Datum
2024-05-28

Energisystem
Emma Johansson, 08-677 25 05
emma.johansson@energiforetagen.se

Till Försvarsdepartementet
Fö2024/00496

Remissvar av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Energiföretagen Sverige ger röst åt omkring 400 företag som producerar, distribuerar, säljer och lagrar energi. Energibranschen investerar omkring 30–35 miljarder kronor årligen. Med rätt förutsättningar kan vi fortsätta trygga energileveranserna till hushåll, företag och samhälle - varje sekund, året om - samtidigt som vi driver på den förändring som möjliggör framtidens energisystem. Vårt mål är att; utifrån kunskap, en helhetssyn på energisystemet och i samverkan med vår omgivning, utveckla energibranschen – till nytta för alla.

Övergripande synpunkter

Förslag till lag om cybersäkerhet

Cybersäkerhet är ett viktigt område för att upprätthålla robusthet, resiliens och redundans i digitala nätverks- och informationssystem. Störningar i leveranser kan leda till påverkan över landsgränser och få kaskadeffekter till följd i samhället. Att Europeiska unionen har ett tydligt och harmoniserat regelverk för medlemsstaterna med cybersäkerhetskrav för väsentliga och viktiga verksamheter är därför naturligt för att hantera cyberhot och säkerställa kontinuitet i samhällsviktiga tjänster.

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

Vi anser att utredningen väcker frågor snarare än att ge konkret vägledning i hur EU´s direktiv ska omsättas och tolkas. Det är bekymmersamt att få frågor besvaras konkret i utredningen för de verksamheter som kommer att omfattas i lagtexten. Då NIS2-direktivet innefattar säkerhet i leveranskedjan är det inte bara de verksamheter som omfattas som kommer att påverkas av den nya cybersäkerhetslagen, utan även deras leverantörer och underleverantörer. På så sätt kommer NIS2 att få betydligt bredare påverkan än nuvarande NIS-lagstiftning. Konsekvensen blir nu i stället att föreskrivande och tillsynsansvariga myndigheter kommer få lösa mycket, dels vilka som omfattas, dels de faktiska kraven och tolkningarna genom kommande föreskrifter, vägledningar och tillsyn.

För att utvecklingen av cybersäkerhet ska ge tydlig effekt vill vi särskilt betona vikten av:

- tydliga, enkla och gemensamma regler och säkerhetskrav för utpekade sektorer och dess leveranskedjor med fokus på ett riskbaserat arbetssätt.
- tillse harmonisering mellan olika sektorer vad gäller såväl krav som tillsyn.
- informationssammanställningar och sårbarhetsscanningar utan tydliga syften bör begränsas och tydligare anpassas vid incidenter till mer specifika behov för att hantera cyberattacker.
- utveckla lagstiftningen utifrån både företags organisatoriska struktur, och det offentligas förutsättningar, för att minska verksamheters administrativa rapporteringsbörda och undvika osäkerheter vid tillämpning och tillsyn av hela verksamheten.
- att helt ta bort kravet på systematiskt informationssäkerhetsarbete som var ett svenskt påfund vid implementeringen av NIS1. Att ta bort detta krav skulle harmonisera kraven medandra länder och minska problematiken för verksamheter med flera tillsynsmyndigheter, verksamheter med verksamhet i flera länder samt minska risken att affärskänslig information sprids felaktigt eller feltolkas. Detta utan att säkerhetsarbetet och säkerheten i sig skulle förändras.
- genomföra fördjupad konsekvensanalys avseende resursmässiga, ekonomiska samt kompetensmässiga effekter enligt direktivet för utpekade verksamheter och leveranskedjor som kommer omfattas av den nya regleringen.
- tydliggöra effekter av mycket och överlappande lagstiftning inom digitaliserings- och säkerhetsområdet som skett på kort tid, samt beskriva hur dessa kan integreras i beredskapssystemet.
- undanta verksamheter som pekas ut i Nätkod för cybersäkerhet för att undvika dubbelreglering inom samma område.

Detaljerade synpunkter

1 kap. Inledande bestämmelser

Lagens tillämpningsområde

Det finns i direktivet möjlighet att göra undantag från storlekskravet så att även mindre verksamheter omfattas givet vissa förutsättningar. Den föreslagna nya cybersäkerhetslagen är mer omfattande än direktivet avseende storleksundantag för verksamheter som är väsentliga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Enligt direktivet artikel 2, punkt 2b) ska sådan verksamhet vara ”den enda leverantören”. I cybersäkerhetslagen 8§ punkt 1 har detta utvidgats genom att begränsningen ”den enda leverantören” utgått.

Vi saknar ett tydligt resonemang och motivering om varför utredningen gör denna utvidgning. Uppdelningen bör ske med tydliga tröskelvärden som är baserade på den samhällskritiska funktionen och möjlig störning av tjänst, snarare än bolagets storlek. I nuvarande lagstiftning är det NIS-leverantören som avgör om verksamheten omfattas eller inte. I det uppdaterade förslaget bör inte verksamheterna själva skönsmässigt bedöma om de omfattas av NIS2 eller inte.

Det riskerar att leda till en fortsatt differentiering av omhändertagandet cybersäkerheten och snedvridning av konkurrensförmåga hos liknande verksamheter.

Energiföretagen har tidigare givit remissvar på kommissionens förslag rörande gränsdragning vid antalet anställda då en stor del av befintliga verksamheter inom energisektorn skulle falla bort och inte skulle omfattas av direktivet då dessa företag huvudsakligen består av mindre verksamheter med färre än 50 anställda. Därmed skulle nyttan med harmonisering av cybersäkerhet i det nya förslaget försvinna för flertalet verksamheter inom energisektorn. Vi välkomnar därför att det finns tillägg som går utöver direktivets förslag. Däremot bör utredningen vid tillämpning av undantag från direktivet väl motiverat detta för att minimera att kravställningen skiljer sig åt mellan olika EU-länder.

Vi vill även lyfta fram att en uppdelning inom en sektor bör vara möjlig så att inte alla tjänster nödvändigtvis hamnar på så samma kravnivå utan att det finns möjlighet att utgå från hur kritisk den enskilda verksamheten är för att avgöra kravnivån. Det är viktigt att identifiering av verksamheter sker utifrån dess samhällspåverkan – det finns i sektorn enheter med liten betydelse som exempelvis små verksamheter av fjärrvärme och fjärrkyla som bör undantas.

Vi hade också önskat se en problematisering kring begreppen entitet, verksamhet, verksamhetsutövare och juridisk person då en icke-optimal implementering som inte är i linje med hur företag verkar och dess organisationsstruktur leder till stora administrativa kostnader utan att för den skull stärka säkerheten.

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 som snarare bygger på ett riskbaserat förhållningssätt utifrån hur verksamheter ska arbeta utifrån begreppet” hela verksamheten”. I praktiken behövs en tydlig kravdifferentiering mellan de nätverk- och informationssystem som kan orsaka signifikanta incidenter gentemot övriga nätverk- och informationssystem.

Relationen moderbolag och dotterbolag som skilda juridiska personer innebär att de enligt NIS2 utgör enskilda verksamhetsutövare och ska göra egna bedömningar om huruvida de omfattas. Tolkningen är dock att dotterbolag som trots att de som enskild verksamhetsutövare inte omfattas utifrån någon av delsektorerna, trots allt kan omfattas på grund av sambandet med moderbolaget. Denna del är komplex och ställer stora krav på detaljering i analysarbetet. Föreskrifter från tillsynsmyndigheten måste här bli tydlig för att kunna göra korrekt bedömningar och senare också för att anmälan till tillsynsmyndigheten ska bli korrekt.

Undantag från lagens tillämpningsområde

Förhållandet mellan svenska säkerhetsskyddslagstiftningen och NIS2-direktivet samt reglering av cybersäkerhet för elenergins aktörer genom Nätkod för cybersäkerhet (NC CS) behöver klargöras av myndigheterna. Då vi ser att direktivets påverkan ökar i omfattning med NIS2-förslaget för verksamheter som hanteras inom ramen av säkerhetsskyddslagen och Nätkoden för cybersäkerhet

Vi får inte hamna i samma otydlighet som idag huruvida legala krav ska implementeras och efterlevas i verksamheterna eller inte. Generellt är tydlighet kring hur lagstiftningar förhåller sig till varandra gynnande för effektiviteten i säkerhetsarbetet genom att minska risken för dubbelarbete med dubbelrapporteringar och dubbla tillsyn inom samma område som cybersäkerhet utgör. NIS2- och kommande CER-utredning behöver även integreras i nuvarande nationella beredskapssystemets förmågekrav på resiliens.

2 kap. Klassificering och registrering

Gällande delsektorn Elektricitet

Enligt direktivet Bilaga 1 HÖGKRITISKA SEKTORER står det att laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn omfattas.

Energiföretagen vill lyfta otydligheten i direktivet och cybersäkerhetslagen gällande om laddinfrastruktur omfattas eller ej.

Gällande delsektorn Fjärrvärme och fjärrkyla

Enligt direktivet Bilaga 1 HÖGKRITISKA SEKTORER står det under punkt b) Fjärrvärme och fjärrkyla — Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001.

Energiföretagen vill lyfta otydligheten i direktivet och cybersäkerhetslagen gällande om anläggningar omfattas eller ej - jämför exempelvis med Fjärrvärmelag 2008:263 där produktion tydligt ingår. Vi avstyrker även referensen till definitionen enligt EU:s förnybart-direktiv som har ett helt annat syfte en nu aktuell lagstiftning. Vi anser i stället att hänvisning bör ske till definitionen av fjärrvärmeverksamhet enligt 1 § fjärrvärmelagen (2008:263) respektive fjärrkyleverksamhet enligt 2 § fjärrkylelagen (2022:332).

Definitionen av fjärrvärme och fjärrkyla enligt direktivet och cybersäkerhetslagen pekar nu tydligt på att distribution från produktionskällor omfattas. Det är dock svårt att utifrån definitionen se att även själva produktionsanläggningen omfattas. I ett svenskt sammanhang utförs distribution och produktion ofta av samma verksamhet samt med samma eller närliggande system. Det bör tydliggöras vad

som omfattas – enbart distribution alternativt båda distributioner och produktion. Inte minst är detta viktigt för att kunna tolka och beskriva vad en ”betydande incident” för undersektorn är.

3 kap. Riskhantering och incidentrapportering

Övergripande om begrepp

Vi anser att läsbarheten och tydligheten i utredningens förslag gällande säkerhetsåtgärder (3kap §1) är rimlig, men då cybersäkerhetslagen i stort är väldigt 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.

Om incidentrapportering

I nya förslaget finns det mer långtgående krav på incidentrapportering. Det är oerhört viktigt att säkerställa metodik, men framför allt genomförbarheten av rapporteringen samt uppföljning och återrapportering till de verksamheterna som incident rapporterar. Fler frågor från myndigheterna innebär inte alltid att verksamheterna får en bättre bild av situationen. De nya förslaget måste likväl vara hanterbart för såväl stora bolag likväl som små energiföretag. Kraven på rapportering är snårigt redan idag med en mängd frågor som skall besvaras och kommande rapportering av incidenter kommer att kräva ökade resurser då även tillbud ska rapporteras in. Därför är det viktigt att rapporteringskravet och dess omfång läggs på en rimlig nivå.

Hur ska verksamheter kan tolka "kan orsaka" bör inte vara fritt för verksamhetsutövaren att tolka. Förtydligande krävs därför i 3 kap.4 § av avseende följande definition av betydande incident: “En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller”.
Leverans av energitjänster, produktion och distribution, är relativt okänsliga för avbrott i övervakning. Tjänsteleveranserna kommer fortsätta i många timmar och även dagar och det är först vid felavhjälpning som driftövervakningen blir viktig i felavhjälpningssyfte. Energiföretagen förslår således att kriterierna för inrapportering justeras för att ta detta i beaktande. Att verksamheter behöver rapportera in några minuters övervakningsbortfall är inte rimligt.

Energiföretagen vill också lyfta behovet av att stärka skyddet av sekretess för de uppgifter och eventuella affärskänsliga uppgifter som lämnas vid incidentrapportering. Det finns annars risk för att verksamhetsutövare kommer att lämna alltför knapphändig information på grund av potentiella brister i konfidentialitet. Vi ser även att innebörden av återkoppling till verksamheten som

rapporterar in förtydligas och ges inom rimlig tid. Samt att behovet av att närmare utreda möjligheten att ge nationella CSIRT-enheten befogenhet att inhämta information via sårbarhetscanningar från verksamheterna som har relevans för att kunna varna och skydda samhällskritisk verksamhet är nödvändigt.

Om underrättelse till kunder

I 3kap 6§ anges "Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot".

Vi välkomnar transparens vid inträffade incidenter där det finns en kundpåverkan och där kund har behov av information för att kunna planera egen verksamhet eller för att vidta egna åtgärder. Dock önskar vi se en tydligare beskrivning av vad och hur som ska informeras för att förhindra oavsiktligt röjande av vår kunskap om en viss händelse.

4 kap. Tillsyn

Energiföretagens förslag är att helt ta bort kravet på systematiskt informationssäkerhetsarbete för att undvika osäkerheter vid tillämpning och tillsyn av hela verksamheten. Ett systematiskt arbete var ett svenskt påfund vid implementeringen av NIS1. Att ta bort detta krav skulle dels harmonisera kraven i NIS2 med andra länder, dels minska problematiken för verksamheter med flera tillsynsmyndigheter, och verksamheter med verksamhet i flera länder. Samt minska risken att affärskänsliga information sprids felaktigt eller feltolkas. Detta utan att säkerhetsarbetet och säkerheten i sig skulle förändras.

Det skulle också minska framtida problematik vid eventuell ytterligare europeiska direktiv. Systematiskt arbete följer redan av det riskbaserade arbetssättet som direktivet kravställer.

Tillsynsmyndighetens uppdrag

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 tydliga krav och som är praktisk tillämpbar.

Energiföretagen bedömer att det är lämpligt på sikt att skapa en cybersäkerhetsmyndighet som har förmåga att utföra relaterat arbete till ansvaret inom cybersäkerhetslagen som att:

- Ta fram föreskrifter och vägledningar med detaljerade krav, även för de mindre tekniska skillnader som finns inom de olika sektorsområdena för samhällsviktiga tjänster.
- Stödja de tekniska tillsynsmyndigheterna för att harmonisera kravnivåer.
- Att ta ansvar som cyberkrismyndighet och koordinera arbetet vid storskaliga cyberkriser.

Anmälningstillsyn bör fortsättningsvis hanteras av respektive sektorsansvarig myndighet.

Säkerhetsrevision
Energiföretagen stämmer in med utredningen om att externa säkerhetsrevisioner starkt bör begränsas och regleras. Möjligheterna för tillsynsmyndigheterna att ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten strakt måste begränsas då detta går emot svensk tradition, samt att stora risker är förbundna med att låta detta bli konsult- och revisionsbolags drivet. Detta kan inte bli en "utväg" för myndigheterna att bedriva tillsyn som saknar kompetenser.

Förbud att utöva ledningsfunktion
I de fall dotterbolag omfattas av direktivet på grund av sambandet med moderbolaget blir det otydligt vilken del av verksamhetsutövarens ledningsfunktion som är ytterst ansvarig för att dels godkänna riskhanteringsåtgärder, dels är ytterst ansvarig vid tillsyn och delgivning av eventuella sanktioner samt eventuellt delgivning av förbud att utöva ledningsfunktion. Detta måste tydliggöras. Vidare bör styrelsen uppdrag strykas då det är underförstått att en styrelse redan har ansvaret för att förbereda, formulera och prioritera rätt frågor för företagets affärsnytta.

Ekonomiska konsekvenser

Det är bristfälligt att det saknas en genomgripande konsekvensanalys av NIS2-direktivet för utpekade verksamheter och leveranskedjor som kommer omfattas av den nya regleringen. Utredaren bör lägga kraft på att utreda konsekvenser för hur ett mer omfattande cybersäkerhetsarbetet påverkar verksamheter resursmässigt och ekonomiskt samt kompetensmässigt. Den kompetensbrist som råder i att upprätthålla kapacitet och kontinuitet i digitala informations- och kommunikationssystem (IKT) system behandlas styvmoderligt. Detta är inte enbart en fråga för ledningen utanför för hela samhället. Därtill sker det cyberattacker på alla fronter i Sverige och i vår omvärld och det pågår ett långdraget krig med cyberkrigsföring i vår närhet. Faktorer som har påverkan på den digitala utvecklingen och unionens samt ytterst Sveriges säkerhet.

Förutom verksamheters ökade ekonomiska risker vid cyberattacker är även konsekvenser av flera nya förslag från EU och överlappande lagstiftning inom

digitalisering- och säkerhetsområdet på kort tid av vikt viktigt att hantera i konsekvensanalysen. 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.

Slutligen vi vill betona vikten av att på ett effektivt sätt upprätthålla en koncernorganisation, som kan ha verksamheter i flera länder, under kriser som storskaliga cyberangrepp. Företag har en koncern bland annat för att bedriva verksamhet effektivt genom att man centraliserar ledningsfunktioner och stödfunktioner som till exempel IT-drift. För att kunna planera affärsverksamheter effektivt är det alltså nödvändigt att en koncern har möjlighet att dela information effektivt. Den andra sidan av myntet är att det är rimligt att cybersäkerhetsåtgärder också utarbetas gemensamt av kostnadsskäl. Det kan gälla IT-plattformar, personalresurser osv.

Utredningen har inte i tillräcklig utsträckning beaktat privata företag merkostnader. Den administrativa pålaga att till exempel rapportera in incidenter på verksamhetsnivå i stället för på koncernnivå riskerar att bli ett hinder för en snabb krishantering av cyberangrepp vilket inte bidrar till ekonomisk effektivitet enligt direktivets syfte. Samma konsekvenser ser vi redan idag i hantering av informationsdelning inom totalförsvarsarbetet och denna nationella säkerhetskyddslagstiftning.

Avslutningsvis

Energiföretagen vill göra det enklare för energibranschen att bidra till digitala omställningar som i sin tur bidrar till att skapa ett robust och hållbart energisystem. Effektiviteten av säkerhetsarbetet inom energi främjas av tydlighet kring hur den nya cybersäkerhetslagen, Nätkod för cybersäkerhet (NC CS) och svenskt säkerhetsskydd kommer att förhålla sig till varandra. Vi ser gärna att utredningen i sitt fortsatta arbete specifikt diskutera ett eventuellt undantag kopplat till nätkoden för att undvika dubbelreglering inom samma områden. Samt åtminstone tar inledande steg till sammanhållande systematik mellan nya cybersäkerhetslagen och säkerhetsskyddslagen (2018:585) som definierar tillsynsmyndigheternas befogenheter, där tillsynsperioderna bör harmoniseras mellan regelverken samt sanktionsavgifternas storlek.

Det är även viktigt att målet med ständiga förbättringar inte tappas bort. Vi tror att det är oerhört viktigt att de nationella myndigheternas ansvar och roll förstärks genom en riskbaserad metodik och inte utarmas genom ett fokus på systematik. Vi behöver alla bidra till att öka cybersäkerhetskapaciteten för att upprätthålla allmänhetens förtroende i samhället och hantera cyberhot och angrepp kraftfullare.

Stockholm som ovan

Åsa Pettersson
vd