Datum 2022-01-10

Dnr 080/2021

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

Till Försvarsdepartementet
fo.remissvar@regeringskansliet.se
diarienummer Fö2021/00796

Yttrande över slutbetänkandet "Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem" (SOU 2021:63)

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.

Inledning

Energiföretagen Sveriges medlemmar bedriver verksamheter som är av betydelse för Sveriges säkerhet och omfattas därmed av betänkandets förslag. Exempel på sådan verksamhet är försörjning av el, värme och kyla.

Energiföretagen Sverige har därför valt att svara på remissen från Försvarsdepartementet, ”SOU 2021:63 Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem”.

Vi skulle självfallet uppskatta att tas med bland remissinstanserna för framtiden för remisser av det här slaget.

Sammanfattning

Energiföretagen instämmer i betänkandets slutsats om behovet av en ökad säkerhet och ett stärkt skydd för säkerhetskänsliga verksamheter. Digitalisering ger möjligheter till förbättrad kvalitet och ökad effektivitet inom många delar av energisektorn. Med de positiva möjligheterna följer även ökade hot, risker och sårbarheter som på olika sätt kan påverka verksamheternas möjligheter att utföra sina åtaganden inom energiförsörjningen.

I förslaget ligger förutom befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning även krav på att omfatta planerade väsentliga förändringar av informationssystem, som kan ha betydelse för säkerhetskänslig verksamhet.

Energiföretagen delar utredningens syn på behovet av en ökad medvetenhet och kunskap om säkerheten hos IKT-produkter, -tjänster och -processer, men ser problem med en tvingande begränsning av konkurrensskäl. Det är Energiföretagens uppfattning att bedömningar av vilka tekniska lösningar som nyttjas i möjligaste mån bör beslutas av den

som är närmast verksamheten och det berörda systemet, så länge lösningarna ger ett ändamålsenligt skydd.

Energiföretagen anser att förslaget om ny rätt för tillsynsmyndigheterna att utan samtycke från verksamhetsutövaren genomföra teknisk tillsyn på aktiva informationssystem innebära en risk för påverkan av leveranssäkerhet vid tillsyn. I utredningen framgår inte syftet varför en tvingande tillsynsåtgärd skulle vara nödvändig för att stärka säkerheten i berörda informationssystem, samt ansvarsförhållandet vid en störning av tjänst som för energisektorn kan leda till en större samhällsstörning.

Vår bedömning är att samrådsförfarande inför driftsättning är tillräckligt skydd, i kombination med en frivillig möjlighet för verksamhetsutövare att utföra tekniska säkerhetsgranskningar.

Övergripande synpunkter

Samråd

Ett krav om godkännande från en samrådsmyndighet vid införande eller förändring av informationssystem som hanterar hemliga uppgifter kan, enligt Energiföretagen Sveriges uppfattning, bidra till att stärka skyddet av säkerhetskänsliga verksamheter. Dock, om samrådsmyndigheten beslutar om ett förbud mot driftsättning innebär det att verksamheten inte fritt kan förfoga över sin egendom, vilket innebär att självbestämmandet påverkas.

Ett ytterligare påpekande är att energisektorn kan ha flera samrådsmyndigheter, beroende på energiförsörjning (el, värme och kyla). Detta komplicerar dels samrådsprocessen och förfarandet om ett godkännande dels om ett eventuellt underkännande av informationssystem sker av en myndighet, då ofta samma informations- och kommunikationssystem används inom hela bolaget för flera olika energitjänster.

Certifieringskrav av IKT

Säkerhetsnivån på en certifierad säkerhetsprodukt är beroende av vilken certifiering som produkten har. Det finns idag, vilket även utredningen konstaterar, flertalet utfärdare av säkerhetscertifikat för IKT produkter, -tjänster och -processer, vilka arbetar utifrån egna krav och certifieringsrutiner.

Ett krav på certifiering av lKT-produkter, -tjänster och -processer skulle innebära en stor utmaning vid upphandling för verksamheterna, där en begränsning av godkända certifikat måste ställas mot att verksamhetsutövare inte bör tilldelas ett alltför begränsat utbud av säkerhetslösningar.

Energiföretagen Sverige har i tidigare remissvar för Nätkod för cybersäkerhet förespråkat en reglering som i stället för certifieringskrav ställer specifika funktionella och tekniska krav på system. Vid en certifikatbaserad reglering av IKT-produkter, -tjänster och -processer, kommer utbudet av leverantörer i viss mån riskera att baseras på marknadens ekonomiska incitament av efterfrågade certifieringar. Skulle leverantörer genom en och samma certifiering ges tillträde till exempelvis hela den Europeiska unionens energimarknad bör konsekvenser av kaskadeffekter på distributionssystemet av energi vägas in i upphandlingen av system. Där bör verksamheterna förutsätta att effekterna är

väsentligen högre än om motsvarande leverantör endast skulle ge tillträde till exempelvis den svenska marknaden.

Tillsynskrav

Utredningen föreslår en rätt för tillsynsmyndigheterna att vid tillsyn få tillgång till informationssystem i syfte att genomföra tekniska kontroller. Utredningen anser att vid genomförandet av teknisk tillsyn även ska vara möjligt att genomföra vad som benämns som teknisk sårbarhetsgranskning, genom simulerade angreppsförsök. Det är direkt olämpligt att genomföra test av cyberangrepp på system i drift inom energiförsörjningen då det finns stor risk för leveransstörningar av tjänst och produkt som kan få en påverkan på hela samhället och individ.

Energiföretagen saknar dessutom en tydligt angiven ansvarsfördelning vad avser skador som kan ske vid aktiva tekniska kontroller. Att simulera angrepp på ett informationssystem kan innebära förlust av data och påverkan på mjukvara eller fysiska skador på utrustning.

Kritiska system i energisektorn bör inte bli föremål för denna typ av teknisk säkerhetsgranskning som utredningen föreslår eller kunna genomföras utan samtycke från systemägaren. Det bör kunna förutsättas att ett informationssystems skyddsvärde följer de rekommendationer som finns för information enligt informationsklassificeringen, enligt Säpos vägledning för informationssäkerhet.

Energiföretagen förespråkar i stället att sårbarheter i IKT-system provas i testmiljöer såsom på FOI:s testlabb i Linköping och inte i verklig driftmiljö.

Harmonisering med övriga säkerhetslagstiftning

Energiföretagen uppmanar att förslaget tar hänsyn till om det finns behov av ytterligare obligatoriska säkerhetskrav i relation till nuvarande säkerhetskyddslagstiftning samt EU:s marknadskontrollmekanismer. Vi anser att dagens informationssäkerhetskrav är långtgående och efterfrågar mer tillsyn för kontroll av efterlevnad snarare än ökad reglering för att säkerställa den nationella skyddsnivån.

Vi ser även ett behov av att harmonisera förslaget med kraven på cybersäkerhetscertifiering på produkter med inbyggd teknik, såsom artificiell intelligens (AI), sakernas internet (IoT)och robotteknik, i enlighet med EU:s säkerhetslagstiftning, såsom pågående NIS-2 direktivets förhandlingar, cybersäkerhetakten och AI-förordning.

Vid behovet av att utveckla obligatoriska certifieringssystem för produkter på nationell nivå bör hänsyn tas till sektorsspecifika aspekter. För att inte produktsäkerhetskrav ska utgör något hinder för innovation inom energisektorn som snabbt kan komma att uppdateras och anpassas till aktuella hot och risker. EU:s NIS-direktiv samt den sektorsspecifika Nätkoden för cybersäkerhet är två av de främsta verktygen för att förbättra informations-och cybersäkerheten på EU-nivå för energiförsörjningen.

Konsekvensutredning

Förslaget påverkar säkerheten i nätverks- och informationssystem hos många olika verksamhetsutövare, flera med höga skyddsvärden. Det är önskvärt om en konsekvensutredning genomförs och att utredningen tar upp helhetsperspektivet på

säkerhetsskyddets regelverk. Såvitt Energiföretagen kan bedöma har konsekvensutredningen inte gjorts.

Det är viktigt att beakta att även små energibolag på ett enkelt och konkret sätt kan arbeta med nät- och informationssäkerhet. För att höja säkerhetsnivån på bred nationell front bör utbildningssatsningar inom området genomföras med ett nationellt samordningsansvar. Vår bedömning är att framför allt de mindre energibolagen saknar finansiella medel och resurser för att skapa den robusthet som krävs för att möta de nya skyddskraven.

Slutord

Behovet av samordning, reglering och kompetensutveckling i informations- och cybersäkerhet är stort inom energisektorn. Den nuvarande digitaliseringen och ökade cyberangrepp har med all tydlighet visat på brister i svensk samhällsberedskap. Inom ett sådant här område, där samhället i sin helhet bäst har nytta av långsiktighet, bör regleringar inom säkerhetsskydd samt informations-och cybersäkerhet inriktas mot hållbara och bestående lösningar i stället för fler regleringar för företag inom energisektorn. Det yttersta målet är att skapa resiliens i energiförsörjningen mot hot, risker- och sårbarheter. Energiföretagen finner att nuvarande säkerhetsskydds- och NIS-lagstiftningen lever upp till det målet varvid vi inte ser behov av mer obligatoriska regleringar på detaljnivå i verksamheterna då:

- Ändringar i säkerhetsskyddslagen är redan genomförda.
- Långtgående certifieringskrav leder potentiellt till följdproblem.
- Befintliga och tillkommande regelverk är tillräckliga, men kan harmoniseras.
- Fokus på tillsyn är viktigare än mer lagstiftning. Föreskriftsrätten bedöms ju dessutom redan finnas.
- Konsekvensutredning är en viktig parameter för att tillsynen ska kunna planeras klokt.
- Ökat stöd med kompetensutveckling och finansiering är viktigt.

Stockholm som ovan

Åsa Pettersson

vd