KOMBIT A/S
Halfdansgade 8
2300 København S

Tlf. +45 33 34 94 00
kombit@kombit.dk
www.kombit.dk

CVR-nr.: 19435075
EAN-nr. 5790001969370

Forsvarsministeriet

22. august 2024

Høringssvar til udkast til
Forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau

KOMBIT indkøber og forvalter en række af de største og mest udbredte it-løsninger for landets 98 kommuner. Det gælder bl.a. for it-løsninger, der sikrer borgerne nogle af de mest centrale velfærdsydelser indenfor den kommunale forvaltning på social-, sundheds- og beskæftigelsesområdet. KOMBIT står også for den nye valg-løsning. En væsentlig del af de it-løsninger, kommunerne anvender, er samfundskritiske og kan dermed også være oplagte mål for ondsindede aktører, der måtte ønske at skade Danmark og danskerne. Cybersikkerhed i den kommunale digitale forvaltning er derfor et kerneområde i KOMBITs strategi.

KOMBIT hilser Forsvarsministeriets udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-lovforslag) velkommen. Reguleringen har potentialet for at skabe et stærkt fundament for den digitalisering, der understøtter samfundskritiske tjenester i Danmark. Det er imidlertid en forudsætning, at det bagvedliggende NIS2-direktiv implementeres med danske forhold for øje. Dette omfatter nødvendigvis også den kommunale struktur, hvor langt størstedelen af borgernes møde med det offentlige foregår, herunder ikke mindst digitalt og tværsektorielt.

1. Implementering efter danske forhold

På den baggrund finder KOMBIT ikke, at cybersikkerheden i kommunerne er tilstrækkeligt varetaget i NIS2-lovforslaget. Det afspejler ikke strukturen, hvor hver enkelt kommune er bemyndiget til som én juridisk enhed at løse opgaver på tværs af sektorer. Desuden tager lovforslaget ikke tilstrækkeligt klart og præcist højde for, at den kommunale digitalisering er bygget op omkring netværk og infrastruktur, der er sammenhængende og effektiv på tværs af sektorer.

Det bagvedliggende NIS2-direktiv giver en udtrykkelig mulighed for at lade kommuner som helhed være omfattet af NIS2-lovforslaget og dermed understøtte en sammenhængende, ensartet og effektiv sikring af cybersikkerheden for kommunerne. Det er fravalgt.

NIS2-lovforslaget har reelt store indirekte konsekvenser i kommunerne, og det vil koste kommunerne langt mere end estimeret i lovforslaget. Dog udelades at lade kommunerne som helhed være omfattet. Der nævnes i lovforslaget et usikkert estimat for udgifter i kommunerne på 95 – 280 mio. kr. årligt foruden såkaldte ”negative implementeringskonsekvenser”.

2. Den sektorspecifikke tilgang til sikring af informationssikkerhed

Forsvarsministeriet har i lovforslaget fremhævet, at det på nuværende tidspunkt ikke er intentionen at fastsætte regler om, at kommunerne som helhed omfattes af loven. Kommunerne vil dog kunne være direkte omfattet, når de udøver aktiviteter indenfor de sektorer, som udtrykkeligt nævnes i NIS2-lovforslaget. De eksisterende organisatoriske og tekniske forhold, der knytter sig til kommunernes virke, indebærer imidlertid, at kommunerne i praksis vil blive ramt af kravene i lovforslaget i langt større omfang:

Organisatoriske udfordringer
Kommunerne udøver både aktiviteter, der er omfattet af de i NIS2-lovforslaget nævnte sektorer, og aktiviteter der ikke er omfattet. I de ikke omfattede aktiviteter vil der ikke desto mindre alligevel skulle gennemføres risikobaserede foranstaltninger til sikring af informationssikkerheden for de it-løsninger, der benyttes. Kommunen står dermed tilbage med en risiko for uhensigtsmæssig differentiering i implementering af sikkerhedskrav, som skaber en kompleksitet, der i sig selv er en risiko for cybersikkerheden. En risiko, der kan nedbringes ved at implementere det strengeste regelsæt; altså det der gælder for væsentlige enheder i NIS2-lovforslaget.

Tekniske udfordringer
Ud fra et teknisk perspektiv er det heller ikke muligt at operere med en sektorspecifik sondring. Det skyldes som nævnt, at kommunernes digitalisering i vid udstrækning er helhedsorienteret. Dvs. at en stor del af infrastrukturen fungerer på tværs af kommunens forvaltningsområder. Dette er såvel økonomisk som sikkerhedsmæssigt en fornuftig model. Det er med andre ord ikke muligt at udskille den del af netværk og anden infrastruktur, der stilles sektorspecifikke krav til i medfør af NIS2-lovforslaget. Derfor vil kommunerne også her skulle implementere det strengeste regelsæt; altså det der gælder for væsentlige enheder i NIS2-lovforslaget.

Konsekvensen af lovforslaget for kommunerne bliver dermed utilsigtet overimplementering, uanset hvor meget det fremhæves af Forsvarsministeriet, at der er tale om minimumsharmonisering.

På den baggrund vil det blive op til den enkelte kommune at sikre en sammenhængende, ensartet og effektiv sikring af cybersikkerheden, der bygger bro over en unødig kompleksitet, som NIS2-lovforslaget pt. lægger op til. I praksis vil lovforslaget føre til, at en kommune skal kunne efterleve forskellige statslige sektormyndigheders bekendtgørelser for de dele af kommunens virke, der er omfattet af NIS2-lovgivningen. Derudover bliver det nødvendigt at implementere tilsvarende sikkerhedskrav for de dele af kommunens virke, der falder udenfor NIS2-lovgivningen. Dette kan undgås ved at lade kommunerne som helhed være omfattet af lovforslaget.

KOMBIT

3. Kommunernes leverandører er omfattet af NIS2-lovforslaget

Der må desuden forventes en udgiftstung konsekvens for kommunerne som følge af, at KOMBIT og KOMBITs største leverandører ser ud til at blive omfattet af NIS2-lovforslaget som væsentlige enheder af typen "udbyder af administrerede tjenester". Denne type enhed hører til Forvaltning af IKT-tjenester (business-to-business), som er en af de nye sektorer, der fremgår af NIS2-direktivet.

Udbyder af administrerede tjenester er defineret som: "En enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand."

Uanset et allerede højt niveau af cybersikkerhed vil der været store udgifter forbundet med, at nye regulatoriske sikkerhedskrav rammer kommunernes leverandørkæde, der forvaltes af KOMBIT. Disse udgifter vil i sagens natur også ende hos kommunerne, som gennem KL ejer KOMBIT.

KOMBIT skal på den baggrund foreslå Forsvarsministeriet

- at drøfte med KL og KOMBIT, hvordan NIS2-lovforslaget vil kunne beriges, så det kan understøtte en sammenhængende, ensartet og effektiv cybersikkerhed i de danske kommuner,

- at præcisere i lovforslaget, så det også beskriver de afledte konsekvenser med dertilhørende realistiske estimat af udgifter, som NIS2-lovforsalget vil indebære for kommunerne, hvis den nuværende sektorspecifikke tilgang bibeholdes, og

- under alle omstændigheder medtager i NIS2-lovforslaget, at der skal ske en evaluering af, om den vedtagne lov virker hensigtsmæssigt til sikring af et højt niveau af cybersikkerheden i det danske samfund, herunder i kommunerne senest tre år fra lovens ikrafttræden.

Med venlig hilsen

Kristian Vengsgaard

Administrerende direktør
Dir. tlf. +45 50 77 71 24
Mail KRV@kombit.dk