

Sammen om NIS2

– hvordan fælleskommunale samarbejder
støtter implementering af NIS2 i kommunen



Baggrund

NIS2 er et EU-direktiv, som implementeres i Danmark for at styrke og ensarte indsatsen for cybersikkerhed. Direktivet stiller skærpede krav til ledelsesansvar, sikkerhed i forsyningskæder, hændelsesrapportering, kompetencer og en række tekniske og organisatoriske foranstaltninger. Disse skal – med udgangspunkt i en risikovurdering af samfundskritikalitet og driftskontinuitet – omsættes til konkrete indsatser. Kommunerne er som helhed omfattet af NIS2, klassificeres som væsentlige enheder og er underlagt tilsyn og sektoransvar hos Styrelsen for Samfundssikkerhed (SAMSIK).

Læs mere om NIS2-loven og de tilhørende vejledninger på:
<https://samsik.dk/nis2/>

Kommunerne blev omfattet af NIS2-lovgivningen den 1. juli 2025. Som omfattede enhed bærer kommunen, ansvaret for at kravene i NIS2-loven efterleves og at cybersikkerheden er tilstrækkelig – både internt og hos eksterne leverandører.

For at løfte opgaven effektivt, kan kommunen med fordel benytte sig af eksisterende fælleskommunale samarbejder. Den politiske aftale om kompensation til kommunerne for implementering af NIS2 forudsætter netop, at omkostningerne holdes nede gennem tværkommunale samarbejder og fælles løsninger.

KL, KOMBIT, KommuneCERT, SKI, Komponent og DBS har udformet denne pjece, som beskriver de opgaver og den vejledning, som disse fælleskommunale samarbejder tilbyder som understøttelse til kommunens arbejde med NIS2.

Formål

Pjecen har til formål at give overblik over, hvilke opgaver der kan løses som en del af et fælleskommunalt samarbejde, og dermed klarhed over, hvem der kan bidrage med hvad. Pjecen behandler følgende emner:

- Leverandørkædesikkerhed
- Overvågning og hændelseshåndtering
- Kompetencer og uddannelse i cybersikkerhed
- Inspirationsmaterialer fra kommunale NIS2-konceptafprøvnings

Leverandør- kædesikkerhed

NIS2-loven pålægger kommunen flere nye forpligtelser i forhold til deres it-leverandører med krav om sikkerhedsforanstaltninger. Formålet er, at kommunen skal sikre sig, at deres leverandører lever op til de sikkerhedskrav, der er nødvendige for at kommunen kan overholde NIS2-loven. Sikkerhedsforanstaltningerne fastlægges med udgangspunkt i krav i NIS2-loven og i en risikovurdering i forhold til den konkrete it-leverandør.

It-leverandørerne skal implementere en række passende foranstaltninger til styring af cybersikkerhedsrisici.

Det giver opgaver med at sikre, at it-leverandørerne pålægges relevante krav til foranstaltninger, at de dokumenterer overholdelsen af disse krav, samt fører tilsyn med at kravene overholdes.

SKI, DBS og KOMBIT kan i samarbejde løse flere af disse opgaver på vegne af kommunen, så kommunen kan fokusere på de risikovurderinger, der er nødvendige ift. den generelle informationssikkerhed.

SKI, DBS og KOMBIT kan på vegne af kommunen sikre, at it-leverandører pålægges de krav til sikkerhedsforanstaltninger, der som et minimum må anses for passende ved kommunens anskaffelse af et it-system eller en it-løsning.

Det er en fælles ambition for SKI, DBS og KOMBIT, at der stilles ensartede sikkerhedskrav til leverandørerne – dels for at sikre, at kravene er på rette niveau, og dels for at gøre det nemmere for kommunen at tilgå relevante krav. SKI, DBS og KOMBIT vil også benytte samme struktur i opfølgingsarbejdet overfor leverandørerne for at sikre opmærksomhed på de samme ting på tværs af kommunernes aftaler.



SKI

SKI har indarbejdet relevante sikkerhedskrav i deres aftaler. Kravene indgår i - eller kan tilvælges som - en del af indkøbet på rammeaftaler eller på dynamiske indkøbssystemer (DIS). SKI's aftaler dækker også behov for indkøb af produkter, ydelser og services på it-området, og kommunen kan således anskaffe sikkerhedsløsninger og rådgivning, som understøtter implementeringen og arbejdet med NIS2.

Kommunen kan vælge mellem at købe ind på rammeaftaler, hvor sikkerhedskravene i forhold til NIS2 er obligatoriske for leverandørerne, eller på DIS, hvor rammerne er mere fleksible. I DIS kan kommunen vælge at bruge SKI's sikkerhedsbilag, tilpasse det eller definere egne sikkerhedskrav som en del af kontrakten.

På alle aftaler med obligatoriske sikkerhedskrav sørger SKI for at indhente og gennemgå revisionserklæringer samt følge op på revisionsbemærkninger overfor leverandøren. Den opfølgning gøres tilgængelig for kommunen, der kan bruge den som grundlag for deres NIS2-efterlevelse.

SKI følger aktuelt op i forhold til NIS2 på følgende områder: it-konsulenter, kommunikationsprodukter (kommende aftale), tablets (kommende aftale), tele & data (kommende aftale). På den måde minimeres kommunens egen opfølgning til eventuelle ekstra specifikke sikkerhedskrav, som den enkelte kommune måtte have stillet ved kontaktindgåelse.

På sikkerhedsområdet arbejder SKI tæt sammen med Styrelsen for Samfundssikkerhed (SAMSIK) for at sikre, at krav og vejledninger baseres på det aktuelle risikobillede.

SKI arbejder systematisk på at opdatere sikkerhedskravene i aftalerne i takt med genudbud og opdateringer, så de forbliver i overensstemmelse med NIS2.

Læs mere her: www.ski.dk/emne/informationssikkerhed/

KOMBIT

KOMBIT sikrer, at NIS2-kravene indgår i KOMBIT's udbud og drift af it-løsninger på vegne af kommunen.

KOMBIT indarbejder relevante sikkerhedskrav i forbindelse med egne udbud og i de efterfølgende driftsaftaler. KOMBIT sørger for at indhente og gennemgå revisionserklæringer samt følge op på revisionsbemærkninger overfor leverandøren. KOMBIT's opfølgning gøres tilgængelig for kommunen, som kan bruge den som grundlag for deres NIS2-efterlevelse.

KOMBIT's kravkatalog kan stilles til rådighed til brug for kommunen, hvis dette ønskes.

Læs mere på: <https://dok.kombit.dk/sikkerhed>

Databehandlersekretariatet (DBS)

DBS tilbyder at løse NIS2-opgaver for foreningens medlemskommuner. Alle kommuner kan blive medlem af DBS ved at henvende sig til foreningens sekretariat.

Aftaler om krav til foranstaltninger med it-leverandører:

DBS tilbyder medlemskommunerne at identificere og aftale minimumskrav til sikkerhedsforanstaltninger, som er passende i forhold til efterlevelsen af krav i lovgivning, vejledninger eller besluttet i fællesskab blandt medlemskommunerne. Den endelige aftale bestående af disse krav samt eventuelle supplerende krav skal forhandles og indgås endeligt af medlemskommunerne - på samme måde som ved forhandling af databehandleraftaler.

Dokumentationspakker:

DBS tilbyder, at medlemskommunerne får adgang til den nødvendige dokumentation fra it-leverandører til blandt andet at udarbejde risikovurderinger. DBS samler dokumentationen i dokumentationspakker og stiller dem til rådighed for medlemskommunerne.

Tilsyn med it-leverandører:

DBS tilbyder - på samme måde som ved sekretariatets tilsyn med databehandleraftaler - at gennemgå it-leverandørernes dokumentation for efterlevelse af krav på baggrund af NIS2-lovgivningen. DBS sikrer, at der er dokumentation for de aftalte krav, følger op overfor leverandørerne og rapporterer omfanget af efterlevelsen til medlemskommunerne.

Læs mere på: <https://kommunedbs.dk>

Overvågning og hændelseshåndtering

KommuneCERT

KommuneCERT er kommunernes fælles operative cybersikkerhedsenhed, der har til opgave at opdage og reagere på cyberangreb. Det foregår typisk gennem monitorering af netværk og it-systemer samt analyse og håndtering af cyberhændelser. KommuneCERT er under opbygning.

KommuneCERT kan stå for den lovpligtige overvågning af systemer, netværk og enheder. Det vil sige bidrage til, at cyberhændelser opdages, håndteres og – inden for 24 timer - indberettes til Styrelsen for samfundssikkerhed (SAMSIK), der er national cybersikkerhedsmyndighed. Som led i NIS2 er der lagt op til, at KommuneCERT bliver et fælles kommunalt led mellem hver kommune og den øvrige nationale overvågnings- og varslingsstruktur.

Samarbejde via KommuneCERT, der leverer 24/7/365 overvågning, betyder, at kommunen kan nøjes med vagtordninger, så kommunen ikke selv behøver døgnbemandet cyberoovervågning.

Læs mere på: <https://kommunecert.kombit.dk>

Kompetencer og uddannelse i cybersikkerhed

NIS2-loven stiller krav til kompetencer og uddannelse. Der stilles krav om, at medlemmer af kommunens direktion skal deltage i relevante kurser om styring af cybersikkerhedsrisici. Kravet skal ses i lyset af det ansvar, som direktionen har for cybersikkerheden i kommunen. Kurserne skal således gøre ledelsen i stand til at vurdere risici, træffe beslutning og følge op på kommunens cybersikkerhedsforanstaltninger.

Direktionen skal som samlet ledelsesorgan have de nødvendige kompetencer til at styre cybersikkerheden i kommunen. Det er ikke et krav, at alle eller et bestemt antal medlemmer af direktionen har gennemført kurser.

Derudover skal kommunen sikre, at relevante medarbejdere modtager den nødvendige træning og uddannelse i cybersikkerhed, så de kan håndtere relevante sikkerhedsrisici og bidrage til kommunens cybersikkerhed.

Kommunernes Cybersikkerhedsskole

Kommunernes Cybersikkerhedsskole er etableret af KL, KOMBIT og Komponent – kommunernes udviklingscenter - for at styrke kommunernes arbejde med cybersikkerhed. Skolen tilbyder målrettede kurser og uddannelsesforløb, der løfter kompetenceniveauet hos politikere, ledere, specialister og medarbejdere i kommunerne.

Indholdet i skolen udvikles løbende med henblik på at understøtte kommunernes implementering af NIS2.

Kommunernes Cybersikkerhedsskole tilbyder:

- Opdateret viden og praksisnære værktøjer: Bliv klædt på til at håndtere de komplekse krav til cybersikkerhed i hverdagen og styrk kommunens kerneopgaver.
- Et stærkt fællesskab på tværs af kommuner: Deltagelse i et helt særligt kommunalt fællesskab med erfaringsudveksling og samarbejde, hvor fælles udfordringer og løsninger deles.
- Ledelse af cybersikkerhed: Styrk ledelsens forståelse og evne til at styre arbejdet med cybersikkerhed.

Læs mere på:

www.komponent.dk/kommunernes-cybersikkerhedsskole



Inspirationsmaterialer fra kommunale NIS2-konceptafprøvninger

KL gennemfører et fælleskommunalt projekt, som har til formål at støtte kommunen i implementering af NIS2. I projektet udvikles og formes en række redskaber og inspirationsmaterialer, som kan anvendes af kommunerne i deres arbejde med NIS2.

Projektet er opbygget omkring en række konceptafprøvninger, hvor få kommuner afprøver redskaber på særligt centrale elementer af NIS2. Erfaringer og input fra de deltagende kommuner samles i en drejebog med tilhørende materialer, skabeloner mv., som stilles til rådighed for alle kommuner.

Drejebøgerne tager afsæt i de krav, NIS2 stiller til kommunens cybersikkerhedsforanstaltninger og gør dem - gennem afprøvningerne i udvalgte kommuner - operationelle i en kommunal kontekst. Formålet er, at den enkelte kommune får overskuelige værktøjer, som kan anvendes til at understøtte den lokale NIS2-implementering og efterlevelse af NIS2-kravene - og ultimativt højne cybersikkerheden i kommunen.

Læs mere om konceptafprøvningerne og følg arbejdet her:

<https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed/cyber-og-informationssikkerhed/implementering-af-nis-2>

Sammen om NIS2 – hvordan fælleskommunale samarbejder støtter implementering af NIS2 i kommunen

© KL, KOMBIT, KommuneCERT, SKI, Komponent og DBS
1. udgave, 1. oplag, november 2025

Produktion: Kommuneforlaget A/S
Design: Kommuneforlaget A/S
Foto: Colourbox

Produktionsnr. 831090

