LÄKEMEDELSVERKET
SWEDISH MEDICAL PRODUCTS AGENCY

Yttrande

Maria Ingevaldsson
Stab Tillsyn

Datum: 2024-05-24
Dnr: 3.4.1-2024-022041
Skyddsnivå: (K0) Ingen/låg

Yttrande över remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Inledning

Läkemedelsverkets genomgång av de förslag som läggs fram i utredningen och de överväganden som görs har skett huvudsakligen utifrån Läkemedelsverkets uppdrag att verka för säkra och effektiva läkemedel av god kvalitet och för god läkemedelsanvändning samt för att medicintekniska produkter är säkra och lämpliga för sin användning.

Läkemedelsverket är positiva till förslaget om nya regler om cybersäkerhet. Myndigheten saknar i dagsläget uppbyggd kompetens för uppdraget som tillsynsmyndighet för detta område. En helt ny funktion kommer att behöva byggas upp men vi välkomnar förslaget och förtroendet.

Läkemedelsverket har, utifrån de aspekter som verket har att beakta, nedanstående synpunkter på utredningens förslag. Texten har disponerats i stycken med rubriksättning som motsvarar rubrikerna i utredningen för att det ska vara enkelt att se i vilka delar av utredningen Läkemedelsverket har synpunkter.

4.3 Hälso- och sjukvårdssektorn

I sektorn ingår sedan tidigare gruppen vårdgivare, över vilka Inspektionen för vård och omsorg (IVO) utövar tillsyn gällande cybersäkerheten. Enligt det nya regelverket tillkommer ytterligare områden där Läkemedelsverket föreslås vara tillsynsmyndighet. I området inkluderas verksamhetsutövare som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan.

Läkemedelsverket vill påtala att även verksamhetsutövare som tillverkar nationella medicinska informationssystem (NMI) bör ingå i detta område. NMI är sådana informationssystem som i sig själva inte är medicintekniska produkter men i sin avsedda användning ligger nära medicintekniska produkter. Eftersom NMI inte är medicintekniska produkter omfattas de inte direkt av EU:s medicinteknikförordning (EU) 2017/745 (MDR) men i och med att de bör omfattas av motsvarande krav på säkerhet och prestanda finns nationell lagstiftning i Sverige som omfattar NMI, se Läkemedelsverkets föreskrifter (HSLF-FS 2022:42) om nationella medicinska informationssystem.

NMI omfattar sådana informationssystem som hanterar data av betydelse för individens hälsa, och är utifrån sin definition stora system som omfattar individer på nationell, regional eller annan liknande nivå. Tillverkare är bland annat myndigheter, branschorganisationer, privata aktörer och vårdgivare. De är av sin natur i de flesta fall kritiska för den svenska hälso- och sjukvården och väsentliga delar i den digitala infrastrukturen. Exempel på sådana NMI är den Nationella Läkemedelslistan (NLL) samt flera andra system hos eHälsomyndigheten, den Nationella Patientöversikten hos Inera och expeditionssystem på

öppenvårdsapoteken. Då NMI kan anses vara kritiska vid ett hot mot folkhälsan bör de ingå i hälso- och sjukvårdssektorn och därmed omfattas av förslaget till lag om cybersäkerhet.

Läkemedelsverket har noterat att partihandlare omfattas av CER-direktivet men inte av NIS2-direktivet och ställer sig frågande till orsaken till att partihandlare inte också behöver omfattas av regler för säkerhet i nätverks- och informationssystem. Partihandlare och grossister som bedriver handel med läkemedel har en viktig roll för läkemedelsförsörjningen då de ansvarar för att läkemedel når ut till detaljhandeln.

4.13 Tillverkning - Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik

Utifrån formuleringen och de exempel på medicintekniska produkter som utredningen ger noterar Läkemedelsverket att det framstår som att utredningen, både i avsnittet om Tillverkning och i avsnittet om Hälso- och sjukvård, inte har uppmärksammat att programvara också omfattas av de medicintekniska regelverken. Detta gäller fristående programvara, programvara som del av annan medicinteknisk produkt och programvara som tillbehör till annan medicinteknisk produkt. Det omfattar både programvara som används inom hälso- och sjukvården och programvara som används av konsumenter (t ex hälsoappar med medicinska syften).

Uppgifter från MDCG (EU Medical Device Co-ordination Group) pekar på att var fjärde medicinteknisk produkt i dagsläget antingen är, eller innehåller, programvara. För fristående programvara gäller att de i flertalet fall levereras i form av tjänster som molntjänster, SaaS (Software as a Service) etc. Ofta är det tillverkaren som också levererar tjänsten, vilket innebär att tillverkaren troligen ingår både i sektorn Tillverkning och sektorn Digital infrastruktur.

Medicinteknisk programvara ingår också i många fall i större IT-system som involverar många aktörer och programvaror inom olika sektorer. Hälso- och sjukvården kan också tillverka programvaror, både som egentillverkning och som medicintekniska produkter.

Verksamhetsaktören har sannolikt ett integrerat system för cybersäkerhet, dvs ett system som hanterar kraven från flera tillämpliga regelverk där samma tillämpning uppfyller kraven i alla regelverken. Läkemedelsverkets tolkning av utredningens förslag är att varje myndighet ska avgränsa tillsynen till sin del av regelverket. Läkemedelsverkets uppfattning är att det inte är tydligt i förslaget hur detta ska tillämpas i praktiken. Det kan därför behöva utredas och analyseras vidare hur samverkan kan och bör gå till vid överlappning mellan myndigheternas ansvar samt om det kan finnas effektiviseringsmöjligheter.

Vidare bör det utredas hur konflikter mellan sektorsspecifika krav från olika tillsynsmyndigheter ska hanteras, liksom fall då tillsynsmyndigheterna gör olika bedömning.

Lämpliga mekanismer för hanteringen av överlappning, subsidiaritet vid regelverkskonflikter, samverkansmöjligheter etc enligt ovan bör, enligt Läkemedelsverkets mening, inkluderas i regelverket på en övergripande nivå. Vägledningar kan därefter tas fram för tillämpningen där så är lämpligt.

Läkemedelsverket ser det även som viktigt att utreda vidare hur en process kan se ut för att lägga till grupper av verksamhetsutövare som i nuläget faller utanför de olika sektorerna, men som ändå eventuellt bör inkluderas i regelverket. Detta gäller även för de fall det i framtiden dyker upp ett behov av att utöka tillämpningsområdet med ytterligare grupper av verksamhetsutövare.

6.2 Register över väsentliga och viktiga verksamhetsutövare

Vid tillsyn är det viktigt för tillsynsmyndigheten att ha en aktuell och korrekt bild av den verksamhetsutövare som ska tillsynas, och det är därför bra med krav på registrering för de olika verksamhetsutövarna. Det finns dock punkter som bör tas i beaktande av utredningen.

Kravet på att väsentliga och viktiga verksamhetsutövare ska registrera sig hos tillsynsmyndigheten kommer att leda till att vissa verksamhetsutövare behöver registrera sig hos flera olika myndigheter, och i vissa fall flera gånger hos samma myndighet då registreringskrav också återfinns i flera regelverk. Verksamhetsutövaren ska också kontinuerligt hålla informationen uppdaterad. Detta kan medföra ökad administration inte bara för verksamhetsutövaren utan också för tillsynsmyndigheterna. Sannolikheten ökar också för felaktigheter och diskrepanser mellan register, exempelvis om verksamhetsutövare och/eller produkt matas in med olika namn i olika register eller att verksamhetsutövaren inte uppdaterar uppgifter såsom byte av kontaktperson. Registreringen bör utformas på ett sätt som så långt möjligt undviker onödig dubbelregistrering och minimerar risken för fel.

Läkemedelsverket föreslår vidare att det tas fram ett Application Program Interface (API) för kontaktpunkten och tillsynsmyndigheterna vilket möjliggör att data överförs mellan olika programvaror på ett strukturerat, formaliserat sätt. Detta skulle kunna användas vid överföring av registerdata men även annan data som ska delas, exempelvis incidentrapporter mellan kontaktpunkten och tillsynsmyndigheterna. Det skulle möjliggöra kontinuerligt uppdaterad information samtidigt som det skulle minska mängden administration.

Många verksamhetsutövare kommer att behöva uppfylla flera olika sektors- och horisontella regelverk med krav på cybersäkerhet hos organisationen. Kraven är i många fall överlappande, men med olika myndigheter som har tillsyn utifrån olika regelverk eller aspekter av regelverk. Utan samordning finns risk att verksamhetsutövaren granskas flera gånger av olika myndigheter som i stort kontrollerar samma saker. Läkemedelsverket vill därför notera att det är av stor vikt att det finns en möjlighet för tillsynsmyndigheterna att få en helhetsbild över vilka regelverk som verksamhetsutövaren omfattas av, och vilka andra tillsynsmyndigheter som berörs, på ett sätt som möjliggör en effektiv myndighetssamverkan.

8.4.5 Föreskrifter

Läkemedelsverket instämmer med den bedömning som MSB gör i sitt remissvar (MSB 2024-03843-4, punkt 4) om att det är lämpligt med gemensamma grundföreskrifter som sedan får kompletteras av tillsynsmyndigheterna med eventuella sektorsspecifika krav. Det skulle underlätta både för tillsynsmyndigheter och verksamhetsutövare som ingår i flera sektorer. För det starkt växande området medicinteknisk mjukvara finns exempelvis redan idag flera

horisontella regelverk, både på EU- och nationell nivå som ställer cybersäkerhetskrav och där kraven i många fall överlappar varandra. Vid behov kan också sektorsspecifik/sektorsövergripande vägledningar tas fram som komplettering till grundföreskrifterna och sektorsspecifik reglering.

9.3 Vilka överträdelser kan läggas till grund för sanktioner?

Läkemedelsverket instämmer i utredningens föreslagna ingripandemöjligheter och anser att de kompletterar de föreslagna tillsynsåtgärderna på ett bra sätt. Läkemedelsverket vill dock framhålla att tillsynsmyndigheterna även bör ha möjlighet att ingripa om en verksamhetsutövare har åsidosatt sin skyldighet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete enligt 3 kap. 2 § förslaget om lag om cybersäkerhet. Myndigheten gör bedömningen att det systematiska och riskbaserade informationssäkerhetsarbetet utgör grunden för verksamhetsutövarens andra bedömningar gällande bland annat riskhanteringsåtgärder och utbildningsinsatser. Det är därför av vikt att det finns en möjlighet för tillsynsmyndigheterna att ingripa för det fall verksamhetsutövarna brister i bedrivandet av ett systematiskt och riskbaserat informationssäkerhetsarbete.

9.3.1 Tillsynsmyndigheten ska kunna avstå från att ingripa i särskilda fall

Enligt förslaget får tillsynsmyndigheten avstå från att ingripa om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen, och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga. Läkemedelsverket ställer sig frågande till hur detta praktiskt ska fungera och noterar att det finns ett behov för tillsynsmyndigheterna att kunna kommunicera över myndighetsgränserna om vidtagna åtgärder.

12.6.7. Utredningens förslag – ekonomiska konsekvenser för tillsynsmyndigheterna och för Myndigheten för Samhällsskydd och beredskap

Läkemedelsverket anser att myndigheten skulle behöva göra en utredning för att kartlägga vilka verksamheter som omfattas av reglerna för cybersäkerhet. Kartläggningen är viktig för att kunna uppskatta resursbehovet och behöver göras innan uppbyggnaden av verksamheten. Läkemedelsverket noterar att det i utredningen föreslagna anslaget på fem miljoner kronor som en initial kostnad är en halvering av den kostnad som myndigheten har uppskattat som en initial kostnad och som verket har lämnat i ett tidigare yttrande till denna utredning.

Detta yttrande har beslutats av ställföreträdande generaldirektören Joakim Brandberg efter föredragning av projektledaren Maria Ingevaldsson. I den slutliga handläggningen har även stabsdirektören Anette Nilsson, gruppchefen Camilla Bysell, verksjuristerna Ellen Nilsson och Isabelle Benfalk deltagit.

Joakim Brandberg

Maria Ingevaldsson

Detta beslut har hanterats digitalt och är därför inte undertecknat

Kopia till: registrator, Joakim Brandberg, Camilla Bysell