Länsstyrelsen
Västmanlands län

Datum
2025-01-07

Diarienummer
5681-2024

Regeringskansliet
Försvarsdepartementet

Yttrande över SOU 2024:64 Motståndskraft i samhällsviktiga tjänster

Er beteckning: Fö2024/01550

Sammanfattning

Länsstyrelsen i Västmanlands län (nedan Länsstyrelsen) har följande synpunkter på utredningens bedömningar och förslag.

5.3.3 Undantag för åtgärder enligt andra regelverk med motsvarande verkan

Länsstyrelsen delar utredningens förslag och ser det som viktigt att regeringen ges möjlighet att i föreskrifter ange vilka bestämmelser om riskbedömning, åtgärder för motståndskraft, bakgrunds-kontroller och incidentrapportering som har motsvarande verkan. Ju tydligare det kan anges desto bättre så att det inte lämnas öppet för olika bedömningar.

5.3.4 Undantag för brottsbekämpning och Sveriges säkerhet

Precis som i länsstyrelsens tidigare remissyttrande avseende nya regler om cybersäkerhet så är Länsstyrelsens mening att hela den offentliga sektorn, utan undantag, borde ha omfattats av denna lag.

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 motståndskraft.

Föreslagna undantag för uppgiftsskyldigheter rörande uppgifter som omfattas av säkerhetsskyddslagen samt tillsynsmyndigheters begränsade undersökningsbefogenheter för sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet bedrivs, kan ses som tillräckligt kompenserande kontroller för att motverka att säkerhetskänslig verksamhet äventyras.

6.2.1 Begreppen samhällsviktig tjänst kontra samhällsviktig verksamhet

Länsstyrelsen delar utredningens beskrivning av utmaningarna med likheterna och olikheterna mellan begreppen samhällsviktig tjänst kontra samhällsviktig verksamhet och de otydligheter som detta skapar.

Länsstyrelsen instämmer med utredningens bedömning av att det stora värdet av att i framtiden se över direktivens koppling till det svenska beredskapssystemet och möjligheten till att ensa såväl begrepp som sektorer som träffas av olika regelverk.

8.2 Åtgärder för motståndskraft

Länsstyrelsen ser det som olyckligt att begreppen *tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft* används.

Länsstyrelsen ser en stor risk för att detta skapar en begreppsförvirring jämfört med andra områden där tekniska och organisatoriska åtgärder utgör delmängder av säkerhetsåtgärder. Det gäller exempelvis begrepp inom standardfamiljen ISO 27000:s definitioner kopplat till informationssäkerhet och dess tillhörande säkerhetsåtgärder inom ISO 27001 och 27002. Det vill säga att säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det organisatoriska, personrelaterade, tekniska och fysiska säkerhetsområdet. Definitioner som används inom både privat och offentlig sektor sedan lång tid.

Ett tydligare ensande av begreppen hade varit att föredra, men det kan troligtvis hanteras genom ytterligare förtydliganden av innebörder i framtida föreskrifter från tillsynsmyndigheterna.

Utredningen menar att det inte är möjligt att i lag föreskriva att standarder ska beaktas, men att använda ensade begrepp vore ett led i att följa direktivets artikel 16:s innebörd om att ”*medlemsstaterna ska, när det är användbart och utan att föreskriva eller gynna användningen av viss teknik, uppmuntra användningen av europeiska och internationellt erkända standarder*”.

8.3 Incidentrapportering

Kritiska verksamhetsutövare ska utan onödigt dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandhållandet av samhällsviktiga tjänster.

För att klargöra begreppet ”*kan medföra*” konstaterar utredningen att ”*det krävs att incidenten potentiellt kan medföra en störning i den samhällsviktiga tjänsten, dvs. det måste finnas viss sannolikhet för att en störning kan inträffa*”.

Länsstyrelsen ser det som viktigt att begreppet ”*kan medföra*” förtydligas så långt det är möjligt i framtida föreskrifter. Bland annat kopplat till aspekter på sannolikhet för att undvika skillnader i tolkning bland tillsynsmyndigheter och verksamhetsutövare.

9 Bakgrundskontroll

9.3.1 Utgångspunkter för utredningens förslag

Länsstyrelsen hade gärna sett en bedömning i utredningen beträffande personer som är inplacerade i säkerhetsklass och lyder under pågående säkerhetsprövning enligt säkerhetsskyddslagen.

Specifikt rörande de fall där dessa individers kontrollorsaker i vissa fall, till delar, skulle kunna likna de kriterier som definieras för befattningsanalysen enligt förslaget till lag och förordning om motståndskraft hos kritiska verksamhetsutövare. Det vill säga hur verksamhetsutövarna ska beakta och hantera detta ur ett bland annat ett integritetsperspektiv utifrån överlappande kontroller.

9.3.3 Befattningsanalys utgör grunden för vilka som ska bakgrundskontrolleras

Bakgrundskontroll ska endast göras för befattningar som kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Utredningen konstaterar i kapitel 9.3.3 att det begrepp som ska användas är ”*ringa skada*” och att det ”*ansluter till etablerad begreppsanvändning inom svensk rätt*”. Länsstyrelsen förordar dock att begreppet förtydligas och exemplifieras ytterligare i framtida föreskrifter.

10.3 Tillsynsmyndigheter i Sverige

10.3.7 Offentlig förvaltning

Som framgår av utredningen så avstyrkte länsstyrelserna i tidigare remissyttrande avseende nya regler om cybersäkerhet (NIS2), att utpekade länsstyrelser ska utöva tillsyn över resterande länsstyrelser. Detta med motiveringen att länsstyrelserna har gemensam it-drift och gemensamma strukturer för informationssäkerhet, utveckling och verksamhetsprocesser. Förslaget skulle därför innebära att länsstyrelserna utövade tillsyn över sig självt.

Exempelvis har regeringen genom regleringsbrev beslutat 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 dessutom en gemensam förvaltningsorganisation av verksamhetsområden som inkluderar gemensamma arbetsutskott, nätverk, processer, rutiner, projekt, resurser och system. Gemensamt arbete bedrivs dessutom inom respektive civilförsvarsområde.

Jämfört med NIS2-direktivet är utredningens bedömning att ”*det inte föreligger samma problematik när det gäller CER-direktivet men att det mest lämpliga är att det är samma tillsynsmyndigheter som ansvarar för sektorn offentlig förvaltning enligt CER-direktivet som enligt utredningens förslag om NIS2-direktivets genomförande. Utredningen föreslår därför att om regeringen beslutar att en annan myndighet ska vara tillsynsmyndighet över länsstyrelserna enligt*

lagen om cybersäkerhet så ska den myndigheten även vara tillsynsmyndighet enligt lagen om motståndskraft hos kritiska verksamhetsutövare.”

Länsstyrelsen delar inte utredningens bedömning att det inte föreligger samma problematik utifrån de gemensamma strukturer som beskrivs ovan. De gemensamma strukturerna har en så pass stor påverkan på området att en korsvis tillsyn inom länsstyrelserna skulle orsaka intressekonflikter och riskera att myndigheternas oberoende ifrågasätts.

De som medverkat i beslutet

I detta ärende där landshövding Johan Sterte beslutat har informationssäkerhetssamordnare Ulf Ranestedt varit föredragande. I den slutliga beredningen har även vikarierande länsråd Stefan Renlund och försvarsdirektör Tomas Borg medverkat.

Denna handling har godkänts digitalt och saknar därför namnunderskrift.