Regeringskansliet
Försvarsdepartementet

Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem

Er beteckning: Fö2021/00796
Länsstyrelsen i Skåne län yttrar sig över Cybersäkerhetsutredningens slutbetänkande ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63). Remissyttrandet har tagits fram i samverkan med Länsstyrelsen i Stockholms län, Länsstyrelsen Västra Götalands län, Länsstyrelsen i Västmanlands län samt Länsstyrelsen i Norrbottens län.

Sammanfattning

Länsstyrelsen delar utredningens uppfattning att det finns ett behov av att öka säkerheten i nätverks- och informationssystem.
Länsstyrelsen tillstyrker förslagen som presenteras av utredningen. Länsstyrelsen lämnar därutöver synpunkter på några av bedömningarna.

Länsstyrelsens utgångspunkt

Länsstyrelsen är den samordnande och sammanhållande aktören i kris och höjd beredskap. Länsstyrelsen ska bland annat säkerställa att egna informationshanteringssystem uppfyller grundläggande och särskilda säkerhetskrav så att myndighetens verksamhet kan utföras på ett tillfredsställande sätt[1]. Som högsta civila totalförsvarsmyndighet är delar av verksamheten säkerhetskänslig och omfattas av kraven på säkerhetsskydd. Från 1 december 2021 har vissa länsstyrelser ett utökat uppdrag att bedriva tillsyn över kommuner, regioner samt statliga myndigheter och enskilda verksamhetsutövare om de inte hör till någon annan tillsynsmyndighets tillsynsområde.
Länsstyrelserna har sedan 15 år tillbaka en gemensam IT-verksamhet. Länsstyrelsernas IT-avdelning är organiserad under Länsstyrelsen i Västra Götalands län. Länsstyrelsernas IT-avdelning har dessutom tilldelats ansvaret för länsstyrelsernas IT-säkerhet genom en överenskommelse beslutad av samtliga landshövdingar 2018.

[1] Krav i Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Remissvaret är därför formulerat ur perspektivet att Länsstyrelsen i Västra Götalands län tillhandahåller IT-drift åt övriga länsstyrelser, har en roll som tillsynsmyndighet för säkerhetskänslig verksamhet samt har en central roll i länet vad gäller civilt försvar.

Kapitel 11 Åtgärder för stärkt säkerhet i nätverks- och informationssystem

11.2 Begreppet informationssystem

Länsstyrelsen håller med utredningen om betydelsen av enhetlig terminologi där begreppen informationssystem och nätverks- och informationssystem används parallellt idag. I utredningens förslag på översyn av terminologi saknar Länsstyrelsen enhetliga definitioner av termerna. Enhetliga definitioner är generellt en förutsättning för att bedriva samverkan och uppnå samsyn mellan aktörer och nivåer. Det ökar också förutsättningarna för en enhetlig regelefterlevnad på området.
Ett exempel på när behovet är aktuellt inom definitioner kopplat till begreppet informationssäkerhet i relation till MSBFS 2020:6 och ISO 27000-området jämfört med säkerhetsskyddslagstiftningens. I den senare definieras informationssäkerhet som en av tre säkerhetsskyddsåtgärder tillsammans med fysisk säkerhet och personalsäkerhet. Inom ISO 27000-området definieras fysisk säkerhet och personalsäkerhet som delmängder av informationssäkerheten.
Säkerhetsskyddsområdet i sig kan dessutom vägas in som en del av informationssäkerheten enligt ISO 27000, där den högsta nivån av informationsklassningens medför normerande skyddsåtgärder utifrån säkerhetsskyddsområdets krav. Olika tolkningar av definitioner kan exempelvis innebära skillnader i hur olika aktörer organiserar sig eller implementerar skyddsnivåer.

11.4 Flera olika åtgärder krävs för att öka säkerheten i informationssystem i säkerhetskänslig verksamhet

Länsstyrelsen instämmer i utredningens bedömning av behovet av ytterligare åtgärder som ger bättre förutsättningar för offentliga och enskilda aktörer att stärka informations- och cybersäkerheten i säkerhetskänslig verksamhet genom systematiskt informationssäkerhetsarbete. Länsstyrelsen vill dock understryka vikten av att bredda perspektivet. Utredningen visar återkommande på att frågan om stärkt säkerhet berör brett och inte nödvändigtvis kan avgränsas till endast säkerhetskänslig verksamhet eftersom sådan befinner sig i en vidare kontext som inte fullt kan separeras från varandra. Verksamheten kan påverkas negativt i stor omfattning även vid brister i delar som inte träffas av krav på säkerhetsskydd. Det är därför viktigt att

även stärka informations- och cybersäkerheten på angränsande områden som inte direkt omfattas av säkerhetsskydd.

Kapitel 12 Certifiering av nätverks- och informationssystem

Länsstyrelsen tillstyrker förslaget att ge Försvarets materielverk (FMV) i uppdrag att i samråd analysera och ta fram förslag för bland annat formerna för en nationell kravställning som grund för evaluering och/eller certifiering av IKT-produkter, -tjänster och processer i nätverks- och informationssystem i säkerhetskänslig verksamhet. För den enskilde verksamhetsutövaren är nationell samordning på detta område av stor vikt.
Länsstyrelsen noterar dock att utredningen på sidan 375 anger att samrådet bland annat ska ske med tillsynsmyndigheter på säkerhetsskyddsområdet och på sidan 425 anger att samrådet ska ske med de myndigheter som har tillsynsansvar för åtgärder för en hög gemensam nivå av säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). Eftersom det inte är samma myndigheter som träffas av de här olika begreppen, behöver detta förtydligas vid ett eventuellt uppdrag till berörda myndigheter.

12.5 Överväganden

Länsstyrelsen instämmer i utredningens slutsats att certifiering ensamt inte är en tillräcklig säkerhetsåtgärd för att öka säkerheten i nätverks- och informationssystem. Tillräcklig säkerhet för nätverks- och informationssystem i säkerhetskänslig verksamhet förutsätter ett i övrigt väl utvecklat och integrerat systematiskt informationssäkerhetsarbete. Certifiering avser ett system och inte hela hanteringen Utifrån detta resonemang är det tydligt att certifiering endast är en delmängd av nödvändiga åtgärder.

12.5.2 Förutsättningar för en nationell certifieringsordning för säkerhetskänslig verksamhet

För att ytterligare öka graden av certifiering delar Länsstyrelsen utredningens bedömning att ett lämpligt nästa steg är att inkludera krav på certifiering i föreskrifter utifrån befintlig lagstiftning. En förutsättning för att en ordning som bygger på frivillighet ska få avsedd verkan, är att styrningen inkluderar en formell beslutspunkt som initierar krav på att en produkt ska certifieras. Införande av krav på certifiering skulle förhoppningsvis även innebära incitament för privata aktörer att sträva mot att certifiera nätverks- och informationssystem. Detta genom att de ges en bättre garant för att deras investeringar skapar bättre affärsmöjligheter.

Kapitel 13 Krav på godkännande och utvidgat samrådsförfarande för informationssystem

Länsstyrelsen tillstyrker utredningens förslag med inriktning på utökad samrådsskyldighet och introducering av lämplighetsprövning genom att flytta bestämmelser från säkerhetsskyddsförordningen till säkerhetsskyddslagen. Det blir ett förtydligande genom att lagen gäller allmänt mot samtliga verksamheter. Samrådsmyndigheterna har i sammanhanget en viktig roll i att stärka säkerheten i och med sin kompetens i dessa frågor.

Länsstyrelsen vill även betona vikten av att redan driftsatta informationssystem inte glöms bort i sammanhanget. Något som utredningen delvis berör i sista stycket på sidan 431. Förändrad informationshantering, förnyade säkerhetsskyddsanalyser och bedömningar av befintliga informationssystem et cetera. kan i vissa fall leda till nyuppkomna behov av att vidta säkerhetsskyddsåtgärder för informationssystem som tidigare inte bedömts ha innefattats av säkerhetsskyddet.

Kapitel 14 Tillgång till informationssystem vid tillsyn

14.2 Det finns skäl att införa ytterligare en undersökningsbefogenhet

Förslaget väcker frågor om kompetensen hos tillsynsmyndigheter är tillräckligt hög för att motivera utvidgad tillgång till informationssystem vid tillsyn. Det finns anledning att titta närmare på om tillämpning av detta utrymme förutsätter ökad kompetens hos den som utövar tillsyn dels för att inte riskera negativa konsekvenser som får påverkan på säkerheten i systemet, dels för att kunna genomföra de moment som avses.

Befintlig ordning med möjlighet att begära stöd från Säkerhetspolisen (Säpo) bedöms tillräckligt för att genomföra tillsyn. Det är därmed av vikt att Säpo tilldelas tillräckliga resurser för att ge stöd vid tillsyn inom rimlig tid.

Allmänna synpunkter

Länsstyrelsen ser viss otydlighet och möjlighet till överlappande uppdrag eftersom vissa uppgifter som att ta fram hotbild är fördelat på flera aktörer. Antagonistiska cyberhot föreslås förebyggas, upptäckas och hanteras inom ramen för samverkan i Cybersäkerhetscentret. Samtidigt föreslår utredningen att FMV ska få en utökad roll, inkluderat samverkan, på samma område. Säpo och Försvarsmakten har vidare redan uppdraget att ta fram generella hotbilder. Om ingen myndighet har ansvaret att ta fram en sammanhållen hotbild måste varje enskild myndighet få underrättelseinformation för att själva kunna ta fram den sammanhållna hotbilden för sin verksamhet. Ett ansvar fördelat på många aktörer kan innebära risk för att frågor förlorar fokus.

Länsstyrelserna framhåller avslutningsvis att det generellt är viktigt att titta på kompetensbehovet. På vissa håll finns det redan idag svårigheter med att rekrytera rätt kompetens. Den problematiken riskerar att öka om frågorna sprids ut på flera aktörer.

De som medverkat i beslutet

Beslutet har fattats av landshövding Anneli Hulthén med säkerhetssamordnare Riyadh Muhammed som föredragande.

Denna handling har godkänts digitalt och saknar därför namnunderskrift.

Så här hanterar Länsstyrelsen personuppgifter

Information om hur vi hanterar dessa finns på www.lansstyrelsen.se/dataskydd.