Dnr Fö2024/00496
2024-05-28
Försvarsdepartementet

Remissvar avseende delbetänkande SOU 2024:18 ”Nya regler om cybersäkerhet”

Swedish Medtech är en branschorganisation för över 200 medicintekniska företag i Sverige. Dessa företag erbjuder en mängd olika produkter, inklusive röntgen, ortopediska implantat, minimalinvasiv kirurgi, pacemakers, dialys, hjälpmedel för funktionshindrade, journalsystem och digitala lösningar. Flertalet lösningar och produkter är uppkopplade. Branschen anställer cirka 27 000 personer och exporterade medicinteknik för över 34 miljarder svenska kronor 2022. De flesta kunderna är offentliga enheter som kommuner och regioner, och många företag deltar i offentliga upphandlingar för att få ut sina produkter på marknaden. En stor del av forskning och utveckling sker i samarbete med hälso- och sjukvården, vilket har resulterat i nya produkter och innovativa behandlingsmetoder som förbättrar patienternas livskvalitet.

Remissvaret har tagits fram genom en ingående process tillsammans med Swedish Medtechs medlemmar. Sectras experter, Johan Åtting och Andreas Ehrlund har haft en särskild roll i att analysera delbetänkandet. I processen har advokat Filip Åhsberger vid Setterwalls advokatbyrå bidragit med en juridisk analys och synpunkter under hand. Underlaget har beretts i Swedish Medtechs grupp för Digital Hälsa. I den slutgiltiga beredningen har jurist Julia Öhman och sakkunnig digitalisering Jesper Olsson deltagit. Underlaget har beslutats av Anna Lefevre Skjöldebrand, VD Swedish Medtech.

BRANSCHORGANISATIONEN FÖR MEDICINTEKNIK

Telefon 08-586 246 00
info@swedishmedtech.se
www.swedishmedtech.se

Innovation • Patientsäkerhet • Hållbar vård och omsorg
Box 3601 103 59 Stockholm
Besök: Sveavägen 63, Stockholm

Remissvar SOU 2024:18 ”Nya regler om cybersäkerhet”

Den demografiska utvecklingen i Sverige gör att antalet personer över 80 år kommer öka drastiskt. Med det följer en ökad sjukdomsbörda samtidigt som antalet händer i vården kommer minska. En avgörande komponent för att lösa utmaningarna är att utveckla användningen av medicinteknik för att fortsätta leverera god och säker vård till hela befolkningen. I dagsläget blir är allt fler medicintekniska lösningar digitala och uppkopplade. Det handlar om allt från diagnostisk utrustning, behandling, övervakning i hemmet eller på sjukhuset till uppföljning, forskningsregister och journalföring. Nästan alla dessa medicintekniska lösningar är dessutom, på olika sätt, sammanflätade i vårdens ekosystem för informationsförsörjning och produktion.

Det aktuella globala läget och de växande hoten mot cybersäkerheten medför risker för patientsäkerheten och de samhällbärande strukturerna så som hälso- och sjukvården. Då medicinteknik är avgörande för vårdens funktion i vardag och i kris är av yttersta vikt att hälso- och sjukvården och branschen fortsätter att aktivt vidta åtgärder för att skydda kritiska verksamhetssystem och kritisk information mot hot och attacker. Den medicintekniska branschen välkomnar därför det övergripande syftet med att införliva NIS2-direktivet i en cybersäkerhetslag.

Att tillverkare av medicintekniska produkter och hälso- och sjukvården har robusta och adekvata cybersäkerhetsåtgärder på plats för att säkerställa verksamhetens kontinuitet är av största vikt.

Synpunkter på delbetänkandet

Swedish Medtech är i grunden är positiv till NIS2 men vi anser att det finns vissa oklarheter i delbetänkandets förslag till implementering. Övergripande synpunkter:

- Det organisatoriska upplägget med roller och ansvarsförhållanden riskerar bli svårt att genomföra i praktiken ur ett medicintekniskt perspektiv. Detta eftersom företag kan komma att stå under tillsyn av flera myndigheter. Det riskerar bli oklart vilken myndighet som bär ansvar liksom parallella tillsynsprocesser som driver kostnadsökningar. Att sprida arbetet på flera myndigheter riskerar att skapa en situation med kompetensbrist vad gäller förmågan att säkerställa genomförande och tillsyn av cybersäkerhetslagen.
- Offentlighetsprincipen kräver att det är mycket tydligt vilken data som är sekretessbelagt, annars finns en påtaglig risk att känsliga data kan komma att lämnas ut, något som kan innebära allvarlig skada för rikets säkerhet. Det är inte tydliggjort i utredningen i vilken mån känslig data kan sekretessbeläggas.
- Vi anser det felaktigt att en hel verksamhet ska omfattas av lagen i de fall delar av verksamheten klassificeras som väsentlig eller viktig verksamhetsutövare. Om verksamheten kan visa på en trovärdig lösning som isolerar den klassade verksamheten bör detta vara tillräckligt.
- Den korta genomförandetiden försvårar för verksamheterna att hinna förbereda och anpassa sig till de nya bestämmelserna i lagen. Detta försvårar möjligheterna till ett lyckat genomförande. För att motverka detta skulle genomförandetiden för beslutad nationell lagstiftning kunna förlängas för att möjliggöra för företagen såväl som tillsynsmyndigheter att göra de insatser som krävs för att kunna leva upp till de nya lagkraven.

BRANSCHORGANISATIONEN FÖR MEDICINTEKNIK

Telefon 08-586 246 00
info@swedishmedtech.se
www.swedishmedtech.se

Innovation • Patientsäkerhet • Hållbar vård och omsorg
Box 3601 103 59 Stockholm
Besök: Sveavägen 63, Stockholm

- Swedish Medtech noterar att det inte funnits representanter från näringslivet med i utredningens expertgrupp. Detta är olyckligt då det hade kunnat bidra med insikter kring industrins behov och lagstiftningens utmaningar och påverkan på företagens verksamhet.

I följande underlag förtydligar vi våra resonemang.

Stor variation i ländernas införlivanden av NIS2-direktivet driver kostnader och sänker genomförandehastigheten

De medicintekniska bolagen verkar många gånger på en internationell marknad, det vill säga både inom och utanför EU. NIS2-direktivet syftar till att skapa en harmoniserad nivå av cybersäkerhet inom EU. Även om direktivet sätter en gemensam ram för alla medlemsländer, kan implementeringen variera mellan länder. Swedish Medtech ser att den svenska implementeringen riskerar att bli resursdrivande och fördyrande för industrin om den skiljer sig åt i allt för hög grad mot andra medlemsländers implementering. Vi anser därför att det är bra om genomförandet av den svenska implementeringen så långt som möjligt är harmoniserad med andra EU länder och, åtminstone, med de nordiska länderna.

Att den medicintekniska branschen är internationell innebär även att svenska företag kan ha sin cybersäkerhetsexpertis utanför Sveriges gränser, antingen i ett EU land eller i tredje land. För att öka kostnadseffektiviteten i genomförandet och för att undvika fördyrande konsultkostnader är det eftersträvansvärt att den svenska lagstiftningen med tillhörande handledningar även får en officiell engelsk översättning så att företagens internationella expertis kan nyttjas effektivt.

Sekretess för inlämnade uppgifter och incidenter

Swedish Medtech ser positivt på delbetänkandets förslag avseende att stärka rapporteringsplikten och därmed det nationella lärandet från incidenter. Det är även positivt att rapporteringen ska ske till MSB. Däremot anser Swedish Medtech att företagens information behöver skyddas genom sekretess. Det är av vikt att information om vilka verksamhetsutövare som är samhällskritiska liksom deras IP-adresser skyddas i system som uppfyller en tillräcklig nivå av säkerhet. Detsamma måste gälla rapporterade sårbarheter. Sådana uppgifter behöver skyddas genom sekretess vid incidentrapportering för att inte hämma incidentrapporteringen eller möjliggöra planeringen av subversiv verksamhet mot nationen. En sammanställning över Sveriges alla samhällskritiska verksamheter och deras IP-adresser skulle vara en guldgruva för hotaktörer. Om denna information skulle vara offentligt tillgänglig, skulle det underminera hela syftet med NIS2 och cybersäkerhetslagen. Swedish Medtech anser att det behövs ett starkt och mer omfattande sekretesskydd för uppgifter som kan komma att behandlas enligt direktiven än det som följer av OSL idag. I frågor om skydd av känsliga uppgifter kopplat till myndighetsutövningen anser vi att utredningens ståndpunkter behöver förtydligas.

Risker med den föreslagna strukturen för tillsyn

Med fem nya tillsynsmyndigheter och 11 nya sektorer ser Swedish Medtech att det kan uppstå flera utmaningar. Ur ett medicintekniskt systemperspektiv sammanstrålar många av tillsynsaktörerna i hälso- och sjukvårdssektorn. För att exemplifiera komplexiteten; Ett forskande medicinskt tekniskt företag med hälso- och sjukvården som kund riskerar att på olika sätt beröras i proaktiv eller reaktiv

tillsyn kopplat till Läkemedelsverket, Inspektionen för vård och omsorg, Post- och telestyrelsen och Länsstyrelsen. Detta blir komplext, kostnadsdrivande och ökar riskerna att utfallet från tillsynen, bedömningen, av verksamheten, ger olika resultat. Det kan då bli oklart vilken tillsyn som ska vara gällande. Det är därför av stor vikt att myndigheterna driver ett aktivt arbete för att säkerställa tydlighet och ansvarsförhållanden liksom likvärdig tillsyn oavsett vilken myndighet som bär ansvaret.

Swedish Medtech hade gärna sett en konsekvensbeskrivning utifrån hälso- och sjukvården som en egen sektor med *en* tillsynsmyndighet. En myndighet med samlat ansvar för hela sektorn som ges möjlighet att ta expertstöd från andra sektorsmyndigheter i föreslagen struktur. En sådan lösning skulle minska komplexiteten för företag och vårdgivare, öka tydligheten i ansvar samt skapa förutsättningar för myndigheten att bygga upp erforderlig kompetens och rutiner för arbetsuppgiftens genomförande.

Risk för stor variation i grunderna för tillsynen

Problematiken förstärks i och med att varje tillsynsmyndighet ska ta fram sina egna föreskrifter och vägledningar på området. Här finns en stor risk att de medicintekniska leverantörerna utsätts för en stor variation i krav, från olika håll, på cybersäkerheten. En sådan utveckling skulle vara olycklig och kontraproduktiv. Swedish Medtech anser därför att utredningens förslag att MSB ska samordna och harmonisera vägledningar är mycket viktig och kräver en ändamålsenlig resurssättning. Annars ser vi en uppenbar risk för kompetensbrist och parallella rapporteringssystem

Risk för kompetensbrist och parallella rapporteringssystem

Vad gäller myndigheternas tillgång på kompetens, då särskilt Läkemedelsverket (som ska utöva tillsyn över den medicintekniska branschen) som ska bygga upp en ny verksamhet, så ser Swedish Medtech detta som en utmaning. En huvudanledning är att det nationellt saknas personer med kompetens inom cybersäkerhetsområdet. Nu riskerar tillgänglig kompetens att spridas över flera myndigheter vilket gör att kritisk massa för professionellt lärande inte uppnås. En lösning är att samla tillsynen till en myndighet, som man exempelvis gjort inom dataskydd där IMY är tillsynsenhet. Här utöver ser inte Swedish Medtech det som rimligt eller resurseffektivt att varje tillsynsmyndighet lägger resurser på att ta fram egna, olika, system för att hantera verksamhetsutövarnas anmälningar och känsliga uppgifter. Vi ser det som viktigt att regeringen följer den rekommendation som framgår av skäl 106 till NIS2 direktivet om att samverka nationellt i syfte att rationalisera administrationen och minska företagens uppgiftslämnarbörda i förhållande till annan författning.

Lagens omfattning bör begränsas

Förslaget att lagen ska tillämpas på hela verksamheten i de fall delar av verksamheten klassas som samhällskritisk av myndighet kan medföra betydande belastningar för organisationer där endast en liten del av verksamheten är samhällskritisk. Lagstiftningen bör därför inte föreskriva vilken lösning som är säker för enskilda bolag. Det ska vara upp till varje företag att identifiera bästa tänkbara lösning för att hantera situationen där endast en del av företaget är samhällskritiskt. det är sedan upp till tillsynsmyndigheten att verifiera om lösningen uppfyller kraven i lagen. Vårt förslag är därför att denna formulering stryks. Det ska räcka med att den samhällskritiska delen av verksamheten är säkrad mot störningar.

Utmaningar för små organisationer

Cybersäkerhetslagen kommer att bli en stor utmaning för flera organisationer, särskilt de som är mindre. Det handlar både om resurs- och kompetensbrist att investera i nödvändig cybersäkerhetsinfrastruktur.

Genom att erbjuda stöd och resurser kan myndigheter hjälpa småföretag att överkomma hinder och skapa förutsättningar för att de ska kunna uppfylla kraven i cybersäkerhetslagen på ett effektivt och hållbart sätt. Det kan exempelvis handla om framtagandet av vägledningar, utbildningar liksom myndighetsfunktioner som kan svara på frågor. Här behöver regeringen säkerställa resurser till utpekade myndigheter.

Kort implementeringstid

För verksamheterna är en av de största utmaningarna med de nya reglerna om cybersäkerhet den korta implementeringstiden. För att möjliggöra för verksamheterna att hinna förbereda och anpassa sig till de nya bestämmelserna i lagen skulle genomförandetiden för beslutad nationell lagstiftning behöva förlängas. Det är även nödvändigt att föreskrifter, riktlinjer och vägledningar utarbetas i god tid innan lagstiftningen träder i kraft och att utrullningen av lagstiftningens tillämpning synkroniseras med offentliggörandet av myndigheternas styrande och vägledande dokument.

Anna Lefevre Skjöldebrand

VD, Swedish Medtech
Stockholm 2024-05-28

Julia Öhman, Jurist

Jesper Olsson, Sakkunnig Digitalisering