

Projektbeskrivelse til digitale initiativer

Projektbeskrivelse - fælles om cyberforsvar

Spor 5

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Side 1 af 7

1. Baggrund og projektidé

Baggrund

Kommunernes it-systemer og opgaver er samfundskritiske. Derfor er kommunerne fra juli 2025 omfattet af NIS2-direktivet, som stiller skærpede krav til cybersikkerhed. Kommunerne står med en stor opgave, som der er brug for at samle sig om.

Cyberangreb er ikke alene en trussel imod kommunale it-systemer, digitale løsninger og it-infrastrukturen ("teknikken") men en direkte og reel trussel imod data om borgerne i kommunen og den daglige borgernære service som kommunerne leverer – dvs. selve kerneopgaven i kommunen. Driftskontinuiteten i et digitaliseret samfund kræver, at systemerne holdes i gang, at de er sikre, og at der er tillid til dem.

Der er meget på spil i et højt digitaliseret samfund som det danske, med stor sammenhæng mellem myndigheders it-systemer, fælles infrastruktur og de ydelser, som kommunerne leverer. NIS2 vil i den kommende periode kræve et stort kommunalt fokus, som vil være styrende for indsatserne i projektet "Fælles om cyberforsvar".

Hvor står vi?

Kommunerne og KL har igennem de seneste år arbejdet fokuseret med at styrke kommunernes cyber- og informationssikkerhed. Der er således et fundament for en kommunal sektor, der er modstandsdygtig på cyber- og informationssikkerhed – også i tider med et stigende trusselsniveau.

Ikke desto mindre er de kommunale ressourcer og kompetencer under pres – i høj grad ift. cyber- og informationssikkerhed. Variationen i sikkerhedsniveau og indsatser er desuden stor. I strategiperioden er der behov for at få mest muligt ud af fælles ressourcer og have blik for, hvordan enkelte greb og redskaber kan hjælpe over en bred kam. Det giver bl.a. udgangspunkt for at samle kommunerne om et fælles blik på særligt kritiske it-systemer.

Samtidigt har der ikke før været stillet krav til kommunernes cyber- og informationssikkerhed. På databeskyttelsesområdet har GDPR i høj grad været driver for arbejdet med beskyttelse af de registreredes rettigheder.

På cyber- og informationssikkerhed er der nu NIS2, som væsentlig lovgivning, som kommunerne som helhed er underlagt. Det giver fornyet anledning til at arbejde med øvrige understøttende krav, standarder og rammeværk. NIS2 løfter i sig selv barren for kommunernes indsats samt udpeger en række indsatsområder.

NIS2 vil således i den kommende periode være en væsentlig og tværgående rettesnor, der vil have stor betydning for kommunernes arbejde (organisatorisk, teknisk og ift. procedurer mv.) med cyber- og informationssikkerhed. KL og kommunerne samt en række fælleskommunale samarbejder har taget hul på arbejdet. Dette arbejde vil blive udbygget og anvendelsen af det vil blive understøttet, så kommunerne understøttes i deres implementering af NIS2-krav mhp. at styrke cybersikkerheden og dermed beskyttelsen af centrale ydelser og tjenester.

I strategiperioden arbejdes der i et parallelt spor på etablering af nye fælleskommunale driftsenheder. Disse driftsenheder vil på sigt styrke kommunernes cyber- og informationssikkerhed i en sikker og stabil it-drift. Konsolideringen og samling af it giver nye muligheder men kræver også fokus på, hvordan sikkerhed tilrettelægges i nye og store organisationer. Der vil i de to projekter ske udveksling af viden samt være fælles opmærksomhed på kommunernes samlede sikkerhedssituation.

Opgaven foran os

I denne strategiperiode skal projektet bidrage til, at kommunernes cyber- og informationssikkerhed når et niveau, hvor der samlet set arbejdes mere systematisk med sikkerhed, og hvor kommunerne kan inspirere hinanden. Cyber- og informationssikkerhed skal blive del af den almindelige topledelsespraksis, som understøttes af den kommunale forvaltning, som det også følger af NIS2, der betoner ledelsesansvar og sætter fokus på procedurer og indsatser inden for en lang række emner.

Der skal fx arbejdes målrettet med videndeling om centrale NIS2-principper som risikostyring, sikkerhed i forsyningskæden, håndtering af hændelser og ledelsens ansvar for implementering samt tilsyn.

Dette projekt giver forudsætninger og bistår til, at det lykkes for kommunerne.

NIS2 har fokus på samfundssikkerheden og dermed indsatser samt arbejds- og rolledeling på tværs af alle omfattede enheder og de sektoransvarlige myndigheder, der har ansvar for vejledning, tilsyn mv.

Som del af det danske samfund skal projektet bidrage til, at kommunernes arbejde med cyber- og informationssikkerhed så vidt muligt er indtænkt i det nationale arbejde og prioriteter. Kommunal sikkerhed kan ikke ses helt adskilt fra andre offentlige myndigheder (særligt SAMSIK og Ministeriet for Samfundssikkerhed og Beredskab), leverandører og fælleskommunale samarbejder og it-driftsenheder, der også kan løfte en betydelig del af opgaven.

Projekt idé

Målsætning

Projektet skal gøre det lettere at være digital kommune, der er omfattet af NIS2, hvor risikoen for alvorlige sikkerhedshændelser og konsekvenserne, når hændelser alligevel rammer, holdes nede.

Afsæt

Projektet bygger videre på indsatser, erfaringer og redskaber fra KL og kommunernes hidtidige samarbejder om cyber- og informationssikkerhed. Det omfatter KL-Baseline til kommunernes modenhedsmåling ift. cyber- og informationssikkerhed, understøttelse af NIS2-implementering, netværk for sikkerhedsmedarbejdere, materiale og støtte på KLs Videnscenter samt dialog og indsatser med fælleskommunale samarbejder og relevante statslige styrelser og ministerier.

Der er fortsat efterspørgsel fra kommunerne ift. flere af de centrale elementer fra forrige indsatser samt stigende opmærksomhed på og efterspørgsel efter greb til at styrke arbejdet med NIS2. Disse kan med et fornyet fokus pege frem på målet om at kommunerne mere struktureret og med styrket ledelsesforankring kan arbejde med at styrke cyber- og informationssikkerhed med passende rolle/ansvarsfordeling.

Der er stigende fokus på, at der med fordel kan gives fælles svar på nogle af de opgaver, som NIS2 pålægger de enkelte kommuner. Det gælder f.eks. behov for fælles forståelse af og håndtering af kritiske opgaver, der løses i alle kommuner og håndteringen af de tilhørende systemer. Her anviser nationale strategier og vejledninger ikke i tilstrækkelig grad retning. Der er behov for at kigge på, hvordan kan dette håndteres, når den enkelte kommune har et selvstændigt ansvar for risici og sikkerhed ift. opgavevaretagelsen, men kommunerne i stor udstrækning mødes af de samme udfordringer.

Tilgang

Projektet vil være delt i flere fokusområder, der alle vil understøtte den fælles målsætning om at gøre det nemmere at være en digital og sikker kommune. Erfaringen fra den foregående periode er, at emner og indsatser er tæt forbundet, og at der er brug for at se og arbejde samlet med dem. Dette er endnu vigtigere i en strategiperiode, hvor der skal arbejdes fokuseret med ny lovgivning i form af NIS2.

Initiativet inddeles til en start i tre overordnede spor, hvor målsætningerne og fremgangsmåden kort er beskrevet nedenfor.

- **Videndeling, organisation og kompetencer**
 - o Fortsat arbejde med KL-baseline survey, med tæt sammenhæng til behov for redskaber eller andre indsatser, særligt ifm. NIS2.
 - o Gode formater for ledelsesinformation samt fokus på anvendelse og styrkelse af kompetencer. Understøtte kommunernes arbejde med at være en organisation gearret til styrket og varig sikkerhed via videndeling i bl.a. dialogportal og KL-videnscenter og ved fysiske arrangementer. mv.
- **Tværgående sikkerhed og samarbejder**
 - o Tydeliggøre og understøtte snitflader og opgavedeling mellem kommunerne, kommunale samarbejder, styrelser mv. med fokus på hvordan kommunerne understøttes ift. arbejdet med NIS2.
 - o Fremme understøttelse af kommunernes sikkerhedsarbejde gennem tværkommunale samarbejder, herunder med særsomt fokus på NIS2-kravet om håndtering og videndeling om hændelser gennem KommuneCERT.

- Styrket sammenhæng mellem arbejdet med beredskab og cybersikkerhed.
- **Fælles NIS2-indsatser**
 - Bygge videre på drejebøger og redskaber til kommunernes implementering af NIS2. Særligt fokus fra start på 'Tekniske afklaringer' og 'Tilsyn'.
 - Fokus på udvalgte (fælles) kritiske opgaver og systemer ift. samfundskritikalitet og behov for driftskontinuitet, så kommunerne er fælles om det vigtigste og dér, hvor it-understøttelsen er den samme.

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Side 4 af 7

I strategiperioden vil der opstå eller ske modning af behov for aktiviteter under det overordnede initiativ. Det kan afstedkomme yderligere analyseopgaver eller anskaffelser/leverancer. Derfor sikres et tæt samarbejde med en kommunal referencegruppe.

På tværs

Initiativet understøttes af en referencegruppe, hvorunder der kan nedsættes enten varige eller midlertidige arbejdsgrupper, der har et mere specifikt sigte og opgaver.

Der oprettes et Netværk for Cyber- og Informationssikkerhed, der forventes at afholde to fysiske og et online møde hen over året, for at sikre videndeling, dialog og inspiration. Netværket opstartes i 2026 og fortsætter strategiperioden ud, hvis der er kommunal tilslutning til det. Det forventes, at Netværket særligt har fokus på elementer i NIS2 i implementeringsfasen.

Der etableres en årlig kommune-dag for cyber- og informationssikkerhed, hvor nye initiativer og produkter kan introduceres, og hvor (foruden KL) eksterne parter, fælleskommunale samarbejder og kommunerne kan dele viden og sikre inspiration.

Der kommunikeres og videndes løbende på KL's Videnscenter og KL's Dialogportal for Sikkerhedsprogrammet. Her skal information, cases mv. deles til understøttelse af det overordnede fokusområde, dér hvor den kommunale efterspørgsel er størst.

2. Resultatmål

Projektet skal måles på:

1. Kommunerne understøttes i at styrke samt tilrettelægge og strukturere egen indsats ift. NIS2 i særdeleshed og cyber- og informationssikkerhed mere generelt.
2. Projektet opretholder dialog og samarbejde med Styrelsen for Samfundssikkerhed, således at vejledning mv. giver kommunerne en god rettesnor ift. efterlevelse af lovgivning (specifikt NIS2).
3. Projektet og kommunerne indgår i et sikkerhedsarbejde med særligt fokus på NIS2, der går på tværs af myndighedsniveau, sektorer

samt kan udnytte fordelene ved eksisterende fælles kommunale samarbejder.

Weidekampsgade 10
Postboks 3370
2300 København S

3. Leverancer

www.kl.dk

Side 5 af 7

Videndeling, organisation og kompetencer

- Årlig afrapportering til kommuner om baseline-analyse samt opfølgning på resultater mhp. at sætte retning for øvrige indsatser.
- Brug af kommunikationskanaler såsom dialogportal og videncenter til at sprede viden og redskaber samt skabe udgangspunkt for kommunalt fællesskab omkring arbejde med sikkerhed.

Tværgående sikkerhed og samarbejder

- KL og kommunerne indgår i nationale fora for cyber- og informationssikkerhed, hvor kommunerne som sektor indgår i nationalt arbejde og indsatser.
- KL understøtter koordinering og samarbejder med relevante fælleskommunale parter.
- KL indgår i nationale beredskabsøvelser med kommunerne.

Fælles NIS2-indsatser

- Udbygning af redskaber og eksempler fra NIS2-afprøvninger.
- Fælles redskaber og eksempler udbredes.
- Opbygning af kommune-dialog til revidering, opdatering og anvendelse af NIS2-redskaber.
- Overblik over særligt kritiske it-systemer/opgaver samt fælles tilgang til håndtering på relevant niveau.

Tværgående

- Oprettelse af kommunalt netværk for cyber- og informationssikkerhed til videndeling og drøftelse af aktuelle emner, udfordringer og løsninger.
- Årligt cyber- og informationssikkerhedsdag i konference-format med mulighed for eksterne oplægsholdere, nyt fra KL/projektet samt case og eksempler fra enkelt kommuner og kommunale samarbejder.
- Løbende levering af indhold til videncenter.
- Løbende rådgivning af kommunerne på strategiens fokusområder.

4. Tidsplan

Projektets tre spor forventes at arbejde med de anviste temaer i de kommende 4 år. NIS2 vil som minimum i implementeringsfasen være drivende for indsatser og prioriteringer i projektet. Konkrete aktiviteter under sporene blive afsluttet eller justeret, ved behov for nye aktiviteter.

Indsatserne kan bl.a. udvides og tilpasses ift. efterspørgsel samt evt. nye eller reviderede lovkrav mv.

Weidekampsgade 10
Postboks 3370
2300 København S

Projektlederne anbefaler, at projektbeskrivelsen genbesøges halvvejs igennem strategiperioden, med fokus på, om projektbeskrivelsen fortsat er dækkende og matcher behovet for fælleskommunale aktiviteter ift. cyber- og informationssikkerhed. Herunder om NIS2-indsatsen er ved at gå fra implementerings til driftsfase samt hvilken betydningen dette har for prioriteringer og aktiviteter i projektet.

www.kl.dk

Side 6 af 7

Modnings- og analysefasen

Projektet er en fortsættelse af etablerede indsatser og samarbejder og der vil løbende ske modning af nye tiltag i samarbejde med kommunerne. Og som vil blive forelagt digitaliseringsrådet.

5. Organisering og ansvar

Roller	Navn og/eller organisation
Projektejer	Pia Færch
Projektleder	Simon Schönenberg, samt Carsten Stange Marianne J. Mortensen
Kommunal inddragelse	5-10 kommuner indgår i referencegruppe på tværs af projektet. Alle kommuner inddrages i netværk og større arrangementer. Der nedsættes efter behov kommune-gruppe med dedikeret fokus på konkrete delleverancer og produkter.
Øvrige samarbejdspartnere	- Styrelsen for Samfundssikkerhed/Ministeriet for Samfundssikkerhed og beredskab - KOMBIT - Kommuncert - Komponent - SKI - Databehandlersekretariatet (DBS).



Roller	Navn og/eller organisation
Forventet drift	Ikke forventning om nyt, der skal i drift. Driften af Baseline-plattform fortsættes. Den ejes og forvaltes af udbyder. Projektet finansierer anvendelse til Baseline og kommunernes basisanvendelse af platformen.

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Side 7 af 7