§ 140

Remiss delbetänkandet nya regler om cybersäkerhet- SOU 2024:18

Ärendenr 2024/477-1.3.1.5

Kommunstyrelsens beslut

Kommunstyrelsen beslutar att anta kommunstyrelseförvaltningens yttrande som sitt eget och överlämna svaret till Försvarsdepartementet.

Sammanfattning av ärendet

Luleå kommun tillstyrker i huvudsak utredningens förslag och bedömningar. Kommunen anför vissa ståndpunkter rörande de föreskrifter som ska utfärdas med anledning av de bemyndiganden som framgår av föreslagen förordning. Luleå kommun anser vidare att samarbetet mellan tillsynsmyndigheterna behöver omfattas av högre krav och att tillsynsmyndigheternas uppdrag behöver förtydligas i syfte att undvika att överlappande tillsyner.

EU-direktivet NIS2 (*The Second Directive on security of network and information systems, direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen*) antogs den 14 december 2022. NIS2 ställer krav på säkerhet i nätverks- och informationssystem. Delbetänkandet föreslår införlivning av NIS2-direktivet i svensk lag, genom att ersätta nuvarande lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster med en ny lag om cybersäkerhet.

Lagförslaget innebär att antalet berörda sektorer utökas från 7 till 18 samt att kraven omfattar hela verksamheten i stället för att avgränsas till den samhällsviktiga verksamheten eller den digitala tjänsten. Sektorerna är bland annat energi, transporter, digital infrastruktur, hälso- och sjukvård, livsmedel, dricksvatten, avloppsvatten, avfallshantering och offentlig förvaltning. Offentlig förvaltning innebär enligt betänkandet att hela kommunens verksamhet, förutom kommunfullmäktige, omfattas. Antalet tillsynsmyndigheter föreslås utökas som en konsekvens av fler sektorer.

Kommunstyrelsens arbetsutskott har 2024-05-06 § 76 föreslagit kommunstyrelsen besluta att anta remissvaret som sitt eget och överlämna svaret till Försvarsdepartementet.

Sammanträdet

Ordföranden ställer kommunstyrelsens arbetsutskotts förslag under proposition och finner att kommunstyrelsen bifaller förslaget.

Beskrivning av ärendet

Kommunstyrelseförvaltningens yttrande

Nedan redovisas kommunens synpunkter på förslagen i betänkandet. Redovisningen följer betänkandets indelning.

1.4 Förslag till förordning om cybersäkerhet

Luleå kommun tillstyrker förslaget till förordning om cybersäkerhet men önskar följande tillägg rörande tillsynsmyndigheternas uppdrag.

Tillsynsmyndigheternas uppgifter framgår av 14-19 §§. Luleå kommun anser att dessa uppgifter bör kompletteras med det krav som ställs på CSIRT-enheten (*Computer Security Incident Response Team*) i 28 § 6 punkt i förslaget till förordning. CSIRT-enheten ska enligt bestämmelsen ha en säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter. Luleå kommun anser att det är rimligt att även tillsynsmyndigheterna har tillgång till säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter.

4.2 Energi

Producenter av elektricitet ska omfattas av NIS2-direktivet, enligt utredningen avses då *producent en fysisk eller juridisk person som framställer el*. Laddningsoperatörer ska omfattas av NIS2-direktivet, enligt utredningen avses då *laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn.* Luleå kommun noterar att detta innebär att ett fastighetsbolag som har solceller på sina fastigheter och/eller tillhandahåller laddningsmöjligheter vid sina parkeringsplatser kan komma att omfattas av NIS2-direktivet. NIS2 direktivet är avsett att öka cybersäkerheten inom 18 sektorer. Fastigheter är inte en sådan sektor men fastighetsbolag kan ändå komma att omfattas.

Luleå kommun anser att de föreskrifter som tillsynsmyndigheterna ska bemyndigas att utfärda måste vara mycket tydliga och adekvata för olika verksamhetsutövare, så som till exempel fastighetsägare, så att det framgår med tydlighet vilka som ska omfattas av kraven i den nya lagen.

4.5 Digital infrastruktur

Enligt NIS2-direktivet och utredningen så ska tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster omfattas av den nya cybersäkerhetslagen. Exempel på sådana tjänster är 5G-mobilnät. Fastighetsägare som äger så kallade ”täta hus” och därför tillhandahåller mobilnät i dessa fastigheter kan komma att klassas som en tillhandahållare av elektroniska kommunikationstjänster och eventuellt även som tillhandahållare av allmänna elektroniska kommunikationsnät.

Täta hus är hus som för att de ska vara energieffektiva och hållbara är byggda med material i väggar och fönster som minskar värmestrålning men då även högfrekventa radiovågor så som 4G- och 5G-mobilnät. Detta medför att hyresgäster inte kan ringa normalt via sina mobiltelefoner eller att mobilbaserade enheter som till exempel 5G-personlarm inte kan kommunicera säkerhet. För att erbjuda fungerande mobilnät i täta hus finns lösningar som förlänger mobiloperatörernas nät in i byggnaden så att alla kommer åt näten. Tekniken gör inte skillnad på hyresgäster och besökare, detta gör näten allmänna.

NIS2 direktivet är avsett att öka cybersäkerheten inom 18 sektorer. Fastigheter är inte en sådan sektor men fastighetsbolag kan ändå komma att omfattas.

Luleå kommun anser att de föreskrifter som tillsynsmyndigheterna ska bemyndigas att utfärda måste vara mycket tydliga och adekvata för olika verksamhetsutövare, så som till exempel fastighetsägare, så att det framgår med tydlighet vilka som ska omfattas av kraven i den nya lagen.

5.2.10 Kommuner

Av utredningen framgår det att Sveriges kommuner och regioner har invänt mot att kommunen som juridisk person ska anses vara verksamhetsutövaren och att kommunen därmed utgör en enhet enligt NIS2-direktivet. En sådan tolkning skulle innebära att en nämnd kan betraktas som en enhet och därmed en verksamhetsutövare. Mot bakgrund av att kommunen enligt förslaget kommer att få flera tillsynsmyndigheter så skulle en tolkning där nämnd kan anses vara verksamhetsutövare bidra till att minska risken för överlappande tillsyn och konsekvenser av det, vilket utvecklas vidare nedan under punkt 8.4.3.

5.2.11 Alternativt förslag

I kapitel 5.2.11 lämnar utredningen alternativa förslag som inkommit till utredningen från Myndigheten för samhällsskydd och beredskap (MSB) respektive Säkerhetspolisen. MSB föreslår att hela den offentliga sektorn (samtliga statliga myndigheter, regioner och kommuner) borde omfattas av föreslagen cybersäkerhetslag för att säkerställa ett allriskperspektiv. Säkerhetspolisen har föreslagit att det inte bör finnas ett undantag för myndigheter som bedriver

säkerhetskänslig verksamhet och har anfört att föreslagen cybersäkerhetslag bör utgöra en bottenplatta för som i förekommande fall kompletteras med säkerhetsskyddslagens bestämmelser.

MSB har i sitt remissvar, MSB 2024-03843-3, utvecklat sin syn på behov av samordning mellan NIS2-direktivet, det närliggande CER-direktivet (*Critical Entities Resilience directive, direktivet om kritiska entiteters motståndskraft)* och säkerhetsskyddslag (2018:585). Bland annat påtalar MSB att när även CER-direktivet implementerats i svensk lag bör dessa tre lagar och samordningen mellan dem ses över för att minska fragmenteringen på området i form av både överlappningar och luckor i regelverken, terminologi och struktur.

Luleå kommun anser att det kan vara rimligt att cybersäkerhetslagen utgör en bottenplatta även för säkerhetskänslig verksamhet och understryker behovet av att lagstiftningen för samhällsviktigt och säkerhetskänslig verksamhet görs mer enhetlig. Luleå kommun vill också anföra att det är viktigt att se över den samlade strukturen över tillsynsmyndigheter, där det redan i nuvarande informationssäkerhetslag och säkerhetsskyddslag är olika tillsynsmyndigheter för dricksvattenförsörjningen.

7.1.1 Övergripande begrepp

Luleå kommun delar inte utredningens bedömning.

Luleå kommun föreslår att begreppet *riskhanteringsåtgärder* ersätts med *säkerhetsåtgärder*. Utredningen anför att *säkerhetsåtgärder* förvisso är ett mer etablerat begrepp och förekommer i nuvarande informationssäkerhetslag men bör ersättas med det *riskhanteringsåtgärder* bland annat eftersom det ska signalera att det är en utökning av kraven. Att kraven utökas framgår av förslaget till ny lag och då informationssäkerhetslagen ska upphävas när föreslagen cybersäkerhetslag träder i kraft så anser Luleå kommun att argumentet inte är relevant. Att använda etablerade begrepp är betydelsefullt i all kommunikation och **säkerhet**såtgärder kopplar också tydligt an till benämningen av föreslagen lag, cyber**säkerhet**slag.

7.1.2 Riskhanteringsåtgärder

Luleå kommun tillstyrker i huvudsak utredningens förslag.

Luleå kommun noterar att i redogörelsen över riskhanteringsåtgärder anges ”personalsäkerhet” som en sådan. Innebörden av personalsäkerhet förklaras inte närmare i betänkandet. Personalsäkerhet förklaras dock i 2 kap. 4 § i säkerhetsskyddslagen och innebär utredningar och registerprövningar. Luleå kommun antar att personalsäkerhet i den föreslagna cybersäkerhetslagen har en annan innebörd än i säkerhetsskyddslagen. Luleå kommun anser att innebörden av personalsäkerhet i cybersäkerhetslagen behöver utvecklas.

8.3.2 Samarbetsforum
Luleå kommun delar inte utredningens bedömning.

Utredningen föreslår att nuvarande lösning för samarbete enligt NIS1-direktivet ska fortsätta gälla även med implementeringen av NIS2-direktivet i svensk lag. Detta trots att utredningen konstaterar att samarbetet mellan tillsynsmyndigheterna inte varit fullt adekvat. Brister i samarbetet och samordningen mellan tillsynsmyndigheterna riskerar att drabba verksamhetsutövare som omfattas av flera sektorer, så som kommuner.

8.4.3 Tillsynsmyndighetens uppdrag
Luleå kommun tillstyrker i huvudsak utredningens förslag.

Enligt utredningens förslag ska varje tillsynsmyndighet (totalt 11 stycken) utöva tillsyn över cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen. Varje tillsynsmyndighet tilldelas en eller flera sektorer att utöva tillsyn inom.

Av 13 § i föreslagen cybersäkerhetsförordning framgår att *om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde […]".* Luleå kommun uppfattar dock att samtliga tillsynsmyndigheter har uppdrag att bedriva tillsyn mot de delar av kommunens verksamhet som inte omfattas av någon sektor. Vidare ska varje tillsynsmyndighet utöva tillsyn enligt cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen (2 § förordningen). Om varje tillsynsmyndighet ska utfärda egna föreskrifter för sin/sina sektorer så bör de endast ha i uppdrag att bedriva tillsyn av att dessa föreskrifter följs, inte att samtliga följs. Luleå kommun uppfattar att nuvarande förslag kan innebär att flera tillsynsmyndigheter ska bedriva tillsyn enligt lag och samtliga föreskrifter och att uppdelningen mellan dem endast gäller för sektorsspecifik verksamhet. Luleå kommun anser att regleringen behöver förtydligas i dessa avseenden.

Luleå kommun uppfattar vidare att kommuner kan hamna i en situation där tillsynsmyndigheter bedriver överlappande tillsyn, gör olika bedömningar och därmed utfärdar icke-samordnade sanktioner mot kommunen. Luleå kommun anser att regleringen behöver förtydligas i dessa avseende så att sådana situationer inte kan uppkomma.

8.4.5 Föreskrifter
Luleå kommun tillstyrker delar av utredningens förslag.

Utredningen föreslår att varje tillsynsmyndighet bemyndigas att inom sitt tillsynsområde (sektor) få meddela föreskrifter om riskhanteringsåtgärder,

systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. Detta innebär att verksamhetsutövare som omfattas av flera sektorer och därmed av flera tillsynsmyndigheter måste förhålla sig till en uppsättning av föreskrifter. Att bedriva ett systematiskt arbete kommer inte att underlättas av att det är flera olika systematiker som ska införas. Luleå kommun avstyrker därför förslaget om att varje tillsynsmyndighet ska få utfärda en egen uppsättning krav på kommunernas arbete. I de fall det förekommer tungt vägande skäl för krav på sektorsspecifika riskhanteringsåtgärder så bör sådan föreskrift kunna utfärdas av tillsynsmyndighet. Samråd med samtliga tillsynsmyndigheter bör ske för att säkerställa att riskhanteringsåtgärden inte är av allmän karaktär.

I betänkandet föreslås att Myndigheten för samhällsskydd och beredskap ska bemyndigas att meddela föreskrifter om vad som utgör en betydande incident. Luleå kommun anser att detta är positivt då den definition av betydande incident som framgår av NIS2-direktivets artikel 23.2 ger för stort tolkningsutrymme. Luleå kommun anser att föreskrifter om betydande incident med fördel preciseras per sektor för att underlätta tillämpningen. Den föreslagna ordningen med att tillsynsmyndigheterna ska ges tillfälle att yttra sig inför att sådana föreskrifter utfärdas skapar förutsättningar för relevanta sektorsvisa definitioner.

Dialog:

Kommunstyrelseförvaltningen har samordnat framtagandet av remissvaret. Samtliga förvaltningar och helägda kommunala bolag har beretts möjlighet att lämna synpunkter. Luleå Hamn AB och Lulebo AB har inkommit med synpunkter på betänkandet.

Beslutsunderlag

- Remissmissiv delbetänkandet nya regler om cybersäkerhet (SOU 2024:18), KLF Hid: 2024.2088
- Kommunstyrelseförvaltningens förslag gällande yttrande över delbetänkandet nya regler om cybersäkerhet SOU 2024:18, KLF Hid: 2024.3685
- Kommunstyrelsens arbetsutskotts beslut 2024-05-06 § 76, KLF Hid: 2024.4047

Beslutet skickas till

Försvarsdepartementet