Kommunstyrelsen

2024-05-20
TJÄNSTESKRIVELSE
Dnr: KFKS-2024-00425

Remiss – Nya regler om cybersäkerhet (2024:18)

Yttrande över delbetänkande till försvarsdepartementet avseende utredningen om genomförande av NIS2- och CER-direktiven

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår att kommunstyrelsen beslutar följande.

Kommunstyrelsen antar yttrande över delbetänkandet Nya regler om cybersäkerhet (2024:18) i enlighet med stadsledningskontorets förslag enligt bilaga 2 till tjänsteskrivelse daterad den 25 mars 2024.

Kommunstyrelsens arbetsutskotts beslut fattas med omedelbar justering.

Sammanfattning av ärendet

I delbetänkandet - Nya regler om cybersäkerhet - lämnas förslag på hur NIS2-direktivet ska införlivas i nationell lagstiftning. Delbetänkandet föreslår att NIS2-direktivet i huvudsak ska införlivas genom en ny lag, cybersäkerhetslagen. Genom direktivet skärps kraven för verksamhetsutövare i syfte att uppnå högre cybersäkerhet inom hela EU. Bland annat föreslås att en verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet, vidta riskhanteringsåtgärder, bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt krav på att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning. Verksamhetsutövare föreslås även ha en skyldighet att rapportera betydande incidenter till Myndigheten för samhällsskydd och beredskap (MSB) inom bestämda tidsgränser.

Ärendet

Ärendets beredning

Försvarsdepartementet har inte utsett Nacka kommun som remissinstans. Stadsledningskontoret bedömer dock att förslagen i delbetänkandet får påverkan på kommunen vilket medför att ett ärende har skrivits fram för yttrande över förslagen i delbetänkandet. Stadsledningskontoret har berett ärendet i samarbete med juridik- och kanslistaben, ledningsstaben och digitaliseringsenheten.

Försvarsdepartementet behöver få in synpunkter för delbetänkandet senaste den 28 maj.

Det ska noteras att ärendet hanteras på kommunstyrelsens arbetsutskott samma dag som synpunkterna ska lämnas in till försvarsdepartementet. Utifrån denna aspekt kommer ett ordförandebeslut förberedas så att kommunstyrelsens ordförande efter kommunstyrelsens arbetsutskotts sammanträde kommer kunna fatta ett brådskande ordförandebeslut avseende yttrandet.

Utredningens förslag i korthet

Direktivet

I remissen, benämnd som Delbetänkande - nya regler om cybersäkerhet, lämnas förslag på hur NIS2-direktivet ska införlivas i nationell lagstiftning. Den 14 december 2022 antog Europaparlamentet och rådet två nya EU-direktiv, NIS2-direktivet samt CER-direktivet. Delbetänkandet föreslår att NIS2-direktivet i huvudsak ska införlivas genom en ny lag, cybersäkerhetslagen. Genom direktivet skärps kraven för verksamhetsutövare och direktivet innefattar bestämmelser rörande mer omfattande samverkan inom unionen, detta i syfte att uppnå högre cybersäkerhet. Genom tilläggsdirektiv den 11 januari 2024 förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av CER-direktivet (dir. 2024:3).

Verksamheter som berörs

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer (antalet sektorer ökar från 7 till 18). Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster. Offentlig förvaltning pekas i utredningen ut som en egen sektor. Det får till följd att nästan hela den offentliga sektorn omfattas av lagens krav. Utredningen föreslår att cybersäkerhetsagen ska gälla för de flesta statliga myndigheter i Sverige. Samtliga regioner och kommuner omfattas av lagens krav. Undantag gäller enbart för region- eller kommunfullmäktige. Dessutom ska verksamhetsutövare vidta riskhanteringsåtgärder, i syfte att skydda nätverks- och informationssystem samt systemens fysiska miljö mot incidenter. Det ställs krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Utöver detta, finns det en skyldighet för verksamhetsutövare att rapportera betydande incidenter till Myndigheten för samhällsskydd och beredskap (MSB), vilket ska ske inom bestämda tidsgränser.

De nya kraven i direktivet

- En verksamhetsutövare som omfattas av lagen ska *anmäla sig till sin tillsynsmyndighet* och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet.
- Verksamhetsutövare ska *vidta riskhanteringsåtgärder* för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas.

- Det ställs krav på att verksamhetsutövaren ska *bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete* samt krav på att *verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning*.
- Verksamhetsutövare har en skyldighet att *rapportera betydande incidenter till Myndigheten för samhällsskydd och beredskap (MSB) inom bestämda tidsgränser*. Det innebär i korthet att en varning ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om en betydande incident. En incidentanmälan ska göras inom 72 timmar och en slutrapport inom en månad.

Tillsyn

Utredningen föreslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Den kompetens som finns hos befintliga tillsynsmyndigheter bör så långt möjligt även nyttjas för de nya sektorer som omfattas av reglering. Flera tillsynsmyndigheter föreslås därför få utökade ansvarsområden. Utredningen föreslår också fem nya tillsynsmyndigheter (länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län samt Läkemedelsverket).

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

För att säkerställa gränsöverskridande samarbete ska varje medlemsstat utse en gemensam kontaktpunkt. MSB föreslås vara gemensam kontaktpunkt i Sverige. Den gemensamma kontaktpunkten ska bland annat utöva en sambandsfunktion och lämna rapporter om betydande incidenter, cyberhot och tillbud till Enisa (Europeiska unionens cybersäkerhetsbyrå).

Varje medlemsstat ska också utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheten ska bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information. Myndigheten för samhällsskydd och beredskap (förkortad MSB) föreslås vara CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige. Varje medlemsstat ska även anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

Ingripanden och sanktioner
Sanktionsavgifterna ska för offentlig förvaltning bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Tillsynsmyndighetens möjligheter att besluta om förelägganden (vid vite) och sanktionsavgifter föreslås behållas. Tillsynsmyndigheten ska även kunna förelägga en verksamhetsutövare att offentliggöra information om överträdelser av lagens bestämmelser, och att informera användare som kan påverkas av ett betydande cyberhot. Vidare föreslås tillsynsmyndigheten få ansöka hos allmän förvaltningsdomstol om att en person med ledningsansvar hos en väsentlig verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där. Anmärkning införs som sanktion och ska alltid beslutas vid överträdelser om ingen annan sanktion har använts av tillsynsmyndigheten.

Tillsynsmyndigheten ska ingripa mot alla överträdelser och beakta fler omständigheter vid val och utformning av sanktioner
Utredningen föreslår att tillsynsmyndigheten ska ingripa mot alla överträdelser av lagen. Om tillsynsmyndigheten inte avstår från att ingripa ska den åtminstone meddela en anmärkning. När tillsynsmyndigheten ingriper ska den alltid beakta alla relevanta omständigheter, men fler omständigheter görs obligatoriska att beakta än vad som tidigare gällt.

Ekonomiska konsekvenser
Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB och verksamhetsutövarna.

För tillsynsmyndigheterna handlar det om att betydligt fler verksamhetsutövare kommer att omfattas av lagen. Utredningen föreslår att de tillsynsmyndigheter som redan bedriver tillsyn med undantag av Finansinspektionen får ett förstärkt anslag med två miljoner kronor vardera för 2025 avseende löpande kostnader. Skälet är att tillsynsmyndigheterna bör ha utökade resurser för att kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn. Även MSB bör tillföras motsvarande belopp. De myndigheter som inte redan har tillsynsuppdrag bör få ett förstärkt anslag med fem miljoner kronor vardera för 2025 för att bygga upp tillsynsverksamheten. Samtidigt föreslår utredningen att regeringen ger Statskontoret i uppdrag att vidare utreda de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB samt att det för de första åren införs ett återrapporteringskrav för myndigheterna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter

medföra besparingar. Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som huvudregel omfattas inte små företag.

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

Stadsledningskontorets bedömning samt förslag till yttrande

Inledningsvis kan konstateras att denna bedömning tar utgångspunkt från de förslag i betänkandet som bedöms ha mest påverkan på kommunen.

Digitaliseringen innebär att en allt större andel av samhällets aktiviteter i olika grad är beroende av nätverk och informationssystem. Den digitala utvecklingen medför stora möjligheter som bland annat bättre tjänster och ökad effektivitet, men också risker. Därför är informations- och cybersäkerhet i dag en fråga som angår hela samhället. Särskilt höga säkerhetskrav ska ställas när det gäller samhällsviktig verksamhet som, för att upprätthålla nödvändiga samhällsfunktioner, måste fungera under alla förhållanden. Stadsledningskontoret välkomnar därför en mer enhetlig reglering för hela den offentliga förvaltningen vad gäller de mest grundläggande hygienfaktorerna inom informationssäkerhetsarbetet. I vissa fall bedöms dock utredningens förslag tyvärr komma att innebära dubbelarbete och ett ineffektivt nyttjande av såväl kommunernas som statens resurser. Kommunernas perspektiv har inte beaktats tillräckligt och vissa förslag kommer att aktivt försvåra för dem att tillvarata sina rättigheter och uppfylla sina förpliktelser.

Av betänkandet framgår det även fortsättningsvis ska vara olika tillsynsmyndigheter för de olika sektorerna som omfattas av NIS2. Stadsledningskontoret bedömer att det i utredningen inte tas höjd för kommunernas spridda och omfattande verksamhetsområde. Detta medför att kommunen som helhet kommer få flera olika tillsynsmyndigheter som formar föreskrifter och bedriver tillsyn inom samma område för att säkerställa att regelverket följs. Även om syftet med de olika tillsynsmyndigheterna är att dessa, med sina särskilda uppdrag och kompetenser, ska säkerställa att de unika riskerna inom respektive sektor finns risk att detta inte blir resurseffektivt för vare sig tillsynsmyndigheterna eller kommunerna. Stadsledningskontoret efterlyser därför en mer samordnad hantering av föreskrifter och tillsyn som träffar just kommuner, i de delar som gäller grundläggande processer i lagkraven. Som utredningen framhåller ska förslagen utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Ur det kommunala perspektivet vore det att föredra att en samordnande myndighet får föreskriva om de grundläggande och gemensamma cybersäkerhetsprocesser som gäller lika för alla. Det bör stärka intentionen att undanröja en ojämn och fragmenterad implementering av cybersäkerhet nationellt och bespara ett flertal föreskrivande myndigheter och tillsynsmyndigheter resurser att inte behöva

uttrycka samma krav i sina respektive föreskrifter. Stadsledningskontoret anser därför att föreskriftsrätten hos de olika sektorsmyndigheterna bör fokuseras på att uttrycka just de unika särdragen som finns inom varje sektor i kompletterande föreskrifter. Detta ligger även i linje med vad som Myndigheten för samhällsskydd och beredskap (MSB) framfört i sitt remissvar över delbetänkandet (MSB 2024-03843-4).

I utredningen anges att kostnaderna för offentliga verksamhetsutövare (däribland kommuner) ska finansieras inom befintlig budgetram. Sammantaget bedömer utredningen att förslagen medför kostnader för offentliga verksamhetsutövare, men övergripande för hela offentliga sektorn även besparingar. Enhetliga regler, tillsyn och möjligheten att få upplysningar av tillsynsmyndighet kommer enligt utredningen att bidra till minskade kostnader för verksamhetsutövaren. Stadsledningskontoret håller med om att det med hjälp av incidenthantering kan identifieras brister som sedan kan åtgärdas och förebyggas. Detta är positivt och antas leda till en ökad motståndskraft och robusthet för de samhällsviktiga tjänsterna. Det är däremot inte likställt med att besparingar kommer att erhållas. För att skapa förutsättningar för hanteringen behöver verksamheterna säkerställa en ändamålsenligt, effektiv och verksamhetsövergripande incidenthanteringsprocess och många verksamheter behöver även investera i systemstöd. Det innebär således att de ökade kraven leder till både mer arbete, behov av ökade personella resurser och fler investeringar, särskilt för offentliga verksamhetsutövare som idag bara i enstaka fall omfattas av gällande NIS-lag (däribland kommuner). Det ska särskilt noteras att den utökade rapporteringsskyldigheteter särskilt beräknas bli kostnadsdrivande. Därtill kommer även behov av ökade resurser vid upphandlingar av nätverks- och informationssystem för att säkerställa korrekt kravställning i enlighet med den föreslagna cybersäkerhetslagen. Stadsledningskontoret saknar en genomarbetad konsekvensanalys vad gäller detta. Utifrån att utredningen inte redogör för detta är det därför svårt att säkerställa att finansieringsprincipen upprätthålls.

Stadsledningskontoret bedömer att det är viktigt att klargöra om kommunala bolag omfattas av sektorn offentlig förvaltning eller inte. Det behövs inte minst eftersom kommuner kategoriseras som väsentliga verksamhetsutövare och därmed träffas av högre krav. I delbetänkandets förslag framgår det att kommuner omfattas i sin helhet. Det förtydligas även att det inte enbart är den sektorsspecifika tjänsten som omfattas, utan hela den verksamhet där tjänsten ingår. Innebörden är att den som bedriver verksamhet inom någon av sektorerna, som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det bedöms vara i linje med direktivets och lagens intentioner om att uppnå en högre gemensam cybersäkerhet för samhällsviktig verksamhet inom hela unionen. Utredningen konstaterar dock att i de fall verksamheten bedrivs genom kommunala bolag är det inte kommunen som är verksamhetsutövare. Det innebär att de kommunala bolagen inte ingår i det som avses med ”hela kommunen” eller i den nya

sektorn ”offentlig förvaltning”. Stadsledningskontoret instämmer i detta. De kommunala bolagen omfattas bara av kraven om de träffas av någon av de specifikt utpekade sektorerna.

Ekonomiska konsekvenser

Förslaget till beslut om yttrande medför inga ekonomiska konsekvenser. Av stadsledningskontorets bedömning och förslag på yttrande framgår att det aktuella delbetänkandet saknar en tillräcklig konsekvensanalys för kommunernas del. Det medför att det utifrån delbetänkandet finns svårigheter att beräkna de ekonomiska konsekvenserna för kommunens del. Det kan dock konstateras att den nya lagstiftningen kommer generera kostnader i kommunen utifrån ökade resurskostnader vid nya upphandlingar, utbildningsinsatser, bemanning för säkerställa rapportering av incidenter etcetera. Konsekvensen om kommunen inte lever upp till de nya kraven i den nya lagstiftningen är sanktionsbelopp på upp till 10 000 000 kronor.

Konsekvenser för barn

Förslaget till beslut medför inga konsekvenser för barn. Det kan däremot konstateras att den föreslagna lagstiftningen sker i syfte att höja informations- och cybersäkerheten vilket medför positiva konsekvenser för bland annat barn och unga. Då uppgifter om barn och unga anses vara särskilt skyddsvärda enligt dataskyddsförordningen är det av stor vikt att dessa särskilt hanteras på ett säkert sätt.

Handlingar i ärendet

Tjänsteskrivelse daterad den 20 maj 2024
Bilaga 1 Utdrag ur 2024:18 - Sammanfattning och författningsförslag
Bilaga 2 Stadsledningskontorets förslag till yttrande

Sara Lauri	Anneli Sagnérius
Kanslidirektör	Kommunjurist
Stadsledningskontoret	Juridik- och kanslistaben