Regeringskansliet

Försvarsdepartementet

103 33 Stockholm

Er ref Fö2024/00496

Vår ref RE2024007

Remiss av Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Drivkraft Sverige är branschorganisationen för bränsle-, smörjmedels, bitumen och drivmedels- och laddoperatörsbranschen. Våra medlemsföretag erbjuder hållbar mobilitet och ser till att det finns bränsle och drivmedel för hållbara resor och transporter samt bitumen till vägar i hela landet. Vi arbetar för att Sverige ska bli klimatneutralt till 2045.

Drivkraft Sverige har fått delbetänkandet Nya regler om cybersäkerhet på remiss och har följande att anföra.

Sammanfattning

Drivkraft Sverige välkomnar denna remiss, då cybersäkerhet är ett viktigt område. Området är även komplext och har stor påverkan på verksamheterna. Vi tycker således det är positivt att Europeiska unionen har ett tydligt och harmoniserat regelverk för medlemsstaterna. Då detta är en fråga som ej har några gränser och behöver således beaktas, likt CER-direktivet, som en unionsfråga.

Drivkraft Sveriges uppfattning är att den föreslagna cybersäkerhetslagen till stor del ligger nära NIS2-direktivet (2022/2555) om åtgärder för en hög gemensam cybersäkerhetsnivå inom hela EU. Vi konstaterar dock att intentionen med ett harmoniserat regelverk inom EU inte helt och hållet omhändertas.

Vi ser heller ingen tydlig konsekvensanalys mellan NIS2 och andra regleringar, detta behövs särskilt inom säkerhetsområdet, här skulle regeringens implementeringsråd

komma till nytta. Regelverket riskerar annars att bli alltför administrativt, vilket kan leda till att verksamheters förmåga att arbeta mer proaktivt reduceras. Det saknas även en tydlig konsekvensanalys för hur ett alltmer omfattande cybersäkerhetsarbetet påverkar verksamheter resursmässigt, ekonomiskt såväl som kompetensmässigt. Vi kan inte skapa ett system som påverkar Sveriges konkurrenskraft negativt, för har vi inte konkurrenskraftiga företag har vi ingen totalförsvarsförmåga.

Då NIS2 har en nära koppling till CER-direktivet så kommer vissa synpunkter ha bäring på även detta direktiv.

Initialt vill vi särskilt lyfta två punkter, harmonisering och samordning, då dessa fångar upp helheten samt är viktiga för att säkra en god implementering av det nya regelverket. Vi kommer även komma med några korta synpunkter för de specifika kapitlen.

Harmonisering

- De nationella lagarna bör inte överskrida den omfattning som definieras i NIS2-direktivet.
    - Detta är för att säkerställa att NIS2-krav är på en liknande nivå i olika medlemsländer, vilket möjliggör harmonisering av NIS2-implementering för internationella företag.
    - Om en viss entitet/enhet/verksamhet eller sektor anses vara nationellt kritisk är CER:s tilldelning av kritiska enheter en mer lämplig regleringsmekanism.

- Nationella tekniska NIS2-krav bör inte införas innan EU-kommissionens genomförande akt för NIS2 har presenterats.
    - Detta för att ha NIS2-krav på en liknande nivå i olika medlemsländer och därmed möjliggöra harmonisering av NIS2-implementering för internationella företag.
    - Om nationella krav tas fram bör de baseras på internationella standarder som ISO/IEC 27001 eller IEC 62443.

- Om det finns befintlig nationell reglering som inte är anpassad till NIS2- eller CER-kraven, bör de nationella kraven anpassas till NIS2 och CER.

- För internationella företag som är verksamma i flera medlemsstater och som omfattas av NIS2 och/eller CER är det viktigt att möjliggöra gränsöverskridande verksamhet och datadelning för att effektivt kunna genomföra cybersäkerhetsåtgärder och övervakning som krävs av NIS2. Lagförslaget fokuserar på verksamhetsutövares ansvar utan att beakta hur arbete bedrivs inom en koncern, där koncernbolag ofta delar gemensamma processer.

- En mekanism bör utvecklas som gör det möjligt för de bakgrundskontroller av personalresurser som krävs enligt CER-direktivets artikel 14 att antingen erkänna bakgrundskontroller som gjorts av en annan medlemsstat eller ge garanterad tillgång till nationella bakgrundskontroller för personal på kritiska entiteter som kontrollerats av en annan medlemsstat för liknande befattningar.

- Vikten av konsekvensanalyser för nya förslag från EU och överlappande lagstiftning inom digitalisering- och säkerhetsområdet. Detta för att undvika administrativa pålagor som inte leder till ökad cybersäkerhet. Den sammanlagda effekten kan snarare riskera att öka misstagen i regelefterlevnad i stället för att bidra till att stärka verksamhets förmågor att hantera cyberhot samt att stärka robustheten, resiliensen och redundansen i hela samhället. Detta vore förödande för konkurrenskraften och motståndskraften inom hela EU.

- Situationsmedvetenhet om cybersäkerhet kräver förmåga att kombinera datauppsättningar från alla medlemsstater där företaget är verksamt. Om nationella krav inte tillåter datadelning minskar effektiviteten i de cybersäkerhetskontroller som krävs enligt NIS2.

- Vi anser att läsbarheten och tydligheten i utredningens förslag gällande säkerhetsåtgärder (3kap §1) är rimlig, men då cybersäkerhetslagen i stort är mycket nära direktivet föreslår vi att även denna paragraf ska formuleras så nära direktivet som möjligt i syfte att underlätta harmonisering och jämförbarhet mellan medlemsländer. Det skulle bidra till att effektivisera säkerhetsarbetet bland annat genom att undvika onödig administration samt minskar risken för snedvriden konkurrens för bolag med verksamhet i flera länder. Om Sverige gör detta annorlunda går det emot syftet att NIS2 ska öka harmoniseringen mellan medlemsstaterna.

- Ta bort kravet på systematiskt informationssäkerhetsarbete, då detta krav inte följer av direktiven. Detta skulle öka likheten med implementationerna i andra länder och minska problematiken för verksamheter med flera tillsynsmyndigheter. Det skulle också minska framtida problematik vid eventuell ytterligare europeiska direktiv. Systematiskt arbete följer redan av det riskbaserade arbetssättet som direktivet kravställer.

- Säkerställ att tillämpning av begreppet ”hela verksamheten” blir tydligt samt att det avser leveranstjänsters kritiska delar inom hela verksamheteten.

Samordning

Med det utökade tillämpningsområdet för NIS2 kommer utredningens förslag att öka fragmenteringen av området ännu mer och resultera i ett flertal överlappande föreskrifter. Dels genom sektorsvisa krav på säkerhetsåtgärder, dels genom att det som tidigare varit gemensamt – kraven på riskbaserat informations- och cybersäkerhetsarbete – nu ska regleras separat för varje sektor. Till det kommer att varje tillsynsmyndighet inom sin sektor ska föreskriva om utbildning inom riskbaserat cybersäkerhetsarbete och reglera krav på hur verksamhetsutövarna ska genomföra utbildningen. Detta är särskilt tydligt då verksamheter och leverantörskedjor ej tagits med i konsekvensbedömningen rörande dess regleringar och överlappningar.

NIS2 och CER direktivet bör även betänka hur dessa relaterar till krisberedskap och totalförsvar samt hur identifierade samhällsviktiga verksamheter knyter an till de 10 beredskapssektorerna. Det är även av vikt att man säkrar tydliga flöden och avgränsningar inom de olika lagstiftningarna (inkl säkerhetsskyddslagstiftningen). Då detta annars kan skapa hinder rörande informationsdelning mellan totalförsvarsviktiga aktörer.

För att implementera detta regelverk krävs tydlighet i vem som gör vad, effektivisering av informationsvägar, samt att detta inte delas upp eller överlappas. Således bör man tydliggöra vem som tar fram föreskrifter och vägledningar med detaljerade krav, även för de mindre tekniska skillnader som finns inom de olika sektorsområdena för samhällsviktiga tjänster. Vem som genomför den tekniska tillsynen samt till vem man genomför anmälningstillsyenen. Vem som tar ansvar och koordinera arbetet vid storskaliga cyberkriser.

För att inte skapa oordning samt undvika att denna lagstiftning blir, resurs- tids- och kostnadsdrivande bör man tydliggöra roller och ansvar för myndigheter och center som berörs av denna lagstiftning.

För att stärka ordningen bör man utgå från att en aktör tar fram systemplattform för stöd, rapportering samt stödjande underlag (vägledning, övning). En myndighet ansvarar för föreskrifter och en myndighet för tillsyn. För energisektor blir det extra viktigt då arbetet kan samordnas mellan de olika lagstiftningarna (NIS2, CER, Säkerhetsskydd) samt dess kopplingar gentemot Totalförsvarsarbetet. Således ser vi att Energimyndigheten bör ha ansvaret som tillsynsmyndighet.

Förslag till lag om Cybersäkerhet

Nedan återges specifika förslag till respektive kap.

1. kap Inledande bestämmelser

Rörande vilka som berörs av lagen bör uppdelningen ske med tydliga tröskelvärden som är baserade på den samhällskritiska funktionen och möjlig störning av tjänst, snarare än bolagets storlek.

Kraven på systematiskt och riskbaserat informationssäkerhetsarbete föreslås gälla för hela verksamheten, även de delar som inte direkt stödjer den samhällsviktiga verksamheten. För att skapa en tydlighet i hur säkerhetsåtgärder ska appliceras för de delar av verksamheten som inte är av betydelse för den samhällsviktiga verksamheten, är det önskvärt med mer vägledning från tillsynsmyndigheten. Vägledningen bör bygga på ett riskbaserat förhållningssätt som grundar sig på hur verksamheter ska arbeta utifrån begreppet ”hela verksamheten”. I praktiken behövs en tydlig kravdifferentiering mellan de system som kan orsaka signifikanta incidenter gentemot övriga informations- och kommunikationssystem (IKT).

2. kap Klassificering och registrering

Gällande delsektorn Elektricitet så anges Enligt direktivet Bilaga 1 HÖGKRITISKA SEKTORER laddoperatörer.

Drivkraft Sverige vill lyfta otydligheten i direktivet och cybersäkerhetslagen gällande om laddinfrastruktur omfattas eller ej, det är ju en förutsättning att el levereras till laddstationen.

3. kap Riskhantering och incidentrapportering

Då branschen möts av en omfattande rapportering inom många områden så är det av stor betydelse att denna rapportering blir både tydlig och förenklas, annars risker denna skapa ett ostrukturerat och ineffektivt arbete där tid läggs på tolkning av administration. Ett exempel på vad som kan bli problematiskt är att låta NIS2- (och CER-) regleringen avseende incidentrapportering och tillsyn även gälla säkerhetsskyddad verksamhet. För att inte överlappa och skapa otydliga gränsytor mot tillsyn respektive rapportering enligt säkerhetsskyddslagen bör därför cybersäkerhetslagens krav på incidentrapportering och tillsyn undantas när det gäller den säkerhetsskyddade verksamheten. Syftet med förslaget är att komplettera kraven som gäller för säkerhetsskydd och i den utsträckning säkerhetsskyddsregleringen innebär strängare krav gäller givetvis dessa framför NIS2- och CER-regleringens krav. NIS2 har en 24-timmars tidslinje för anmälan av cybersäkerhetsincidenter. Formuleringen i den nationella NIS2-förordningen bör övervägas noga för att säkerställa att 24-timmarsklockan endast startar när det har analyserats att något kritiskt faktiskt har hänt. (GDPR har 72 timmars anmälningstid och tillsynsmyndigheterna översvämmas av onödiga anmälningar).

Ur ett samhällsekonomiskt perspektiv är det inte rimligt eller resurseffektivt att varje tillsynsmyndighet lägger ned resurser på att ta fram nya egna system som kan hantera verksamhetsutövarnas anmälningar och känsliga uppgifter med tillräcklig säkerhet. Verksamhetsutövare ska inte endast dela känslig information med de myndigheter som har utpekade uppdrag utifrån NIS2-regleringen i form av anmälningar. Samtliga verksamhetsutövare ska även skicka in incidentrapporter till CSIRT-enheten. Även incidentrapporter behöver hanteras med motsvarande säkerhetsnivå.

Rörande 3 kap 6§ Informationsplikt så finns det vissa utmaningar, då denna skrivelse idag är ej så tydlig. Det ska självklart finnas transparens, dock får den inte äventyra hur man lyckas upptäcka incidenter då angriparen kan få en bättre bild över verksamhetens arbetssätt.

4. kap Tillsyn

Att låta de olika föreslagna tillsynsmyndigheterna ta fram specifika föreskrifter för respektive område motverkar direktivets syfte, att vara homogent inom Europeiska unionen och även inom landet. Många verksamhetsutövare verkar dessutom inom flera samhällsviktiga sektorer och behöver därmed förhålla sig till många olika kravställningar för samma tekniska område som cybersäkerheten utgör. De skillnader som finns inom området bedömer vi kan få plats i samma föreskrift utan att vara begränsade till en specifik sektor. Det är också av stor vikt att tillsynsmyndigheterna i samverkan ger vägledning som är tydlig och praktisk tillämpbar.

Drivkraft Sverige bedömer därför att det är lämpligt att låta Energimyndigheten ha tillsynsansvaret då de kan samordnas mellan de olika lagstiftningarna (NIS2, CER, Säkerhetsskydd) samt dess kopplingar gentemot Totalförsvarsarbetet.

Ansvar

Skrivelsen rörande styrelsens uppdrag bör strykas då den redan har ansvaret för sitt företag.

Drivkraft Sverige håller med utredningen om att det för aktiebolag förefaller rimligt att styrelsen och VD ska anses utgöra ”ledningen” enligt direktivet. Självklart ska styrelsen ha god insikt och kunskap och cyberrisker. Det förefaller dock ha blivit vanligare att olika regelverk ställer specifika kompetenskrav på styrelser och reglerar vem som ska ansvara för vad i ett företag. Det är olyckligt. Hur ett företags verksamhet styrs och organiseras måste styrelse och ledning ha utrymme att själva bestämma. Detta gäller även beslut om vilka frågor som ska lyftas till vilken nivå och på vilket sätt.

Slutord

Syftet med lagförslag är att vi ska stärka både EU:s och Sveriges cyberförmåga – Bättre att bygga ett säkrare samhälle tillsammans genom samarbete, i stället för bara bot och piska. Ordet systematisk nämns i denna utredning, och här bör man se till så att det finns en sammanhållande systematik mellan nya cybersäkerhetslagen och säkerhetsskyddslagen (2018:585) som definierar tillsynsmyndigheternas befogenheter, där tillsynsperioderna bör harmoniseras mellan regelverken samt sanktionsavgifternas storlek.

Endast ökad regelbörda, administration och sanktionsavgifter som verktyg, skapar inte en stärkt cyberförmåga. Tvärtom skapar det snarare större distans än samarbete och tillit mellan stat och näringsliv. För att stärka vår cyberförmåga behöver vi stärka samarbetet och bygga förtroende tillsammans. Här bör man möjliggöra så att återkoppling och underrättelse genomförs löpande så att ständiga förbättringar kan genomföras samt att man kan implementera effektiva proaktiva åtgärder, således bör vi tillsammans jobba risk- och informationsbaserat.

Jessica Allenius
VD

Namn på expert: David Sällh
Titel på expert: Verkställande utskottschef

Stockholm den 28 05 2024