KS BedriftEnergi

NVE
Postboks 5091, Majorstua
0301 Oslo

Oslo, 23.03.2018

Høring – endring i regelverk for beredskap i energiforsyningen

Innledning

KS Bedrift Energi representerer lokale og regionale energibedrifter over hele landet. Våre medlemmer er aktive over hele landet og over hele verdikjeden, fra produksjon via distribusjon til omsetning. Mens nett er det viktigste forretningsområdet for de fleste av våre medlemmer, er det også flere medlemsselskap med betydelige volumer av kraftproduksjon. Dette medfører at KS Bedrift Energis medlemmer påvirkes på ulike måter av NVEs forslag til endringer i regelverket for beredskap i energiforsyningen.

Sammendrag

Selv om KS Bedrift ønsker at bransjens håndtering av, og bevissthet rundt, sikkerhetsutfordringer er så god som mulig, ser vi at enkelte av kravene NVE ønsker å innføre er unødvendig strenge, mens andre av forslagene fremstår som tvetydige.

Vi mener NVE bør vurdere å innføre en bestemmelse om at leverandører og tilbydere må være ISO-sertifiserte, heller enn utelukkende å legge alt ansvar på nettselskapet. Vi mener også at samarbeidsordninger kan bidra til å heve sikkerhetsnivået i bransjen, og at NVE bør legge bedre til rette for at samarbeid kan opprettes.

Vi ser behovet for en lettfattelig veileder på temaet, og ber NVE om å forbedre dagens veileder.

Bakgrunn

Dette høringssvaret dreier seg i hovedsak om paragrafene 6.9 om digitale informasjonssystemer, i tillegg til 6.10, om bryterfunksjonalitet i avanserte måle- og styringssystem, ettersom det er disse delene av NVEs forslag som i særlig grad påvirker medlemsmassen i KS Bedrift Energi. Vi omtaler også andre av forslagene i høringsdokumentet.

Forsterkede krav til IKT-sikkerhet i kraftsektoren kommer som en følge av at digitalisering i bransjen øker sårbarheten til en samfunnskritisk infrastruktur. Dersom sikkerhetsregimet i kraftselskapene er mangelfullt, kan de samfunnsmessige konsekvensene være store. NVE mener det er behov for ytterligere presisering i regelverket slik at virksomheter og systemer i energisektoren er beskyttet mot hele bredden av digitale trusler. På vegne av bransjen støtter vi innføringen av helhetlige krav til sikkerhet i selskapene, herunder grunnsikring av digital informasjonssystemer.

Mens driftskontrollsystemer og håndteringen personsensitive opplysninger er og har vært underlagt strenge krav til sikkerhet, utvides virkeområdet til også å gjelde administrative IKT-systemer. Dette er fordi slike systemer kan fungere som en bakdør for innbrudd i mer sensitive systemer, med tap av kontroll og/ eller sabotasje som mulige, negative tenkelige utfall.

Bransjen kjøper inn, og bruker, slike administrative systemer fra et stort antall leverandører.

6.3 og 6.4 Beskyttelse, avskjerming og tilgangskontroll/ sikkerhetsinstruks

NVE ønsker at alle virksomheter som har eller behandler sensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon.

NVE vil innføre krav om at beskyttelse omfatter tiltak mot avlytting og manipulering fra uvedkommende.

Et enkelt tiltak er å innføre rutiner for å hindre at telefoner/ nettbrett og annet bringes inn i rom hvor det oppbevares eller diskuteres sensitiv informasjon. KS Bedrift Energi mener samtidig det er praktisk umulig å helgardere seg mot avlytting og/ eller manipulering fra uvedkommende. Eksempelvis kan avansert avlyttingsutstyr fange opp vibrasjoner i ruter og glass som oppstår under samtaler, og slik få tilgang til informasjon. KS Bedrift Energi mener dette ikke er praktisk mulig innenfor rimelighetens grenser å fjerne enhver risiko for dette.

Vi støtter utover dette NVEs foreslåtte krav om at virksomheter som har eller behandler sensitiv infrastruktur innfører tiltak som minimerer risikoen for at informasjon kommer på avveie, og utarbeider en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas.

Vi foreslår at NVE inkluderer et generisk oppsett for en slik instruks til veilederen direktoratet utarbeider på sikkerhetsfeltet.

6.9 Plikt til grunnsikring

NVE vil innføre krav til grunnsikring for alle digitale informasjonssystemer hos alle virksomheter som er underlagt forskriften, og at det etableres funksjonskrav som sørger for et minstenivå på informasjonssystemsikkerhet. Kravene vil i praksis gjelde de aller fleste aktører i bransjen.

NVE henviser flere steder til NSMs grunnprinsipper for IKT-sikkerhet. Utfordringen ved dette er skrevet i NSMs publikasjon: grunnprinsippene beskriver hva som må gjøres for å sikre et IKT-system, hvorfor det bør gjøres, men ikke hvordan. KS Bedrift Energi mener utelatelsen av dette hvordan er egnet til å skape forvirring heller enn oppklaring. Vi oppfordrer derfor NVE til å lage detaljert beskrivelse av hva selskapene bør gjøre, som inkluderes i veilederen på feltet.

Vi mener prinsippene i grunnsikringen for så vidt er bra, og gir en pekepinn på hvordan selskapene bør organisere sikkerhetsarbeidet. Samtidig er vi av den oppfattelse at kravet om å kartlegge leveranser og verdikjeder pålegger selskapene en betydelig byrde. Vi mener det også er unødvendig kompliserende å kreve at dokumentasjonen skal oppdateres minst en gang i året. Her mener vi NVE kan innføre en bestemmelse om at dokumentasjonen skal oppdateres ved *nyanskaffelser*.

Videre ønsker NVE å innføre en bestemmelse om at virksomheten, ved tjenesteutsetting, skal sørge for at sikkerhetsnivået opprettholdes. NVE henviser på dette punktet til IT-leverandører og digitale tjenestetilbydere.

KS Bedrift Energi mener at ettersom kravene til grunnsikring vil gjelde alle systemer for elektronisk kommunikasjon, og bransjen benytter seg av et stort antall leverandører for slike løsninger, vil kravet om at selskapene selv skal stå for sikkerhetsrevisjon av leverandører være krevende å etterfølge. En bestemmelse om at leverandører og tilbydere må være sertifiserte i henhold til ISO 27000-serien bør her være dekkende.

Vi ønsker å påpeke at det i fotnote vises til at «*tiltak for sikkerhetsnivå kan være at avtale med IKT-leverandør sikrer at NVE gis tilgang til opplysninger fra for eksempel tredjepartsrevisjon hos IKT-leverandøren, der NVE finner det nødvendig som et ledd i tilsynet med virksomheten*». KS Bedrift Energi tolker dette dithen at innsyn i tredjeparts revisjoner er tilstrekkelig for å kunne demonstrere at sikkerhetsnivået opprettholdes eller forbedres, men anbefaler at NVE gjør dette tydelig i veilederen for å unngå tvil.

I tillegg ønsker vi å påpeke at store skyleverandører generelt har høy sikkerhet i sine tjenester, men at disse av sikkerhetsgrunner ikke aksepterer at kunder gjennomfører egne revisjoner. Dette innebærer at dersom tredjeparts revisjonsrapport fra skyleverandører ikke aksepteres av NVE, forhindres kraftselskapene i å benytte store skyleverandører som Apple, Google og Microsoft. Om dette er tilfelle, vil det kunne være svært kostnadsdrivende for selskapene. Ettersom det generelt er ønskelig at selskapers kundekostnader skal holdes nede, er dette i strid med samfunnsøkonomisk aksepterte prinsipper. Her minner vi om at praksis for å akseptere tredjeparts revisjonsrapporter fra skyleverandørene er akseptert hos Datatilsynet.

Vi mener videre at NVE bør vurdere løsninger som leder mot akkreditering og bygger en felles kompetansebank for bransjen. En løsning vil kunne være å legge ansvar for å føre oppdaterte lister i KraftCert, og at disse gjøres tilgjengelige for kraftselskapene. Videre mener vi samarbeidsløsninger mellom ulike selskap kan bidra til å bygge kompetansemiljøer på sikkerhet. Her ønsker vi å påpeke at opprettelse av felles driftssentraler i så måte vil kunne tjene flere hensyn, deriblant etablering av rutiner for IKT-sikkerhet og revisjon av leverandører. Her mener KS Bedrift at NVEs oppdaterte retningslinjer for felles driftssentraler bidrar til å komplisere opprettelsen av slike driftssentraler. Vi oppfordrer derfor NVE til heller å best mulig tilrettelegge for opprettelsen av slike.

6.10 Sikring av bryterfunksjonalitet

NVE ønsker å sikre funksjonaliteten for bryting av strøm eller begrensning av effektuttak mot uønsket tilgang og manipulasjon, og ønsker dermed å innføre krav om sikring av AMS bryterfunksjonalitet.

Vi mener NVEs bruk av begrepet «adgangskontrollert sone» i §6-10 bør defineres bedre, ettersom begrepet slik det står i høringsdokumentet kan bety alt fra et kontorlandskap beskyttet av nøkkelkort, til en lukket nettverksone med separat tilgangskontroll. Videre kan begrepet tolkes i retning av et fysisk kontorlandskap med lukket nettverkskobling til informasjonssystemet. En slik løsning vil medføre en betydelig merkostnad sett opp mot dagens løsning, hvor man beskytter datatrafikk over åpent internett ved hjelp av kryptering. Det siste er i henhold til NVEs krav.

KS Bedrift Energi foreslår derfor at NVE endrer ordlyd til «fysisk adgangskontrollert sone».

Videre står det i samme paragraf at det skal være «nettselskap som har tillatelse til å utføre fjernstyring av bryterfunksjonalitet». KS Bedrift Energi tolker ordlyden dithen at det kun er

nettselskap som kan initiere fjernstyringen av bryterfunksjonaliteten, og at leverandøren kan bistå med dette så fremt handlingen er initiert av nettselskapet. Dette punktet bør tydeliggjøres i veilederen.

KS Bedrift Energi foreslår derfor at NVE endrer ordlyd til «kun nettselskap har tillatelse til å bestille fjernstyring av bryterfunksjonaliteten».

Vi mener leverandører med fjerntilgang til funksjonaliteten også bør kunne være lokalisert i land Norge har sikkerhetsavtale med. Krav om at kun EU/EØS-land skal være innenfor godkjente leverandørland fremstår som unødvendig strengt.

§ 7-12 Integrasjon mellom driftskontrollsystemer og andre informasjonssystemer

KS Bedrift Energi mener begrepet «integrasjon» bør defineres mer nøyaktig, eventuelt endres tilbake til «sammenkoblet». Begrepet kan tolkes fra å bety en fysisk kobling mellom to nettverkssoner for overføring av data begge veier, til tunnelering av data én vei ved at en nettverksport åpnes for utgående trafikk. Vi forstår NVE slik at tunnelering av data ut sannsynligvis vil være tillatt så lenge dataene ikke går direkte ut til åpent internett fra indre sone.

Vi foreslår at NVE endrer ordlyd til: «De deler av informasjonssystemet som er sammenkoblet med virksomhetens driftskontrollsystem skal sikres i henhold til driftskontrollsystemets klasse».

Med vennlig hilsen,

Asle Strand
Direktør KS Bedrift Energi

Audun Kolstad Wiig
Næringspolitisk rådgiver