Länsstyrelsen
Västerbotten

Remissvar Länsstyrelsen Västerbotten NIS2-direktivet. Nya regler om cybersäkerhet. (SOU 2024:18)

Länsstyrelsen Västerbotten lämnar här sina synpunkter på NIS 2-direktivet. Nya regler om cybersäkerhet.

Sammanfattning

Länsstyrelsen konstaterar att utredningen gjort en god insats utifrån den komplexitet som finns i uppgiften och de facto att det har skett under knappa tidsförhållanden.

Sammanfattningsvis vill Länsstyrelsen trycka på att det skulle underlätta tillämpningen och öka acceptansen för regelverket om samtliga aktörer omfattades av lagens tillämpningsområde (avsnitt 5.5.4). Där instämmer Länsstyrelsen med MSB och Säkerhetspolisens förslag (som redovisas i avsnitt 5.2.11) att hela den offentliga sektorn, utan undantag, borde ha omfattats av lagen. Kraven kan, precis som säkerhetspolisen anfört, differentieras enligt de behov som finns.

Angående tillsyn 8.4.2 ser länsstyrelsen det som problematiskt att utpekade länsstyrelser ska utöva tillsyn mot varandra och över resterande länsstyrelser. Länsstyrelserna har gemensam IT-drift och gemensamma strukturer för informationssäkerhet och utveckling. Förslaget skulle därför innebära att länsstyrelserna utövade tillsyn över sig själva. Länsstyrelsen avstyrker förslaget.

Länsstyrelsen Västerbottens kommentarer

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 länsstyrelsens bytas ut mot det vedertagna begreppet ”säkerhetsåtgärder”.

5.2.2 Verksamhetsutövare

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

Länsstyrelsen delar utredningens bedömning att hela verksamheten bör omfattas av lagens tillämpningsområde. Ett informationssystem verkar inte i ett vacuum utan har kopplingar och beröringspunkter med verksamheten i stort. Ett fullgott informationssäkerhetsarbete bygger på att hela verksamheten integreras. Samtidigt föreslås att riskhanteringsåtgärderna ska vidtas i syfte att skydda nätverks- och informationssystem. 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 cybersäkerhet i samhället anser Länsstyrelsens 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 subsidiär behöver det framgå tydligt vilka rättsregler som har företräde. Allt för att göra lagen enkel att tillämpa och utöva tillsyn över med syfte att uppnå en god cybersäkerhet. Utredningens förslag om att göra cybersäkerhetslagen subsidiär vid krav på riskhanteringsåtgärder eller incidentrapportering med motsvarande verkan bedöms bidra till oklarheter om tillämpningsområdet. Det riskerar att göra lagen både svår att tillämpa och utöva tillsyn efter.

5.5.4 Undantag för offentliga verksamhetsutövare

Länsstyrelsen instämmer med MSB och Säkerhetspolisens förslag (som redovisas i avsnitt 5.2.11) att hela den offentliga sektorn, utan undantag, borde ha omfattats av lagen. Länsstyrelsen anser vidare att det skulle underlätta tillämpningen och öka acceptansen för regelverket 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 eller brottsbekämpning krävs god cybersäkerhet.

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 bör göras för enskilda verksamhetsutövare som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet eller brottsbekämpning krävs god cybersäkerhet.

8.4.2 Tillsynsmyndigheter i Sverige

Länsstyrelsen avstyrker förslaget att utpekade länsstyrelser ska utöva tillsyn över resterande länsstyrelser. Länsstyrelserna har gemensam IT-drift och gemensamma strukturer för informationssäkerhet och utveckling. Förslaget skulle därför innebära att länsstyrelserna utövade tillsyn över sig självt.

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 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, Safir, med Länsstyrelsen Stockholm som värdmyndighet. All anskaffning och utveckling av it hanteras gemensamt på länsstyrelserna med en gemensam förvaltningsmodell som har länsstyrelsen Västmanland som värdlänsstyrelse. 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 cybersäkerheten att en korsvis tillsyn inom länsstyrelserna skulle orsaka intressekonflikter och riskera att myndigheternas oberoende ifrågasätts.

8.4.5 Föreskrifter

För att göra det lätt att göra rätt anser länsstyrelsen att MSB bör 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.

Allmänna synpunkter

Länsstyrelsens uppfattning är att NIS2 ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. Direktivet ställer även ökade krav på ledningens deltagande i organisationens cybersäkerhetsarbete vilket är i grunden positivt och blir i jämförelse likt arbetet med säkerhetsskydd och den implementeringen vid de olika verksamhetsutövarna.

I tjänsten//

Magnus Hansson
Beredskapsdirektör
Länsstyrelsen Västerbotten