Malmö stad
Stadskontoret

Tjänsteskrivelse

Datum
2024-05-21
Vår referens
Kajsa Thelin
Utvecklingssamordnare
kajsa.thelin@malmo.se

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

STK-2024-527

Sammanfattning

Malmö stad har beretts tillfälle att yttra sig över delbetänkandet ”Nya regler om cybersäkerhet (SOU 2024:18)”. Delbetänkandet redovisar förslag om införlivning av NIS 2-direktivet i svensk rätt. Direktivet ställer krav på säkerhet i nätverks- och informationssystem för en högre cybersäkerhet i EU. NIS-lagen och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster föreslås upphävas och i stället ersättas av cybersäkerhetslagen och cybersäkerhetsförordningen. Antalet sektorer föreslås utökas från sju till arton. Kraven kommer gälla för hela verksamheten och inte enbart för samhällsviktiga och digitala tjänster.

Stadskontoret instämmer generellt i de synpunkter som lämnats av servicenämnden, förvaltningar, bolag och förbund. Eftersom många kommuner ingår i flera sektorer ser stadskontoret utmaningar, särskilt vad gäller föreskrifter och tillsyn, som föreslås hanteras sektorsvis. Stadskontoret efterfrågar därför flera förtydliganden och förslag på andra åtgärder för att de nya reglerna ska kunna genomföras effektivt i kommuner.

Några exempel som lyfts fram är att stadskontoret särskilt efterfrågar ett förtydligande kring om kommuner ingår i sektor offentlig förvaltning samt om kommunalförbund omfattas av regleringen. Vidare anser stadskontoret att det krävs ytterligare åtgärder för att minska risken för motstridiga föreskrifter och resurskrävande administration och granskningar. Stadskontoret tar även upp att det bör införas en grundnivå för ekonomiskt stöd till kommunerna för genomförandet av riskhanteringsåtgärder och därefter en uppräkning beroende på antalet invånare i kommunen.

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

SIGNERAD
2024-05-21

1. Kommunstyrelsen godkänner förslag till yttrande och skicka yttrandet till Försvarsdepartementet.

Beslutsunderlag

- Remiss Försvarsdepartementet - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
- Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
- G-Tjänsteskrivelse KSAU 240527 Remiss Försvarsdepartementet - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
- Förslag till yttrande KSAU 240527 Remiss Försvarsdepartementet - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
- Remissvar servicenämnden
- Servicenämnden beslut 240423 § 43

Beslutsplanering

Kommunstyrelsens arbetsutskott 2024-05-27
Kommunstyrelsen 2024-06-05

Beslutet skickas till

Försvarsdepartementet
Servicenämnden
Stadskontorets handläggare

Ärendet

Malmö stad har beretts tillfälle att yttra sig över utredningen ”Nya regler om cybersäkerhet (SOU 2024:18)”. Yttrande ska ha inkommit till Försvarsdepartementet senast den 28 maj 2024. Anstånd med att inkomma med yttrandet har beviljats till och med den 6 juni 2024. Utredningen innehåller förslag till genomförande av Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2) och har skickats på internremiss till servicenämnden. Övriga förvaltningar, kommunala bolag och förbund i Malmö stad har beretts tillfälle att framföra sina synpunkter underhand genom en intern remisskonferens.

NIS 2-direktivet ska i huvudsak genomföras genom att NIS-lagen och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster upphävs. De ersätts av ny lag och ny förordning med benämningarna cybersäkerhetslagen respektive cybersäkerhetsförordningen.

Gällande lagstiftning och förslaget till cybersäkerhetsreglering skiljer sig åt på framför allt två sätt. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer,

eftersom antalet sektorer utökas från sju till arton. Den andra skillnaden är att kraven kommer att gälla för hela verksamheten – inte bara för samhällsviktiga och digitala tjänster.

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig för rätt personer, i rätt tid. Det handlar också om att förhindra att information läcker ut, förvanskas och förstörs. Cybersäkerhet är en form av informationssäkerhet som tar sikte på att hantera risker i alltmer komplexa digitala ekosystem. Det kan till exempel handla om att hantera IT-attacker eller beroenden till leverantörer som levererar digitala tjänster.

Utredningarnas förslag och bedömningar i korthet

Klassificering och registrering

Av artikel 3 i direktivet följer att samtliga verksamhetsutövare som omfattas ska klassificeras som väsentliga eller viktiga. Viktiga verksamhetsutövare kan endast bli föremål för reaktiv tillsyn och har lägre maxtak för sanktionsavgifter. Utredningen föreslår att kommuner klassificeras som väsentlig verksamhetsutövare, vilka kan bli föremål för ordinarie tillsyn.

Utredningen föreslår ett delat tillsynsansvar vilket innebär att varje tillsynsmyndighet inom sitt ansvarsområde ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Varje verksamhetsutövare ska själv identifiera om verksamheten omfattas av lagen och göra anmälan till relevant tillsynsmyndighet. Uppgifter bör lämnas in senast den 17 januari 2025. Tillsynsmyndighetens register ska överföras till den centrala kontaktpunkten, Myndigheten för samhällsskydd och beredskap (MSB), minst vartannat år.

Övergripande lagreglering om riskhanteringsåtgärder

Utredningen föreslår att riskhanteringsåtgärder ska regleras övergripande i lagen och att kraven inte bör anges alltför detaljerat. Lagen ska fyllas ut av sektorsspecifika föreskrifter från varje tillsynsmyndighet. Utredningen menar att det är angeläget att föreskrifterna kan anpassas sektorvist och att den myndighet som har tillsyn också har föreskriftsrätten. MSB får yttra sig och ska ta fram en vägledning om riskhanteringsåtgärder. Vägledningen är inte juridiskt bindande.

Begrepp

Utredningen menar att det inte är möjligt att anpassa begrepp som exempelvis ”riskhanteringsåtgärder” i lagen till nuvarande Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där ”säkerhetsåtgärder” används och att det finns skäl för att använda direktivets begrepp. Den menar vidare att

det är förvirrande att använda samma begrepp som i nuvarande NIS-reglering eftersom kraven är nya.

Riskhanteringsåtgärder

Artikel 21.1 och 21.2 i direktivet anger att medlemsstaterna ska säkerställa att väsentliga och viktiga verksamhetsutövare vidtar lämpliga och proportionella åtgärder för att hantera risker som hotar säkerheten i nätverk- och informationssystem och systemens fysiska miljö. I utredningens förslag har vissa riskhanteringsåtgärder och formuleringar tagits bort till förmån för mer allmänna beskrivningar. Av direktivet framgår att verksamhetsutövaren i tillämpliga fall ska beakta relevanta europeiska och internationella standarder. Utredningen menar att det inte är möjligt att i lag föreskriva att standarder ska beaktas utan detta får uppmuntras på andra och frivilliga sätt.

Systematiskt informationssäkerhetsarbete

Från MSB har anförts att det är viktigt att föreskriva att informationssäkerhetsarbetet ska ske systematiskt och riskbaserat på samma sätt som följer av Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Krav på detta återfinns i lagförslaget men framgår inte uttryckligen i direktivet.

Ansvar och utbildning

Ledningsorgan i enskilda verksamheter ska ha ett personligt ansvar för överträdelser av kraven om riskhanteringsåtgärder. Innebörden av detta ansvar är att det ska vara möjligt att vidta åtgärder eller rikta sanktioner mot denna personkrets. Det ska vara möjligt att meddela ett förbud för en person att utöva en ledningsfunktion. Utredningen föreslår att förbudet inte ska få användas mot offentliga verksamhetsutövare.

Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder. I kommuner innebär det kommunstyrelsen. Anställda ska också erbjudas sådan utbildning.

Incidentrapportering

Betydande incidenter ska underrättas CSIRT-enheten (Computer Security Incident Response Team) hos MSB. En tidig varning ska lämnas inom 24 timmar, en incidentanmälan och information till drabbade kunder ska lämnas inom 72 timmar och en slutrapport inom 1 månad. Om incidenten fortfarande pågår ska en lägesrapport lämnas inom 1 månad.

Tillsynsmyndigheter

Det ska finnas en eller flera tillsynsmyndigheter för varje sektor. Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. För den nytillkomna sektorn offentlig förvaltning ska Länsstyrelserna i Stockholms, Skånes, Västra Götalands och Norrbottens län ansvara

för tillsynen. Det anses vara mest resurseffektivt eftersom det är de fyra länsstyrelser som idag bedriver tillsyn enligt säkerhetsskyddslagstiftningen. Utredningen anser att MSB:s roll även i fortsättningen bör vara stödjande och samordnande utifrån argumentet att det är svårt att kombinera denna roll med ett tillsynsuppdrag.

System för tillsyn

Utredningen bedömer att nuvarande system för tillsyn är ändamålsenligt men att det kan finnas skäl för regeringen att följa upp arbetet med föreskrifter och tillsyn. Vad gäller möjligheten till en central tillsynsmyndighet föreslås detta utredas i särskild ordning. Utredningen menar att nuvarande tillsynsmyndigheter har byggt upp kunskap och erfarenhet i arbetet med den nuvarande NIS-regleringen. Utredningen anser därför att det är en effektiv lösning att så långt möjligt nyttja den kompetens som finns hos befintliga tillsynsmyndigheter och att befintlig tillsynsmyndighet i första hand bör få tillsynsansvar över en tillkommande sektor.

Föreskrifter

Utredningen menar att en gemensam föreskrift med grundkrav som gäller för samtliga sektorer och som kan kompletteras av föreskrifter från tillsynsmyndigheterna inte är en framkomlig väg. Som skäl för detta ges bland annat att det kan komma genomförandeakter på EU-nivå för olika sektorer och att det finns en risk för att det uppstår en regelkonflikt mellan den övergripande föreskriften och tillsynsmyndighetens verkställighetsföreskrift. För att underlätta för verksamhetsutövare som bedriver verksamhet i flera sektorer föreslår utredningen att regeringen bör ge MSB i uppdrag att skyndsamt utarbeta en vägledning till stöd för föreskriftsarbetet. Vägledningen är inte juridiskt bindande. Utredningen föreslår även att Inspektionen för vår och omsorg (IVO) i egenskap av tillsynsmyndighet, och inte Socialstyrelsen, ska få utfärda föreskrifter för hälso- och sjukvård.

Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. MSB ska i dessa fall få möjlighet att yttra sig.

MSB får meddela föreskrifter för offentlig förvaltning då det finns fyra tillsynsmyndigheter för denna sektor.

MSB får även meddela föreskrifter för betydande incident och incidentrapportering, vilka verksamhetsutövare som omfattas och om de är väsentliga samt verksamhetsutövarnas anmälningsskyldighet.

Tillsynsmyndighetens undersökningsbefogenheter

Tillsynsmyndigheten får, om det finns särskilda skäl, beordra en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att

redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner som inte ska bekostas av verksamhetsutövaren.

Tillsynsmyndigheten får även låta genomföra säkerhetsskanningar. Utredningen gör tolkningen att detta avser en sårbarhetsskanning som kan göras på verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemet.

Samordning och informationsutbyte

MSB ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Utredningen anser att tillsynsmyndigheterna har kunskap om det tillsynsområde som de ansvarar för. Därför lämnar utredningen inget förslag om att en central myndighet, MSB, skulle vara tillsynsvägledande myndighet för samtliga sektorer. Utredningen menar att samarbetsforumet räcker för en effektiv och likvärdig tillsyn och förutsätter engagemang och personalresurser från tillsynsmyndigheterna. Utredningen föreslår även att det bör ges tydliga återrapporteringskrav i samtliga tillsynsmyndigheters regleringsbrev för att ge förutsättningar för uppföljning och effektiv styrning.

Utredningen gör bedömningen att MSB inte kan ges ett tydligare mandat eftersom de inte är huvudansvariga för tillsyn enligt föreslagen reglering. För att hantera tillsyn av verksamhetsutövare som bedriver verksamhet inom flera sektorer föreslår utredningen att respektive tillsynsmyndighet inte ska utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde. Utredningen menar att situationen sannolikt främst kommer uppstå när det gäller kommuner, men att i många fall bedriver kommuner sådan verksamhet i ett kommunalt bolag.

Ingripanden och sanktioner

Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt lagen om cybersäkerhet eller föreskrifter som har meddelats. Det gäller föreskrifter om skyldighet att utse företrädare, anmälningsskyldighet, riskhanteringsåtgärder, utbildning samt incidentrapportering. Utredningen föreslår att tillsynsmyndigheten får avstå från att ingripa om någon annan har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga. Samtidigt ska det, enligt utredningens mening, råda stark presumtion för ingripande. Det ska enligt utredningen vara möjligt att genomföra åtgärder även om en annan myndighet ingripit, så länge dubbelprövningsförbudet inte överträds.

Konsekvensanalys

Utredningen bedömer att förslagen innebär en viss inskränkning i den kommunala

självstyrelsen men att det är nödvändigt på grund av det stora intresset av att öka cybersäkerheten.

Utredningen avfärdar finansieringsprincipen och menar att kraven inte är omfattande eftersom förslagen med undantag av skyldigheten om systematiskt informationssäkerhetsarbete inte innehåller några krav som syftar till att uppnå en högre nivå av säkerhet än de som följer av direktivet. Utredningen menar att kommunerna tjänar på att införa säkerhetsåtgärder. Vidare argumenteras det för att enhetliga regler, tillsyn och möjligheten att få upplysningar av tillsynsmyndigheten kommer bidra till minskade kostnader för verksamhetsutövaren. Utredningen föreslår därför att de ekonomiska konsekvenserna ska finansieras inom offentliga verksamhetsutövares befintliga budgetram.

Remissinstansens yttrande

Servicenämnden

Servicenämnden delar utredningens uppfattning att verksamhetsutövare som under dagens lagstiftning bedöms vara tillhandahållare av samhällsviktiga tjänster, i ny lagstiftning, inte per automatik ska anses vara av typen väsentlig verksamhetsutövare. Nämnden anser dock att övergångsbestämmelser måste tas fram.

Nämnden anser också att begreppet säkerhetsskanning bör förtydligas i syfte att skapa samsyn kring begreppets innebörd.

Interna remisskonferenser

Övriga förvaltningar, kommunala bolag och kommunalförbund har genom interna remisskonferenser beretts tillfälle att inkomma med synpunkter på författningsförslagen. Samordnare från grundskoleförvaltningen, serviceförvaltningen, gymnasie- och vuxenutbildningsförvaltningen, miljöförvaltningen, hälsa-, vård och omsorgsförvaltningen, kulturförvaltningen, arbetsmarknads- och socialförvaltningen, förskoleförvaltningen, stadsbyggnadskontoret och fritidsförvaltningen har deltagit. Även representanter från VA-Syd, MKB Fastighets AB, Boplats Syd AB, Parkering Malmö AB, Parkeringsövervakning i Malmö AB samt Sysav har deltagit.

På remisskonferensen lyfts det fram en önskan om att föreskrifter skyndsamt ska tas fram kring vilka verksamhetsutövare som omfattas av regleringen och vad som utgör en betydande incident.

Det har även lyfts fram synpunkter om att lagtexten ska vara så konkret som möjligt. Detta skapar bättre förutsättningar för en hög lägstanivå av cybersäkerhet. Redan etablerade begrepp från nuvarande reglering och standarder bör därför användas. Förvaltningarna anser att det är bra att krav på systematiskt

informationssäkerhetsarbete inkluderas i förslaget eftersom begreppet informationssäkerhet är relativt väletablerat och känt från nuvarande reglering medan cybersäkerhet är ett nytt begrepp för många. För tydlighetens skull framförs det att också lag och förordning borde heta ”Informations- och cybersäkerhetslag” samt ”Informations- och cybersäkerhetsförordning”. Förvaltningarna anser att det säkerställer kontinuitet och länkar samman det nya begreppet cybersäkerhet med en större och väletablerad kontext.

Avseende det system för tillsyn som föreslås har förvaltningarna framfört att de gärna ser att möjligheten till en central tillsynsmyndighet utreds. Förvaltningarna anser också att MSB bör ta fram gemensamma föreskrifter rörande systematiskt och riskbaserat informations- och cybersäkerhetsarbete, grundläggande krav på säkerhetsåtgärder och utbildning som sedan tillsynsmyndigheterna kompletterar vid behov.

Avseende ingripande och sanktioner anser förvaltningarna att det borde finnas någon typ av karantänstid så att tillsyn av en tillsynsmyndighet utifrån vissa paragrafer inte får ske inom en viss tid av en annan tillsynsmyndighet. Slutligen skulle ekonomiskt stöd till kommunerna ge en tydlig signal om att införandet av säkerhetsåtgärder i offentlig förvaltning är en prioritet för staten.

Stadskontorets bedömning

Stadskontoret instämmer generellt i de synpunkter som lämnats av servicenämnden, förvaltningar, bolag och förbund. Stadskontoret anser dock inte att övergångsbestämmelser krävs.

5.1 Direktivet ska i huvudsak genomföras genom ny NIS-lag

Stadskontoret anser att den reglering som föreslås istället bör benämnas ”Lag (2024/5:XX) om informations- och cybersäkerhet” och ”Förordning (2024/5:XX) om informations- och cybersäkerhet”.

Utredningens förslag till benämning antyder att lagen endast inbegriper skydd av informations- och nätverkssystem mot cyberhot. Men stadskontoret anser att 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 begreppet informationssäkerhet är mer väletablerat genom nuvarande reglering samt relevanta europeiska och internationella standarder och därmed välkänt hos de verksamhetsutövare som omfattas av lagen.

5.2.10 Kommuner

Stadskontoret saknar ett resonemang i utredningen huruvida kommunalförbunden ska omfattas utifrån föreslagen lagstiftning. Av kommunallagen (2017:725) framgår att om inget annat anges eller följer av bestämmelserna om kommuner och regioner i

kommunallagen tillämpas de bestämmelserna även för kommunalförbund. Stadskontoret anser därför att frågan huruvida kommunalförbund omfattas av regleringen bör förtydligas.

Stadskontoret anser även att det bör förtydligas hur kommuner förhåller sig till sektorn offentlig förvaltning. Utredningen bedömer att en stor andel av kommunerna omfattas i sin helhet av regleringen eftersom de flesta kommuner bedriver hemsjukvård och uppfyller storlekskravet. Utredningen konstaterar dock att det finns kommuner som inte bedriver hemsjukvård och därmed inte ingår i sektorn hälso- och sjukvård, men att även dessa bör omfattas av regleringen. Av utredningens förslag framgår det inte uttryckligen huruvida kommuner omfattas av sektorn offentlig förvaltning. Av utredningen framgår inte heller i vilka fall en kommun kan bli föremål för tillsyn utifrån sektorn offentlig förvaltning.

Utredningen drar slutsatsen att det är kommunen som juridisk person som är vårdgivare och därmed verksamhetsutövare och att hela kommunen omfattas på den grunden. Stadskontoret vill dock påpeka att det är i nämnderna som verksamhet bedrivs alternativt i de kommunala bolagen. Detta har även Sveriges kommuner och regioner (SKR) framfört. Stadskontoret instämmer i SKR:s invändning att det inte är nödvändigt att det är kommunen som juridisk person som är verksamhetsutövare enligt föreslagen reglering.

Stadskontoret hänvisar till bestämmelsen i 6 kap. 15 § kommunallagen om att styrelsens allmänna processbehörighet inte med nödvändighet leder till slutsatsen att det är kommunen som juridisk person som ska omfattas av föreslagen reglering. Stadskontoret anser därför att en nämnd inom kommunen, som inte är en egen juridisk person, borde kunna utgöra en särskild enhet. Det innebär att enskilda nämnder skulle kunna omfattas av de föreslagna kraven snarare än kommunen som helhet.

6.2 Register över väsentliga och viktiga verksamhetsutövare

Stadskontoret anser att anmälnings- och uppgiftsskyldigheten behöver underlättas genom att anmälan sker till den centrala kontaktpunkten MSB istället för till respektive tillsynsmyndighet. MSB kan sedan förmedla uppgifter vidare till tillsynsmyndigheterna.

Kommuner kan ingå i flera sektorer, och det kan därför bli aktuellt med flertalet tillsynsmyndigheter. Utredningens förslag kräver att kommunen överför uppgifter på ett säkert sätt till flera olika tillsynsmyndigheter, i värsta fall genom olika IT-system som tillsynsmyndigheterna tillhandahåller. Uppgifterna ska sedan vidareförmedlas till MSB. Stadskontoret anser att detta innebär en onödig administrativ belastning för både kommunerna och tillsynsmyndigheterna.

7.1 Övergripande lagreglering om riskhanteringsåtgärder

Stadskontoret anser att lagstiftaren bör vara så konkret som möjligt i lagtexten så att minimikraven från direktivet framgår. Vad gäller föreskrifter bör MSB ta fram gemensamma grundföreskrifter rörande systematiskt och riskbaserat informations- och cybersäkerhetsarbete, grundläggande krav på säkerhetsåtgärder (riskhanteringsåtgärder) och utbildning. Tillsynsmyndigheterna ska kunna komplettera dessa vid behov.

Stadskontoret vill lyfta fram att det är viktigt att lagen är så tydlig som möjligt. Det främjar en hög lägsta nivå för informations- och cybersäkerhet i Sverige och minskar risken för motstridiga föreskrifter.

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. Motstridiga föreskrifter kan vara svåra för kommuner att omhänderta eftersom de ska gälla i hela verksamheten och inte bara för den samhällsviktiga tjänsten.

7.1.1 Övergripande om begrepp

Stadskontoret anser att lagen bör använda begreppet ”säkerhetsåtgärder” istället för ”riskhanteringsåtgärder”. Detta knyter an till nuvarande NIS-reglering och harmoniserar även med relevanta europeiska och internationella standarder och uppmuntrar därigenom till användningen av dessa. Riskhanteringsåtgärderna i direktivet är välbekanta åtgärder från standarder. ”Säkerhetsåtgärder” är ett väletablerat begrepp med koppling till standarden "SS-EN ISO/IEC 27001:2023 - Informationssäkerhet, Cybersäkerhet och Integritetsskydd", som många verksamhetsutövare inom offentlig förvaltning använder och som MSB förespråkar.

8.4.1 System för tillsyn

Stadskontoret anser att möjligheten att ha en central tillsynsmyndighet bör utredas eftersom det hade underlättat för verksamhetsutövare som ingår i flera sektorer. Som utredningen påpekar krävs det expertkunskap för att utöva tillsyn avseende cybersäkerhet, vilket i sig ur ett kompetensförsörjningsperspektiv är ett argument för att ha en central tillsynsmyndighet eftersom konkurrensen om kompetens då inte blir lika stor.

8.4.5 Föreskrifter

Stadskontoret anser att kommuner bör tillåtas omhänderta de sektorsspecifika föreskrifterna i de nämnder som bedriver verksamhet inom respektive sektor och föreskrifter för offentlig förvaltning i den övriga verksamheten.

Utredningens förslag innebär att en kommun kan behöva beakta föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt

utbildning från flertalet olika tillsynsmyndigheter. Om IVO övertar föreskriftsrätten från Socialstyrelsen ser stadskontoret att det kan innebära ytterligare risk för motstridiga föreskrifter. Socialstyrelsen meddelar föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården och socialtjänsten.

Stadskontoret bedömer att det kan vara mycket svårt att i praktiken hantera denna flora av föreskrifter eftersom utredningen menar att kraven ska gälla för hela verksamheten och inte bara för samhällsviktiga och digitala tjänster.

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Stadskontoret anser att begreppet säkerhetsskanning bör förtydligas i en ny författning för att skapa en samsyn kring begreppets innebörd.

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).

8.4.7 Samordning och informationsutbyte

Stadskontoret anser att MSB bör få ett tydligare mandat att samordna metodik, planering och uppföljning av tillsyn. Om det inte är genomförbart bör länsstyrelserna, som fått ansvar för offentlig förvaltning, få samordningsansvar för tillsyn av verksamhetsutövare inom offentlig förvaltning som även ingår andra sektorer.

Stadskontoret gör bedömningen att utredningens förslag inte är tillräckligt för att samordna arbetet med tillsyn. Det framgår inte hur tillsynsmyndigheternas avgränsning av deras granskningar ska genomföras i praktiken när kommunens linjeorganisation bedriver verksamhet inom flera sektorer, samtidigt som nämnderna inte betraktas som enheter hos den juridiska personen. Det kan medföra granskningar som följer så pass nära inpå varandra att kommunen inte hinner vidta åtgärder innan nästa granskning inleds. Stadskontoret förespråkar att det bör införas en tidsfrist efter genomförd granskning. Stadskontoret vill undvika att två olika tillsynsmyndigheter samtidigt eller för tätt inpå varandra ska granska en verksamhetsutövare.

Utan utökad samordning finns det en risk att kommunerna kommer behöva lägga mycket resurser på att hantera granskningar snarare än att vidta de riskhanteringsåtgärder som kravställs i regleringen. Detta är särskilt angeläget i relation till utredningens förslag om att skärpa tillsynsmyndigheternas återrapporteringskrav.

9 Ingripanden och sanktioner

Stadskontoret anser att utökad samordning behövs för att skapa tydlighet.

Stadskontoret anser att det är bra att säkerställa att tillsynsmyndigheter kan avstå från att ingripa om någon annan redan har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och tillsynsmyndigheten anser åtgärderna tillräckliga. Det är samtidigt viktigt att samplanering av granskningar sker från centralt håll så att det så långt möjligt undviks att tillsynsmyndigheterna agerar på samma område och inom samma tidsram.

Stadskontoret anser däremot att det inte är rimligt att en tillsynsmyndighet ska kunna göra bedömningen att ett åtgärdsföreläggande är tillräckligt och att en annan tillsynsmyndighet trots det kan göra bedömningen samma överträdelse ska leda till en sanktionsavgift.

12.7 Ekonomiska konsekvenser för offentliga verksamhetsutövare

Stadskontoret anser att det bör införas en grundnivå för ekonomiskt stöd till kommunerna för genomförandet av riskhanteringsåtgärderna (säkerhetsåtgärderna) i regleringen. Därefter bör en uppräkning ske baserad på antalet invånare i kommunen.

Resultatet från MSB:s uppföljningsstruktur 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.

Stadskontoret menar att det krävs ett omfattande arbete och utökade resurser, inte minst för kompetensförsörjning, för att kommunerna ska kunna införa proportionella säkerhetsåtgärder som löpande följs upp och utvärderas.

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. Stadskontoret befarar att detta kan komma vara mycket kostnadsdrivande, samtidigt som de mindre kommunerna kan sakna en mottagarorganisation som systematiskt kan omhänderta och vidareutveckla det som levereras. Dessa faktorer beaktas inte i utredningens konsekvensanalys.

Utifrån vad som ovan anförts förordas att kommunstyrelsen godkänner förslag till yttrande och skickar det till Försvarsdepartementet.

Ansvariga

Per-Erik Ebbeståhl Avdelningschef
Magdalena Bondeson Sektionschef
Andreas Norbrant Stadsdirektör