YTTRANDE

Datum 2021-12-17
Ärendenummer 2021-POL000445

Yttrande. Remiss. Cybersäkerhetsutredningens slutbetänkande Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021_63)

Region Skånes remissyttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Region Skåne har granskat betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63), mot bakgrund av den verksamhet som bedrivs av myndigheten som helhet.

Region Skåne lämnar följande synpunkter som följer utredningens rubriksättning i de fall regionen har något att anföra.

Kapitel 11. Åtgärder för stärkt säkerhet i nätverks- och informationssystem

Region Skåne instämmer i den analys som utredningen redovisar angående generella brister i informations- och cybersäkerheten, såväl nationellt som internationellt. Region Skåne instämmer också i att en nationell styrning och samordning av en gemensam hot-, sårbarhets- och riskbedömning är nödvändigt för att kunna uppnå en ökad kvalitet i arbetet med informations- och cybersäkerhet hos verksamhetsutövare.

Utredningen föreslår att Försvarets materielverk (FMV) ska ges i uppdrag att i samråd och samverkan med andra myndigheter och aktörer ta fram formerna för arbetet med en nationell gemensam hot-, sårbarhets- och riskbedömning. Region Skåne vill lyfta fram vikten av att arbetet samordnas med befintliga krav på risk- och sårbarhetsanalys enligt exempelvis LEH. Detta för att uppnå synergieffekter och undvika ineffektiv resursanvändning på regional så väl som nationell nivå.

Besöksadress: Rådhus Skåne, Västra Storgatan 12
Postadress: Region Skåne 291 89 Kristianstad
Telefon (växel): 044-309 30 00
E-post: region@skane.se
Internet: www.skane.se
Organisationsnummer: 23 21 00-0255

Kapitel 12. Certifiering av nätverks- och informationssystem

Region Skåne instämmer i utredningens förslag om att FMV anses bäst lämpad myndighet såsom framtida certifieringsorgan för de IKT- produkter, tjänster och -processer vilka är tilltänkta att användas för säkerhetskänslig verksamhet.

Kapitel 13. Krav på godkännande och utvidgat samrådsförfarande för informationssystem

Region Skåne saknar en konkretisering av vilka överväganden en lämplighetsprövning ska innehålla. Det behöver enligt Region Skåne vara tydligt för verksamhetsutövaren hur bedömningar ska genomföras och mot vilka bedömningsgrunder. Förutsägbarhet avseende vilka krav som ställs på verksamhetsutövarens bedömningar är nödvändigt för att verksamhetsutövaren ska kunna utarbeta rutiner och arbetssätt som säkerställer regelefterlevnad.

Kapitel 14. Tillgång till informationssystem vid tillsyn

Region Skåne värnar om att säkerhetsskyddsklassificerade uppgifter inte görs tillgängliga i högre utsträckning än vad som är nödvändigt för att bedriva verksamhet och ifrågasätter därför behovet av tillsynsmyndighetens tillgång till informationssystem vid tillsyn.

Region Skåne ställer sig frågande till om det är nödvändigt att tillsynsmyndigheten ges befogenheter att genomföra säkerhetstester på verksamhetsutövarens informationssystem och föreslår istället att verksamhetsutövaren åläggs att visa~~r~~ upp resultat av egeninitierade säkerhetstester.

Tillgång till informationssystem med anledning av tillsyn kan medföra exponering för person- och/eller patientuppgifter. Eventuell tillsyn~~en~~ behöver därför ske under reglerade former som inte innebär att verksamhetsutövaren riskerar att inte uppfylla övriga krav på informationshantering som följer av exempelvis europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), patientdatalagen (2008:355) och offentlighet- och sekretesslagen (2009:400).

I det fall det ändå bedöms motiverat att ge tillsynsmyndigheten tillgång till informationssystem anser Region Skåne att det bör framgå på ett tydligt sätt hur tillsynsmyndighetens tillgång ska och får hanteras praktiskt, exempelvis vad gäller säkerhetsskyddsavtal, säkerhetsprövning och behörighetshantering.

Kapitel 16. Offentlighet och sekretess

Region Skåne saknar en beskrivning av hur ett utlämnande av information med anledning av tillsyn ska genomföras i det fall tillsynsmyndigheten har rätt att bereda sig tillgång till informationssystem på ett sätt som innebär att tillsynsmyndigheten ges *direktåtkomst* till informationssystem, exempelvis vid genomförande av säkerhetstester. Verksamhetsutövaren har vid åtkomst genom direktåtkomst inte möjlighet att på förhand kontrollera vilken information personal hos tillsynsmyndigheten tar del av och kan därmed inte genomföra en sekretessprövning.

Övriga synpunkter

Region Skåne vill lyfta fram vikten av att underlätta arbetet med hantering av kravställning vid införandet av informationssystem genom nationell samordning av kravhantering. Det stöd som föreligger idag är otillräckligt och lämnar alltför stora tolkningsmöjligheter vilket komplicerar för både verksamhetsutövare och leverantör.