Malmö stad
Kommunstyrelsen

Datum
2024-05-20
Adress
August Palms Plats 1
Diarienummer
STK-2024-527

Yttrande

Till
Försvarsdepartementet

Remiss Försvarsdepartementet - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
Fö2024/00496

Sammanfattning
Ny reglering för att öka informations- och cybersäkerhetsnivån i Sverige och EU ser Malmö stad som något positivt. Malmö stad konstaterar att utredningen under kort tid hanterat en omfattande och utmanande uppgift.

Sammanfattningsvis har Malmö stad följande synpunkter:

- Namnge den nya lagen och förordningen på ett sätt som främjar kontinuitet och en helhet (avsnitt 5.1)
- Nämnden i stället för kommunen borde utgöra en enhet och därmed juridisk person. Ett förtydligande behövs huruvida kommuner omfattas av sektorn offentlig förvaltning. Ett förtydligande behövs gällande om kommunalförbund omfattas av regleringen och i sådant fall på vilken grund (avsnitt 5.2.10)
- Underlätta anmälnings- och uppgiftsskyldigheten (avsnitt 6.2)
- Undvik alltför övergripande lagtext samt tydliggör kraven (avsnitt 7.1)
- Använd begreppet "säkerhetsåtgärder" istället för "riskhanteringsåtgärder" (avsnitt 7.1.1)
- Utred möjligheten till en central tillsynsmyndighet (avsnitt 8.4.1)
- Ge Myndigheten för samhällsskydd och beredskap rätt att meddela grundföreskrifter (avsnitt 8.4.5)
- Säkerhetsskanning bör definieras i 2 § - Uttryck i lagen (avsnitt 8.4.6)
- Tillsyn och informationsutbyte behöver samordnas i högre utsträckning samt tidsfrist bör införas (avsnitt 8.4.7)

- Ge kommuner ekonomiskt stöd för genomförandet av den nya lagen och kommande föreskrifter (avsnitt 12.7)

Yttrande

Nya undersökningar som bör beaktas

Myndigheten för samhällsskydd och beredskaps (MSB) rapport "Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen: Resultatredovisning av Infosäkkollen och It-säkkollen 2023" publicerades i mars 2024. Resultatet visar att det kan krävas ett omfattande arbete och ökad resurssättning för att Sveriges kommuner ska kunna omhänderta de kommande regulatoriska kraven. Nuvarande föreskrifter från MSB avseende informationssäkerhet motsvarar nivå 3 i uppföljningsstrukturen. 76,5 procent av de deltagande kommunerna uppnådde enligt rapporten inte grunderna i systematiskt informations- och cybersäkerhetsarbete, vilket motsvarar nivå 0.

Namnge den nya lagen och förordningen på ett sätt som främjar kontinuitet och en helhet (avsnitt 5.1)

Malmö stad motsätter sig delvis förslaget om att en ny lag och ny förordning ska ha benämningarna cybersäkerhetslagen respektive cybersäkerhetsförordningen.

Skälet till detta är att utredningens förslag till benämning antyder att lagen endast inbegriper skydd av informations- och nätverkssystem mot cyberhot. I grunden är det information som ska skyddas och lagförslaget ställer även krav på ett systematiskt informationssäkerhetsarbete. Cybersäkerhet är ett relativt nytt och okänt begrepp, medan informationssäkerhet är mer väletablerat hos de verksamhetsutövare som omfattas av lagen. Det finns skillnader mellan begreppen cybersäkerhet och informationssäkerhet. Informationssäkerhet beskrivs dock ofta som en förutsättning för cybersäkerhet och de två begreppen används vanligtvis tillsammans. Ett exempel på sådan kontext ges i standard "SS-EN ISO/IEC 27001:2023 - Informationssäkerhet, Cybersäkerhet och Integritetsskydd". Att tydligare sammanlänka informationssäkerhet och cybersäkerhet främjar kontinuitet och sätter det nya begreppet cybersäkerhet i en större och väletablerad kontext.

Malmö stad föreslår att benämningarna på ny lag och ny förordning ska vara ”Lag (2024/5:XX) om informations- och cybersäkerhet” samt ”Förordning (2024/5:XX) om informations- och cybersäkerhet”. Som en följd av detta bör syftet med lagen (avsnitt 5.1.2) i stället vara "att uppnå en hög informations- och cybersäkerhetsnivå".

Kommuner (avsnitt 5.2.10)

Malmö stad anser att en nämnd inom kommunen, som inte är en egen juridisk person, borde anses utgöra en särskild enhet. Utredningen drar slutsatsen att det är kommunen som juridisk person som är vårdgivare och därmed verksamhetsutövare och att hela kommunen omfattas på den grunden. Malmö stad vill dock påpeka att det är i nämnderna som verksamhet bedrivs alternativt i de kommunala bolagen, vilket även SKR har framfört. Bestämmelsen i 6 kap. 15 § kommunallagen om styrelsens allmänna processbehörighet leder inte med nödvändighet till slutsatsen att det är kommunen som juridisk person som ska omfattas av föreslagen reglering. Utifrån detta resonemang instämmer Malmö stad i SKR:s invändning att det inte är nödvändigt att det är kommunen som juridisk person som är verksamhetsutövare enligt föreslagen reglering.

Malmö stad önskar även ett förtydligande rörande kommuner och sektor offentlig förvaltning. Av utredningens förslag framgår det inte uttryckligen huruvida kommuner omfattas av sektorn offentlig förvaltning. Av utredningen framgår inte i vilka fall en kommun kan bli föremål för tillsyn utifrån sektorn offentlig förvaltning.

Malmö stad önskar vidare ett förtydligande av huruvida kommunalförbunden omfattas av regleringen och på vilken grund i sådant fall. I utredningen nämns inget om kommunförbunden och huruvida de omfattas av regleringen.

Underlätta anmälnings- och uppgiftsskyldigheten (avsnitt 6.2)

Malmö stad motsätter sig utredningens förslag om att verksamhetsutövare ska göra en anmälan och lämna uppgifter till respektive tillsynsmyndighet.

Skälen för detta är att kommuner i sin linjeorganisation kan tillhöra flera sektorer och därmed flertalet tillsynsmyndigheter. Utredningens förslag innebär onödigt merarbete och resurskrävande administration för både kommunerna och tillsynsmyndigheterna eftersom det kräver att kommunen överför uppgifter på ett säkert sätt till flera olika tillsynsmyndigheter, i värsta fall genom olika IT-system som tillsynsmyndigheterna tillhandahåller. Utredningen har vad gäller incidentrapportering gjort bedömningen att underrättelsen av incidenter av effektivitetsskäl sker direkt till CSIRT-enheten (MSB). Malmö stad anser att samma resonemang bör gälla för anmälnings- och uppgiftsskyldigheten.

Malmö stad anser att ett mer resurseffektivt förslag är att verksamhetsutövare ska genomföra en enskild anmälan som inbegriper alla sektorer som verksamhetsutövaren bedriver verksamhet inom. Anmälan bör göras direkt till den gemensamma kontaktpunkten (MSB) som sedan förmedlar uppgifter vidare till

tillsynsmyndigheterna. MSB håller redan på att utveckla en systemplattform för säker informationsdelning och incidentrapportering som kan användas för detta ändamål.

Undvik för övergripande lagtext och tydliggör kraven (avsnitt 7.1)

Malmö stad invänder mot att utredningens förslag att lagen bör utformas övergripande och fyllas ut av föreskrifter som meddelas av tillsynsmyndigheten.

Skälen för detta är att det inte är ändamålsenligt att överlämna detaljbeskrivningen av krav på riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning till respektive tillsynsmyndighet i föreskriftsarbetet. Syftet med ny lagstiftning bör vara att tydliggöra och samordna regelverket med målsättningen att höja och kravställa kring en lägstanivå avseende informations- och cybersäkerhet. Genom att vara oprecis i lagen finns en risk att lagstiftaren i praktiken sänker direktivets krav. Förslaget innebär även att en kommun kan träffas av flera föreskrifter som reglerar samma sak, men som kan skilja sig åt eftersom det är i föreskrifterna som kraven ska tydliggöras. Eftersom kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster kan det då innebära att kommunen behöver genomföra flertalet motstridiga föreskrifter i hela verksamheten.

Utredningens förslag är därmed inte resurseffektiv och dessutom mycket svårt att implementera i praktiken för verksamhetsutövare som tillhör flera sektorer. Övergripande reglering om riskhanteringsåtgärder i lagtexten i kombination med föreskrifter för varje sektor, där MSB:s vägledning och yttranden inte är juridiskt bindande, ökar risken för motstridiga föreskrifter som kommer vara svåra eller omöjliga för kommuner att omhänderta. Malmö stad efterfrågar en tydlighet i lagen och menar vidare att detta främjar en hög lägsta nivå för informations- och cybersäkerhet i Sverige och minskar risken för motstridiga föreskrifter.

Malmö stad föreslår att övergripande krav på säkerhets- och riskhanteringsåtgärder enligt artikel 21.2 tydliggörs i lag och förordning. Det är att föredra att kraven från direktivet framgår för att säkerställa en enhetlig tolkning och efterlevnad av kraven, exempelvis vad gäller multifaktorsautentisering och kontinuerlig autentisering.

Använd begreppet "säkerhetsåtgärder" istället för "riskhanteringsåtgärder" (avsnitt 7.1.1)

Malmö stad invänder mot utredningens uppfattning om att det inte är möjligt att anpassa begreppen i cybersäkerhetslagen till begreppen i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Skälen till detta är att det inte är helt okomplicerat att frångå vedertagna begrepp som används i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Användningen av etablerade begrepp utesluter inte en utvidgning eller ett förtydligande av exempelvis befintliga krav på åtgärder. En omskrivning av det välkända begreppet "säkerhetsåtgärder" till "riskhanteringsåtgärder" i ny lagstiftning skulle exempelvis kunna innebära att verksamhetsutövare tolkar det senare begreppet som ensam ersättare för säkerhetsåtgärder, även inom området informationssäkerhet. ”Säkerhetsåtgärder” är ett väletablerat begrepp med koppling till standardserien SS-EN ISO/IEC 27001:2023 - Informationssäkerhet, Cybersäkerhet och Integritetsskydd, som många verksamhetsutövare inom offentlig förvaltning följer. Riskhanteringsåtgärderna i NIS 2-direktivet är välbekanta åtgärder från etablerade standarder, men där benämns de som "säkerhetsåtgärder". Malmö stad anser att ett språkbruk som harmoniserar med etablerade standarder är ett sätt att uppmuntra till användningen av dessa, vilket medlemsstaterna enligt NIS 2-direktivet ska göra.

Malmö stad föreslår att lagstiftaren använder begreppet "säkerhetsåtgärder" istället för "riskhanteringsåtgärder.”

Utred möjligheten till en central tillsynsmyndighet (avsnitt 8.4.1)

Malmö stad föreslår att möjligheten till en central tillsynsmyndighet utreds.

Skälen till detta är att det hade underlättat för verksamhetsutövare som ingår i flera sektorer att ha en central tillsynsmyndighet. Som utredningen påpekar krävs det expertkunskap för att utöva tillsyn avseende cybersäkerhet. Ur ett kompetensförsörjningsperspektiv är detta även ett argument för att förorda en central tillsynsmyndighet så att konkurrensen om kompetens inte blir lika stor.

Ge Myndigheten för samhällsskydd och beredskap rätt att meddela grundföreskrifter (avsnitt 8.4.5)

Malmö stad motsätter sig att tillsynsmyndigheten inom sitt tillsynsområde får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning.

Skälen till detta är att förslaget innebär att en kommun kan behöva omhänderta föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning från flera olika tillsynsmyndigheter. Malmö stad anser att om IVO skulle överta föreskriftsrätten från Socialstyrelsen skulle detta bidra till ytterligare risk för motstridiga föreskrifter. Detta eftersom Socialstyrelsen meddelar föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården och verksamhet som bedrivs

med stöd av SoL, LVU, LVM och LSS. I utredningen föreslås att kraven ska gälla för hela verksamheten och inte bara för samhällsviktiga och digitala tjänster. Malmö stad anser att det är svårhanterligt för en kommun att hantera denna flora av föreskrifter och kunna tillämpa dessa i praktiken. Det borde vara mer resurseffektivt för både verksamhetsutövarna och tillsynsmyndigheterna att det tas fram gemensamma grundföreskrifter som kan kompletteras av de tillsynsmyndigheter som ser behov av detta utifrån sitt ansvarsområde.

Malmö stad föreslår att Myndigheten för samhällsskydd och beredskap får meddela gemensamma grundföreskrifter för alla verksamhetsutövare rörande systematiskt och riskbaserat informations- och cybersäkerhetsarbete, grundläggande krav på säkerhetsåtgärder (riskhanteringsåtgärder) och utbildning. Tillsynsmyndigheterna ska kunna komplettera dessa vid behov. Om detta inte är möjligt hade en framkomlig väg kunnat vara att kommuner tillåts omhänderta de sektorsspecifika föreskrifterna i de nämnder som bedriver verksamhet inom respektive sektor och föreskrifter för offentlig förvaltning i den övriga verksamheten.

Säkerhetsskanning bör definieras i 2 § - Uttryck i lagen (avsnitt 8.4.6)

Utredningen är tydlig med att NIS 2-direktivet inte innehåller en definition eller entydig beskrivning av vad en säkerhetsskanning faktiskt är. Däremot ger utredningen en bred typbeskrivning av begreppet och ett konkret exempel på vad begreppet inte är (penetrationstester).

Malmö stad föreslår att begreppet säkerhetsskanning, i ny författning, förtydligas i syfte att skapa samsyn kring begreppets innebörd.

Tillsyn och informationsutbyte behöver samordnas i högre utsträckning samt tidsfrist bör införas (avsnitt 8.4.7)

Malmö stad invänder mot att ett samarbetsforum under ledning av MSB är tillräckligt för att samordna arbetet med tillsyn. Malmö stad önskar även att det klargörs hur länsstyrelserna och övriga tillsynsmyndigheter i praktiken ska samordna tillsynen av offentliga verksamhetsutövare som ingår i flera sektorer.

Skälet till detta är att en kommun kan komma att granskas av flera olika myndigheter i sin linjeorganisation. Malmö stad ser en poäng av att ha en struktur för att försöka undvika att granskning sker på en annan tillsynsmyndighets område. Utredningen tydliggör inte hur förslaget kan genomföras i praktiken. Därmed kan det innebära att granskningar följer så nära inpå varandra att kommunen inte hinner vidta åtgärder innan nästa granskning inleds.

Utan utökad samordning finns det en risk att kommunerna behöver lägga mycket resurser på att hantera granskningar snarare än att vidta säkerhetsåtgärder (riskhanteringsåtgärder). Malmö stad menar att detta blir särskilt viktigt i relation till utredningens förslag om att skärpa tillsynsmyndigheternas återrapporteringskrav. Det bör också nämnas att det ofta inom en kommun är samma resurser som arbetar vid en tillsyn som också arbetar med ständiga förbättringar utifrån valda säkerhetsåtgärder. Om en stor del av arbetet läggs på tillsyn så kommer därmed utvecklingsarbetet gå långsammare.

Malmö stad föreslår att MSB ges ett tydligare mandat att samordna metodik, planering och uppföljning av tillsyn, eller att länsstyrelserna får ett utökat samordningsmandat för verksamhetsutövare inom offentlig förvaltning som ingår i flera sektorer. Malmö stad anser även att det är lämpligt att införa en tidsfrist efter genomförd granskning så att en tillsynsmyndighet med ansvar för en annan sektor inte kan granska en verksamhetsutövare för nära inpå en annan tillsynsmyndighets granskning.

Ge kommuner ekonomiskt stöd för genomförandet av den nya lagen och kommande föreskrifter (avsnitt 12.7)

Malmö stad motsätter sig förslaget om att de ekonomiska konsekvenserna ska finansieras inom offentliga verksamhetsutövares befintliga budgetram.

Skälen till detta är att utredningen menar att kraven inte är omfattande, samtidigt som resultatet från Cybersäkerhetskollen 2023 visar att det kan krävas ett omfattande arbete och ökad resurssättning för att Sveriges kommuner ska kunna efterleva lagkraven. Nuvarande föreskriftskrav från MSB avseende informationssäkerhet motsvarar nivå 3 i uppföljningsstrukturen. 76,5 procent av de deltagande kommunerna uppnår inte grunderna i systematiskt informations- och cybersäkerhetsarbete, vilket motsvarar nivå 0. Regeringen bör beakta detta och överväga ekonomiskt stöd till kommunerna för att underlätta genomförandet av den nya lagen och kommande föreskrifter.

För att komma till punkten att kommunerna har infört proportionella säkerhetsåtgärder som löpande följs upp och utvärderas krävs ett omfattande arbete och utökade resurser, inte minst för kompetensförsörjning. Kompetens avseende informations- och cybersäkerhet är en bristkompetens i hela EU, vilket medför att de mindre kommunerna i synnerhet kan komma att behöva förlita sig i hög utsträckning på konsulttjänster. Detta kommer i sig vara mycket kostnadsdrivande, samtidigt som de mindre kommunerna kan sakna en mottagarorganisation som systematiskt kan omhänderta och vidareutveckla det som levereras.

Malmö stad efterfrågar en grundnivå för ekonomisk ersättning och därefter en uppräkning beroende på antalet invånare i kommunen. Detta ger en tydlig signal om att införandet av säkerhetsåtgärder i offentlig förvaltning är prioriterat för staten.

Ordförande [Förnamn Efternamn]

[Fyll i titel] [Förnamn Efternamn]

[Här anger du om det finns reservationer/särskilda yttranden.]