ENERGI FÖRETAGEN

Datum
2021-06-29

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

Till Försvarsdepartementet
forsvarsdepartementet.registrator@regeringskansliet.se
Kopia till
i.registrator@regeringskansliet.se

Gällande ACER:s förslag om Nätkod för cybersäkerhet

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.

Bakgrund och generella synpunkter

En utökad elektrifiering av samhället är viktig för konkurrenskraft, säkerhet och ett fossilfritt Sverige. Dessutom bidrar elektrifieringen till uppfyllande av Agenda 2030 och de globala målen för hållbar utveckling. ACER:s förslag, på uppdrag av den Europeiska kommissionen, till ramriktlinje om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden, bygger på begreppet om en EU-gemensam hantering av cyberangrepp riktad mot energisektorn.

Det finns dock en betydande oro för att förslaget till en EU gemensam nätkod för cybersäkerhet är alldeles för omfattande och vag för att ge ett uppsving för EU:s cybersäkerhet och ett starkare och tryggare samhälle. Tvärtom är förslaget svårt att tillämpa, oproportionerligt, inte teknikneutralt, saknar ansatser för informationshantering samt ambition att stärka hela de europeiska elnätets säkerhet. Förslaget ökar skillnader inom de europeiska länderna för företagen och medlemsstaterna i och med att kravet om omfattning inte sätts utifrån påverkan av störning av tjänst (produktion och distribution av el) och eventuella kaskadeffekter vid ett cyberangrepp. En inkludering av och krav på säkerhetsåtgärder utifrån storlek på bolag och omsättning saknar logisk koppling till de möjliga konsekvenserna av ett cyberangrepp på energisystemet och påverkan i samhället och kritisk infrastruktur.

Energiföretagen Sverige är positiv till ansatsen att skydda elnätet mot ökade cyberangrepp, men vill framföra skarp kritik av förslaget då det medför negativa konsekvenser för den nationella säkerheten, förståelsen av en komplex hotbild mot energisektorn och vikten av hög informationssäkerhetsnivå inom sektorn. ACER beskriver i FG att ett litet företag definieras som ett företag som sysselsätter färre än 50 personer och vars årliga omsättning och / eller årliga balansomslutning inte överstiger 10 miljoner euro. I Sverige har vi cirka 160 DSO: er och de flesta har då färre än 50 anställda som inte skulle omfattas av förslaget.

Förslagets konsekvenser bör utredas ytterligare av den europeiska kommissionen då ACERs förslag brister i helhetssyn och i konsekvensanalys.

Detaljerade synpunkter

Energiföretagen Sverige

- anser att förslaget oproportionerligt ställer krav på arbetsstrukturen inom företag i stället för att reglera säkerhetsåtgärder för att öka motståndskraften mot cyberangrepp. Vi rekommenderar i stället ett processbaserad tillvägagångssättet för att bara välja tillgångsbaserat tillvägagångssätt, eftersom det första ger en bättre överblick över elföretagens verkliga risker som kan påverka gränsöverskridande elförsörjning. Ett tillgångsbaserat tillvägagångssätt listar bara komponenter, medan ett processbaserat tillvägagångssätt ger en översikt över alla sammankopplade system.

- konstaterar att förslaget överlappar med flera existerande regelverk samt att kraven på databehandling och informationsspridning i och med förslaget om ett EU gemensamt risk-och sårbarhetsregister strider mot både den nationella säkerhetsskyddslagstiftningen och NIS-lagstiftningen. Vi anser, baserat på nationella erfarenheter, att det är viktigt att ställa krav på funktionalitet och processer för att stärka cybersäkerheten. Anledningen är att processerna kan vara desamma i hela Europa, men riskbedömningarna som ingår i processerna kan regleras av nationell lagstiftning som för närvarande förhindrar att sådan information rapporteras.

- Ifrågasätter förslaget om EU:s överstatliga incidenthantering av cyberangrepp. I det nya förslaget finns det mer långtgående krav på incidentrapportering till CSIRT på EU-nivå. Det är oerhört viktigt att säkerställa metodik, men framför allt genomförbarheten av rapporteringen samt uppföljning och återrapportering till de entiteterna som incidentrapporterar. Fler frågor från myndigheterna innebär inte alltid att verksamheterna får en bättre bild av situationen. De nya förslaget måste vara hanterbart för såväl stora bolag likväl som små energiföretag. Kraven på rapportering kommer att kräva ökade resurser, därför är det viktigt att rapporteringskravet läggs på en rimlig nivå. Att samla information om incidenter hos en instans i EU kan också innebära risker för hackerattacker och att kunskap om svagheter i nationella system läcker.

Avslutande ord

Frågan om hur energibranschen skyddar sin verksamhet mot cyberattacker är en högst aktuell fråga och avbrott i elförsörjning som beror på cybersäkerhet innebär risk för stora kostnader för samhället. Det är därför ytterst angeläget att både nationella som EU-relaterade regelverk är träffsäkra, kostnadseffektiva och ger möjlighet till nationella anpassningar vid behov.

Vi tror att det vore bra om Försvarsdepartementet i samverkan med andra berörda departement engagerar sig i frågan, inte minst eftersom nya krav i förslaget till nätkod

träffar aktörer som redan idag har andra regelverk på området att följa. Det finns idag varken en nationell myndighetsföreträdare eller offentlig nordisk företrädare av Nätkod för cybersäkerhet. Energiföretagen önskar få detta tillstånd för ökad samverkan av cybersäkerhets arbetet. Vi finns självklart tillgängliga för dialog och frågor.

Vi bifogar för kännedom vårt remissvar till ACER som vi givit in som ett svar på det samråd som ägt rum.

Stockholm som ovan

Åsa Pettersson
vd