Länsstyrelsen Västernorrland

Datum
2024-05-24

Diarienummer
2184-2024

Regeringskansliet
Försvarsdepartementet

Remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Er beteckning: Fö2024/00496

Sammanfattning

Länsstyrelsen i Västernorrlands län ställer sig i grunden positiv till att Sverige har ett klart och tydligt regelverk med krav på att verksamheter som har en viktig betydelse för ett robust och fungerande samhälle ska arbeta systematiskt och riskbaserat med informationssäkerhet och cybersäkerhet.

Länsstyrelsen bedömer däremot att den föreslagna cybersäkerhetslagen kan bli svår att både tillämpa och utöva tillsyn efter. Länsstyrelsen har synpunkter på utredningens bedömningar och förslag, vilka sammanfattningsvis är följande:

- Lagen bör använda redan vedertagna begrepp och definitioner.
- Lagen bör gälla i hela verksamhetsutövarens verksamhet.
- Lagen bör inte innehålla omfattande undantag eller vara subsidiär.
- Undantag bör inte göras för offentliga verksamhetsutövare, annat än för incidentrapportering, om sådan ska göras enligt bestämmelser i säkerhetsskyddsförordningen (2021:955).
- Undantag bör inte göras för enskilda verksamhetsutövare som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet.
- Länsstyrelser bör inte vara tillsynsmyndigheter för andra länsstyrelser.
- Försvarets radioanstalt bör vara CSIRT-enhet och cyberkrishanteringsmyndighet i Sverige, samt ha den övergripande föreskriftsrätten för systematiskt informationssäkerhetsarbete och cybersäkerhet.

I följande stycken redovisar länsstyrelsen mer detaljerat synpunkterna och skälen för dem. Avsnitten följer delbetänkandets rubriksättning.

5.2.1 Utgångspunkter

Länsstyrelsen stödjer användningen av vedertagna begrepp och normalt språkbruk. Att regleringen använder begrepp och språk som finns i annan reglering, standarder och normalt språkbruk kommer att underlätta tillämpningen av reglerna.

Utredningens begrepp ”riskhanteringsåtgärder” bör enligt länsstyrelsen bytas ut mot det vedertagna begreppet ”säkerhetsåtgärder”. Säkerhetsåtgärder är också det begrepp som används i standarden ISO/IEC 27000:2018 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi, samt i den tekniska rapporten SIS-TR 50:2015 Terminologi för informationssäkerhet.

5.2.2 Verksamhetsutövare

Länsstyrelsen anser att verksamhetsutövare är ett bra samlingsbegrepp för den som kan träffas av lagen. Det är redan ett vedertaget begrepp inom säkerhetsskyddsområdet, vilket kan förenkla implementeringen.

Länsstyrelsen delar utredningens bedömning att hela verksamheten bör omfattas av lagens tillämpningsområde. Ett informationssystem i en verksamhetsdel verkar i regel inte helt separat, utan har kopplingar och beröringspunkter med verksamheten i stort.

Ett fullgott informationssäkerhetsarbete bygger på att hela verksamheten omfattas och att inte enbart nätverks- och informationssystem skyddas. Det kan leda till gränsdragningsproblem i förhållande till krav på andra säkerhetsåtgärder som verksamhetsutövaren behöver vidta.

5.4 Undantag för sektorsspecifika rättsakter och andra författningar

För att uppnå en god informations- och cybersäkerhet i samhället anser länsstyrelsen att reglerna behöver vara enkla och lättillgängliga. Det innebär att länsstyrelsen gärna hade sett en reglering som inte innehåller omfattande undantag och som inte heller är subsidiär.

Om det ska vara en subsidiär författning behöver det framgå tydligt vilka rättsregler som har företräde, för att göra lagen enkel att tillämpa och utöva tillsyn efter i syfte att uppnå en god informations- och cybersäkerhet.

Utredningens förslag om att göra cybersäkerhetslagen subsidiär vid krav på riskhanteringsåtgärder (säkerhetsåtgärder) eller incidentrapportering med motsvarande verkan bedöms till viss del kunna bidra till oklarheter om tillämpningsområdet. Det riskerar att göra lagen svår att tillämpa och att utöva tillsyn efter.

5.5.4 Undantag för offentliga verksamhetsutövare

Länsstyrelsen instämmer i det som Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen föreslagit om att hela den offentliga sektorn ska omfattas (vilket utredningen redovisar i avsnitt 5.2.11). Samtidigt har länsstyrelsen förståelse för att utredningens tidsram inte medgivit en djupare utredning i den frågan.

Det skulle underlätta tillämpningen, öka acceptansen och bidra till en höjning av informations- och cybersäkerheten i hela den offentliga sektorn om samtliga aktörer omfattades av lagens tillämpningsområde.

Länsstyrelsens uppfattning är därför att undantag inte bör göras för myndigheter som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet i hela eller delar av verksamheten eller brottsbekämpning, krävs god informations- och cybersäkerhet.

Däremot anser länsstyrelsen att det bör finnas ett undantag från kravet på att rapportera incidenter enligt den nya lagen, i de fall incidenten samtidigt ska rapporteras till Säkerhetspolisen enligt 2 kap. 4 § säkerhetsskyddsförordningen (2021:955).

Redan i dagsläget finns ett sådant undantag för statliga myndigheter att rapportera it-incidenter till MSB som idag är CSIRT-enhet i Sverige, om incidenten är sådan att den också ska rapporteras till Säkerhetspolisen enligt den nämnda bestämmelsen i säkerhetsskyddsförordningen.

Enligt länsstyrelsen bör man eftersträva att en verksamhetsutövares säkerhetsresurser utnyttjas effektivt. Det torde inte anses vara effektivt att en och samma incident ska rapporteras till flera olika instanser enligt respektive mottagares rutiner och formulär.

Om rapportering ska göras till flera aktörer måste utgångspunkten vara att rutiner och formulär eller motsvarande är identiska, så att rapporten bara behöver skrivas en gång.

5.5.5 Undantag för enskilda verksamhetsutövare

I enlighet med synpunkter lämnade på föreslagna undantag för offentlig verksamhet, är det länsstyrelsens uppfattning att undantag inte heller bör göras för enskilda verksamhetsutövare som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet.

Även för det fall en enskild verksamhetsutövare bedriver säkerhetskänslig verksamhet eller brottsbekämpning krävs god informations- och cybersäkerhet.

8.4.2 Tillsynsmyndigheter i Sverige

Länsstyrelsen avstyrker förslaget att utpekade länsstyrelser ska utöva tillsyn över resterande länsstyrelser. Länsstyrelserna är 21 självständiga myndigheter med samma grunduppdrag.

Länsstyrelserna har, på uppdrag av regeringen, ett långtgående samarbete med gemensam it-drift, gemensamma it-system och gemensamma strukturer för informationssäkerhet och utveckling. Förslaget skulle därför innebära uppenbar intressekonflikt där länsstyrelserna utövade tillsyn över sig själva.

Som jämförelse har lagstiftaren valt att i säkerhetsskydds-förordningen (2021:955) reglera att länsstyrelserna inte ska utföra tillsyn av varandra, trots att det förekommit som förslag i förarbeten gällande förändringar av säkerhetsskyddsförfattningen.[1]

[1] I betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) från Utredningen om vissa säkerhetsskyddsfrågor föreslogs att fyra länsstyrelser skulle få ansvar för tillsyn över de andra länsstyrelserna, men i säkerhetsskyddsförordningen (2021:955) valde man i stället att låta tillsynsansvaret för länsstyrelserna ligga kvar hos Säkerhetspolisen.

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 i Västra Götalands län som värdlänsstyrelse. Värdlänsstyrelsen 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 med Länsstyrelsen i Stockholms län som värdmyndighet.

All anskaffning och utveckling av informations- och kommunikationsteknik ska hanteras gemensamt inom länsstyrelserna med en gemensam förvaltningsmodell, som har Länsstyrelsen i Västmanlands län som värdlänsstyrelse.

Sammanfattningsvis innebär det att länsstyrelsernas informations- och cybersäkerhetsarbete har en långtgående integration varför tillsyn inte med lätthet kan göras av länsstyrelserna var för sig.

De gemensamma strukturerna har en så pass stor påverkan på cybersäkerheten att en korsvis tillsyn inom länsstyrelserna skulle orsaka intressekonflikter och riskera att myndigheternas oberoende ifrågasätts.

8.4.5 Föreskrifter

Länsstyrelsen avstyrker utredningens förslag om föreskriftsrätt för Myndigheten för samhällsskydd och beredskap, MSB.

Regeringens utredare har i delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning, del 1, Fö2024/00785 lagt fram förslag om att Försvarets radioanstalt, FRA, ska ta över CSIRT-funktionen i Sverige (se avsnitt 5.3.3 CSIRT-funktionen CERT-SE, s. 43 ff).

Den utredningen föreslår också att FRA ska bli cyberkrishanterings-myndighet i Sverige. I linje med dessa förslag, som länsstyrelsen instämmer i, borde det också vara FRA som får den föreskriftsrätt som den nu aktuella utredningen föreslår att MSB ska få. Även den nuvarande föreskriftsrätten om informationssäkerhet och it-

incidentrapportering för statliga myndigheter bör som en konsekvens flyttas över till FRA för att få det samlat.

För att göra det lätt att göra rätt bör FRA få i uppdrag att ta fram gemensamma och generella föreskrifter för alla sektorer. Dessa föreskrifter kan därefter kompletteras med sektorsspecifika föreskrifter i de delar som inte täcks in av de generella föreskrifterna. Detta förslag skiljer sig från utredningens förslag där tillsynsmyndigheterna, förutom länsstyrelserna, ges föreskriftsrätt inom sitt tillsynsområde.

10.2.2 CSIRT-enhet i Sverige

Länsstyrelsen avstyrker utredningens förslag om att MSB ska vara CSIRT-enhet i Sverige.

Länsstyrelsen anser i stället att CSIRT-funktionen vid MSB bör överföras till FRA i enlighet med det förslag och med den motivering som regeringens utredare lagt fram i delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning, del 1, Fö2024/00785 (se avsnitt 5.3.3 CSIRT-funktionen CERT-SE, s. 43 ff).

Det bör också utredas djupare om även övrigt ansvar för informationssäkerhet och cybersäkerhet som idag finns vid MSB bör överföras till FRA med hänsyn till effektivitet och kompetens.

10.3.2 Cyberkrishanteringsmyndighet i Sverige

I likhet med och av samma skäl som i föregående avsnitt avstyrker länsstyrelsen utredningens förslag om att MSB ska vara cyberkrishanteringsmyndighet i Sverige.

I stället bör FRA bli cyberkrishanteringsmyndighet i enlighet med de överväganden som framförts i delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning, del 1, Fö2024/00785 (se avsnitt 5.3.3 CSIRT-funktionen CERT-SE, s. 43 ff).

Allmänna synpunkter

Länsstyrelsens uppfattning är att den föreslagna regleringen, i motsats till utredningens intentioner, riskerar att öka regelbörda och administration.

Som verksamhetsutövare är det, enligt länsstyrelsens uppfattning, inte helt enkelt att förstå om den egna verksamheten omfattas av reglerna eller inte. Regelverket innehåller en inte obetydlig mängd undantag. Dessutom har i vissa fall andra rättsregler företräde framför de föreslagna bestämmelserna. Synpunkterna på dessa förslag har framförts ovan kopplat till avsnitt 5.4 och 5.5.

Sammantaget är det, enligt länsstyrelsens uppfattning, tveksamt om de föreslagna reglerna kommer att uppnå syftet att uppnå en hög cybersäkerhet.

De som medverkat i beslutet

Beslutet har fattats av landshövding Carin Jämtin med säkerhetsskyddschef Erik Landgraff som föredragande. I den slutliga handläggningen har också dataskyddssamordnare Charlott Parhammar medverkat.

Denna handling har godkänts digitalt och saknar därför namnunderskrifter.