Mottagarens referens: Fö2024/00496
Regeringskansliet
Försvarsdepartementet
fo.remissvar@regeringskansliet.se
Kopia till: visnja.raguz@regeringskansliet.se

Remissvar över betänkande "Nya regler om cybersäkerhet" (SOU 2024:18)

Statens veterinärmedicinska anstalt (SVA) har anmodats att inkomma med synpunkter på ovan rubricerade remiss och önskar framföra följande.

Sammanfattning

SVA är en beredskapsmyndighet där delar av vår verksamhet omfattas av säkerhetsskydd. Enligt betänkandets förslag skulle reglering och tillsyn skilja mellan den verksamhet som omfattas av säkerhetsskydd och övrig verksamhet. Utifrån ett totalförsvarsperspektiv sker dessutom styrning inom liknande frågor genom beredskapssektorn. Sammantaget kan detta uppfattas som onödigt uppdelat och eventuellt ge upphov till överlappande arbete och oklart ansvar. SVA förordar ett mer integrerat upplägg när det gäller riskbedömningar, incidentrapporteringar och tillsyn då det annars kan resultera i omfattande dubbelarbete för verksamhetsutövarna.

Vidare vill SVA understryka vikten av ett fullgott sekretesskydd för anmälningar och incidentrapporter, för att inte dessa ska riskera att behöva lämnas ut som allmän handling och därmed avslöja sårbarheter eller effekter av genomförda cyberattacker.

Specifika synpunkter

Cyber- och informationssäkerhetsarbetet på en myndighet utformas utifrån verksamhetens behov, men också utifrån yttre krav. Då SVA är en utpekad beredskapsmyndighet åläggs myndigheten även att göra risk- och sårbarhetsanalyser och riskbedömningar inom cyber- och informationssäkerhetsarbetet. I betänkandet framgår även olika perspektiv på hur tillsynsansvaret fördelas. Det finns i betänkandet två olika perspektiv, ett geografiskt och ett sektorsbaserat enligt NIS2-

direktivet. Till det ska läggas att det finns tillsynsansvar fördelat avseende beredskapssektorerna. I SVA:s fall kan det innebära att SVA tillsynas av Länsstyrelsen i Stockholms län, Länsstyrelsen i Örebro län, Läkemedelsverket, Livsmedelsverket och möjligen Myndigheten för samhällsskydd och beredskap (MSB). Det finns inte en tydlig ledning hur detta tillsynsansvar ska fördelas. I det fall respektive tillsynsmyndighet upprättar specifika föreskrifter finns även risk att dessa innebär motsatsförhållande till varandra. SVA förordar att exempelvis MSB upprättar en förteckning gällande vilken myndighet som har tillsynsmandat över respektive verksamhetsutövare avseende NIS2-regleringen och att man undviker att flera tillsynar en och samma myndighet.

SVA upplever att gränsdragningen mellan verksamhet som berör Sveriges säkerhet och de verksamhetsområden som berörs av betänkandet är oklar. När det gäller verksamhet som är säkerhetskänslig är verksamhetsutövaren skyldig att i sin säkerhetsskyddsanalys identifiera sådan verksamhet. När det inte finns en tydlig definition hur en gränsdragning ska göras mellan den säkerhetskänsliga verksamheten och verksamhet som berörs av betänkandet, finns en överlappning både vad gäller tillsyn, som görs av Säkerhetspolisen när det gäller säkerhetskänslig verksamhet till skillnad från verksamhet som berörs av betänkandet, och föreskrifter och riktlinjer för respektive område. Här finns således en konfliktsituation där en sektors tillsynsmyndighet inte är behörig att ta del av verksamheten inom sektorn alternativt en icke behörig organisation får tillgång till säkerhetskänsliga uppgifter samt viket regelverk som ska tillämpas för respektive verksamhet.

SVA:s uppfattning är att det behövs en central harmonisering av alla olika regleringar inom cybersäkerhetsområdet. Det finns i annat fall en risk för otydlighet som gör att målbilden blir svårare att uppnå. Om det tas fram olika detaljregleringar vad gäller cybersäkerhetsåtgärder kommer det att försvåra och fördyra för verksamhetsutövarna.

SVA anser att det finns otydligheter i betänkandet dels vad gäller system och metoder för incidentrapportering till tillsynsmyndigheterna, och dels vad gäller antalet rapporter som kan bli nödvändiga. SVA:s inställning är att incidentrapporter enbart ska skickas till MSB via ett sammanhållet säkert system som i sin tur förser de övriga berörda tillsynsmyndigheter med nödvändig information.

När det gäller incidentrapporter kan dessa dels innehålla känslig information om sårbarheter dels information om till exempel effekten av ett cyberangrepp. Det är uppgifter som kan underlätta nya cyberangrepp och ge en angripare information över effektiviteten i ett genomfört angrepp. Informationen i en incidentrapport är således känslig och det förslås att det införs en sekretessreglering vad gäller incidentrapporter som sänds mellan verksamhetsutövare och tillsynsmyndigheten.

SVA ställer sig även frågande till att en metod för att hitta sårbarheter i nätverk genom säkerhetsscanning kodifieras in i författningstexten. SVA:s uppfattning är cybersäkerhetsverktyg förändras över tid och inte ska beskrivas i en lagtext.