



Regeringskansliet - Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Yttrande över remiss om delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Er beteckning: Fö2024/00496

Sammanfattning

Länsstyrelsen i Stockholms län (Länsstyrelsen) ser positivt på arbetet med att stärka cybersäkerheten i unionen. I utredningen föreslås Länsstyrelsen bli en av fem nya tillsynsmyndigheter. Länsstyrelsen yttrar sig med utgångspunkt i de delar av utredningen som berör tillsyn över de tillkommande sektorerna i NIS2-direktivet.

Länsstyrelsen tillstyrker förslaget om att bli en ny tillsynsmyndighet.

Länsstyrelsen lämnar därutöver några synpunkter på utredningens förslag och bedömningar.

5.2.1 Utgångspunkter

Länsstyrelsen anser att utredningens begrepp "riskhanteringsåtgärder" bör bytas ut mot det vedertagna begreppet "säkerhetsåtgärder". Det kommer att underlätta tillämpningen av den föreslagna cybersäkerhetsregleringen om regleringen använder begrepp finns i annan reglering och standarder.

5.5.4 Undantag för offentliga verksamhetsutövare

Länsstyrelsen instämmer inte i utredningens förslag om att undanta offentliga verksamhetsutövare som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning. Länsstyrelsen anser att det skulle underlätta tillämpningen och öka acceptansen för regelverket om samtliga aktörer omfattades av lagens tillämpningsområde. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig eller brottsbekämpande verksamhet krävs god cybersäkerhet.

5.5.5 Undantag för enskilda verksamhetsutövare

Länsstyrelsen instämmer inte i utredningens förslag om att undanta enskilda verksamhetsutövare som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig eller brottsbekämpande verksamhet krävs god cybersäkerhet.

6.2 Register över väsentliga och viktiga verksamhetsutövare

Länsstyrelsen anser att tidsramen för myndigheten att upprätta ett register över väsentliga och viktiga verksamhetsutövare är väldigt kort. Särskilt med tanke på att uppdraget att genomföra tillsyn utifrån NIS2-direktivet är nytt för myndigheten.

Verksamhetsutövarna har ännu kortare tid på sig att inkomma med en anmälan. Det föreslås även vara sanktionsgrundande vid utebliven anmälan. Länsstyrelsen ställer sig därför frågande till den snäva tidsramen och anser att den bör förlängas.

Länsstyrelsen vill även framhäva att det administrativa arbetet med att förvalta ett register kommer vara mödosamt och resurskrävande för att säkerställa konfidentialitet, tillgänglighet och riktighet av uppgifterna. Det kommer kräva särskilt it-stöd för myndigheten.

Länsstyrelsen anser att Myndigheten för samhällsskydd och beredskap (MSB) bör få i uppdrag att etablera och förvalta en gemensam systemplattform för hantering av registren över väsentliga och viktiga verksamhetsutövare. Då det ur ett samhällsekonomiskt perspektiv inte är resurseffektivt att varje tillsynsmyndighet tar fram egna systemlösningar som ska hantera verksamhetsutövarnas anmälningar, som i slutända ska delas med MSB i egenskap av gemensam kontaktpunkt.

8.4.1 System för tillsyn

Länsstyrelsen vill understryka utredningens konstaterande om att tillsyn av it- och informationssäkerhet kräver expertkunskap och att det råder brist på kompetens inom området. Det är även stor konkurrens på arbetsmarknaden. Länsstyrelsen ser redan idag stora utmaningar med att rekrytera medarbetare med denna typ av kompetens.

8.4.2 Tillsynsmyndigheter i Sverige

Länsstyrelsen tillstyrker att Länsstyrelsen i Stockholms län ska vara en av fem nya tillsynsmyndigheter.

Utmaningar med fler tillsynsmyndigheter för en verksamhetsutövare

I utredningen framförs förslag om att en verksamhetsutövare ska kunna ha flera tillsynsmyndigheter. Det innebär att tillsynsmyndigheten ska bedriva tillsyn över en aktörs verksamhet som inte omfattas av en annan aktörs tillsyn. Länsstyrelsen anser att detta kan bli en stor utmaning för både verksamhetsutövarna och tillsynsmyndigheterna. Exempelvis kan vissa kommuner komma ha flera tillsynsmyndigheter, då de bedriver hälsosjukvård, vattenverksamhet och kommunal verksamhet. Kommunen kommer i denna situation behöva anmäla sig till flera tillsynsmyndigheter och kan komma omfattas av flera föreskrifter. Det kan även skapa otydlighet för verksamhetsutövaren angående vem de ska vända sig till vid frågor och osäkerhet vid tillsyn.

För tillsynsmyndigheten kan detta kräva stora resurser för att samverka och samarbeta med andra tillsynsmyndigheter så att tillsynen blir likvärdig. Det kan även bli administrativt betungande och ta resurser från den faktiska tillsynen. Länsstyrelsen anser även att det kan bli svåra gränsdragningar gällande vilken tillsynsmyndighet som kan bedriva tillsyn mot vad, då hela verksamheten omfattas. Länsstyrelsen menar att det kan bli ett ineffektivt arbetssätt som inte kommer öka cybersäkerheten.

Problem med att länsstyrelserna utövar tillsyn över varandra

Offentlig förvaltning är i NIS2-direktivet en ny sektor. De fyra länsstyrelserna som föreslås bli nya tillsynsmyndigheter ska ansvara för tillsynen för kommuner, regioner och statliga myndigheter som inte hör till någon annan myndighets ansvarsområde.

Länsstyrelserna kommer enligt utredningen själva att ingå i sektorn offentlig förvaltning. Eftersom en tillsynsmyndighet inte ska utöva tillsyn över den egna organisationen föreslår utredningen att Länsstyrelsen i Stockholms län och Länsstyrelsen i Norrbottens län ska vara tillsynsmyndigheter för varandra. På samma sätt ska Länsstyrelsen i Västra Götaland och Länsstyrelsen i Skåne utöva tillsyn över varandra.

Länsstyrelsen anser att det finns utmaningar med att de fyra Länsstyrelserna ska bedriva tillsyn gentemot varandra. Dels på grund av att det finns ett nära samarbete mellan Länsstyrelserna, dels då vi har gemensam it som ökar problematiken.

Länsstyrelsernas gemensamma strukturer

Regeringskansliet har genom regleringsbrev förordnat att Länsstyrelserna ska ha en gemensam och effektiv it-verksamhet. Länsstyrelserna har en överenskommelse som reglerar den gemensamma it-verksamheten med Länsstyrelsen Västra Götaland som värmlänsstyrelse. Värmlänsstyrelsen ansvarar för Länsstyrelsernas it-säkerhet samt för att it-miljön ges en ändamålsenlig, effektiv och enhetlig utformning.

Länsstyrelserna har också en gemensam stödfunktion för informationssäkerhet och dataskydd, Safir, med Länsstyrelsen i Stockholm som värmyndighet. All anskaffning och utveckling av it hanteras gemensamt på Länsstyrelserna med en gemensam förvaltningsmodell som har Länsstyrelsen Västmanland som värmlänsstyrelse. Sammanfattningsvis innebär det att Länsstyrelsernas informations- och cybersäkerhetsarbete är väl integrerat och inte med lätthet kan tillsynas var för sig. De gemensamma strukturerna har en så pass stor påverkan på it- och informationssäkerheten att en korsvis tillsyn inom Länsstyrelserna skulle orsaka intressekonflikter och riskera att myndigheternas oberoende ifrågasätts.

8.4.5 Föreskrifter

Utredningen föreslår att tillsynsmyndigheten inom sitt tillsynsområde får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. I och med att en verksamhetsutövare kan anses bedriva verksamhet inom flera sektorer kan det innebära att en verksamhetsutövare omfattas av flera föreskrifter.

Länsstyrelsen anser att detta kan skapa stora svårigheter för verksamhetsutövarna vid arbetet med säkerhetsåtgärder. Länsstyrelsen föreslås bli tillsynsmyndighet för bl. a. kommuner, vilka då skulle behöva förhålla sig till flera olika föreskrifter eftersom deras verksamhet kan komma träffas av flera olika sektorer.

Länsstyrelsen bedömer att tillsynsmyndigheterna kommer behöva lägga ner omfattande resurser på detta. Då det kommer kräva stor

samverkan mellan tillsynsmyndigheterna för att säkerställa att tillsynen blir likvärd. Länsstyrelsen anser inte att detta kommer vara ett effektivt arbetssätt som höjer cybersäkerheten.

Länsstyrelsen menar att det därför bör övervägas att ge MSB föreskriftsrätt att utfärda gemensamma grundföreskrifter gällande riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete och utbildning

8.4.6 Tillsynsmyndighetens undersökningsbefogenheter

Tillsynsmyndigheten föreslås få anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare. Länsstyrelsen anser att det är otydligt kring finansieringen. Det framgår inte om det ska rymmas inom ramen för finansieringen för tillsynsuppdraget eller om det tillkommer särskilda resurser för dessa säkerhetsrevisioner. Om det är tänkt att ske inom ramen för finansieringen av tillsynsuppdraget ställer sig Länsstyrelsen frågande till om detta verktyg kommer användas.

Utredningen föreslår att tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen. Länsstyrelsen menar att det är otydligt gällande vem som ska genomföra säkerhetsskanningarna. Om det är tillsynsmyndigheten som ska genomföra detta skulle det innebära att förmågan samt it-stöd för att utföra säkerhetsskanningarna behöver finnas internt hos myndigheten. Detta bör därför tas hänsyn till i beräkning av anslaget för myndigheten.

9 Ingripanden och sanktioner

Länsstyrelsen anser att tillsynsmyndigheterna bör ha möjlighet att ingripa, på samma sätt, som beskrivet i 5 kap. 1 § förslag till lag om cybersäkerhet, mot verksamhetsutövare som inte bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete.

Länsstyrelsen anser att grunden till ett ändamålsenligt informationssäkerhetsarbete utgår ifrån ett systematiskt och riskbaserat arbetssätt. Utan denna möjlighet finns risk att tillsynen inte blir ändamålsenlig.

9.5.4 Utse övervakningsansvarig hos tillsynsmyndigheten

Tillsynsmyndigheten har möjlighet att utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda entiteterna efterlever artiklarna 21 och 23. Länsstyrelsen menar att det är otydligt vad detta innebär i praktiken och anser att det bör förtydligas.

12.6.2 Uppgifter för Myndigheten för samhällsskydd och beredskap

Länsstyrelsen anser att det bör övervägas att ge MSB i uppgift att utveckla utbildningar inom it- och informationssäkerhet för bland annat tillsynsmyndigheterna. Detta på samma sätt som Försvvarshögskolan har i uppdrag att utveckla utbildningar inom säkerhetsskydd¹. Länsstyrelsen anser att det är nödvändigt eftersom det råder stor brist på kompetens inom området.

12.6.7 Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för samhällsskydd och beredskap

Länsstyrelsen anser att de ekonomiska konsekvenserna för myndigheten behöver utredas vidare.

Även om Länsstyrelsen har i uppdrag att utöva tillsyn inom säkerhetsskyddsregleringen så krävs en annan typ av kompetens för att genomföra tillsyn inom den föreslagna cybersäkerhetslagen. Kunskap inom sakområdet är en förutsättning för att en ändamålsenlig tillsyn kan bedrivas.

Inom området föreligger en stor brist på kompetens. Ännu färre är de med tillsynserfarenhet och kunskap inom it- och informationssäkerhet. Dessa faktorer bör tas hänsyn till vid beräkning av anslaget till tillsynsmyndigheterna.

¹ Regleringsbrev för budgetåret 2024 avseende Försvvarshögskolan

Övrigt

- För att förtydliga ansvaret för tillsynsmyndigheterna anser Länsstyrelsen att det bör övervägas att, på samma sätt som i säkerhetsskyddsregelverket² införa ett kartläggningsuppdrag och ett vägledningsuppdrag i regleringen. Länsstyrelsen anser även att det är otydligt till vilken myndighet verksamhetsutövaren ska vända sig till vid vägledningsfrågor.
- Regeringen förslås ha ansvaret för återrapportering av uppdraget. Länsstyrelsen ser positivt på detta då det, enligt Länsstyrelsen, kommer leda till att tillsynsuppdraget prioriteras hos myndigheterna.

De som medverkat i beslutet

Beslut i detta ärende har fattats av vikarierande länsöverdirektör Claes Lindgren med Christel Manner som föredragande. I den slutliga handläggningen har avdelningschef Helene Munkner medverkat.

Denna handling har godkänts digitalt och saknar därför namnunderskrift.

² Se 8 kap. 4 & 12 §§ säkerhetsskyddsförordningen (2021:955)