analyse ift. kompetencer, teknologiske, organisatoriske og økonomiske behov.

Referencegruppen medvirker i fortolkninger og beslutninger af resultaterne.

Konklusioner og implementeringstakten for kommunerne afstemmes med projektet i Sundhedsdatastyrelsen og regionerne

Leverancer
• Udsendelse af analyseværktøj til kommuner • Evt. Forslag til et fælleskommunalt samarbejde på området

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

• Overblik over konsekvenser for kommunerne ift. krav om tilslutning til den centrale overvågnings- og analysecenter i Sundhedsdatastyrelsen • Konsekvenser for kommunerne af regeringens cyberstrateig (og NIS2-direktivet) er beskrevet (såfremt kommunerne bliver omfattet)
Succeskriterier
• Konsekvenser for kommunerne kendes ift. tilslutningen til den centrale enhed. • Samlet overblik, for kommuner og beslutningstagere • 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.

Leverancer
• Det er ikke muligt at beskrive denne fase, før resultaterne af de første fases kendes
Succeskriterier
• Det er ikke muligt at beskrive denne fase, før resultaterne af de første fases kendes

3. Tidshorisont

Vurdering af (økonomiske) konsekvenser for kommunerne ift. tilslutningen til det centrale overvågnings- og analysecenter forventes i første udgave i foråret 2022. Mere uddybende konsekvenser og anbefalinger for ventes gennemarbejdet i 2022.

4. 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. cyberstrusler, er det nødvendigt, at der cyber tages alvorligt og der handles på det. den største risiko ofr projektet, er således at det ikke lykkes at få ørenlyd og opbakning i kommunerne.

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

5. 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 og regionerne er afgørende for at kommunerne tilgodeses i deres valg af cyber-løsning, da kommunerne først kobles op i 2. fase og 3. fase efter regionerne, der kobles på i 1. Fase.

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

6. Organisering

Programleder Beth Tranberg, Center og Digitalisering og Teknologi i KL er programleder på projektet. 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 prægeret af hurtig teknologisk udvikling. Der er derfor brug for indkøb af eksterne ressourcer til projektet, der har indsigt i området, og som kender til prissætning.

Det er aftalt med Københavns kommune, at de er sparingsparter ift. teknologiske valg, da kommunen er langt med eget Cyber-værn, og der er brug for erfaringer fra den kommunale sektor.

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.