Oslo, 12.mars 2018

Norges vassdrags- og energidirektoratet
nve@nve.no

Deres referanse: hjmy@nve.no

Vår referanse: Arvid Bekjorden

Innspill til uttalelse fra Distriktsenergi til NVEs høringsforslag til endringer i beredskapsforskriften.

Distriktsenergi organiserer 66 lokale energiverk.

Våre medlemsbedrifter arbeider hver dag – og langsiktig - med å ivareta sitt ansvar for forsyningssikkerhet. Bruk av digitale verktøy og løsninger er viktige virkemidler i arbeidet med å effektivisere drift, overvåke og raskest mulig gjenopprette strømforsyningen ved alle former for tenkbare skader. Det er viktig at reguleringen tilrettelegger for bruk av digitale løsninger og samarbeid om dette mellom selskapene i bransjen.

De vanligste årsakene til strømbrudd i Norge er tekniske feil og uværsskader. Så vidt vi kjenner til har det ikke vært hendelser i norsk energiforsyning som har medført alvorlige konsekvenser for forsyningssikkerheten i landet. Det er viktig å ha dette i betraktning i arbeidet med den samlede reguleringen av norsk energibransje. Distriktsenergi er samtidig opptatt av viktigheten av å være føre var. Våre medlemsbedrifter tar aktivt i bruk nye digitale verktøy, og IKT-systemene blir stadig viktigere for både å optimalisere investeringer og overvåke, styre og rette opp skader etter feil på anlegg. Verdien av å beskytte de digitale systemene blir stadig viktigere. Vi støtter således fullt ut NVEs understrekning av IKT-sikkerhet som *en integrert og viktig del av en helhetlig regulering* av bransjens arbeid med forebyggende sikkerhet og beredskap mot alle former for ekstraordinære hendelser.

I takt med dette tar også våre medlemsbedrifter aktivt tak i IKT-sikkerheten på egen hånd, både enkeltvis og i samarbeidskonstellasjoner. Distriktsenergi følger opp disse initiativene, og er opptatt av at NVE – og andre statlige myndigheter – like mye bidrar til å støtte opp under bransjeinitiativer som å stille krav og føre tilsyn. Vi tar derfor til orde for at det tas initiativ til en samlet strategi for kollektivt å løfte IKT-sikkerheten i bransjen, hvor regulering er et av flere virkemidler. Distriktsenergi benytter samtidig også anledningen til å si at vi gjennom flere år har satt pris på NVEs invitasjoner til å delta i ulike drøftinger om beredskap, og vi ønsker å bidra konstruktivt til å evaluere og videreutvikle den samlede virkemiddelbruken til å fremme vår felles interesse – god forsyningssikkerhet.

Distriktsenergi, Dronning Eufemiasgt. 16, 0191 Oslo tlf.: 911 87 713 epost.: post@distriktsenergi.no

Vi merker oss at NVE begrunner lemping av krav til produksjonsselskapene med at disse har en egeninteresse av å ivareta sikkerhet. Dette gjelder jo også for nettselskapene, og dette resonnementet mener vi det er viktig for NVE å legge til grunn fremover. Vi mener videre det er viktig at NVE som tilsynsmyndighet er spesielt oppmerksom på selskaper og tjenesteleverandører som mange er avhengige av, også ut fra prinsippet om at statlig tilsyn skal være tuftet på risiko og vesentlighet.
I NVEs videre bearbeiding av utkastet til endrede sikkerhets- og beredskapskrav er vi som bransjeorganisasjon **prinsipielt** opptatt av:

- Reguleringen må være forståelig, forutsigbar og fornuftig. Dette betyr bl.a. at kravene til IKT-sikkerhet og tiltak mot sikkerhetstruende hendelser må avveies mot andre viktige samfunnsinteresser og også balanseres mot andre sikkerhets- og beredskapsbehov. Det er avgjørende at kravene er forankret i sektorens egenart og differensieres ut fra størrelse / kritikalitet av de ulike anlegg og systemer. Det er således logisk at f.eks. driftskontrollsystemene klassifiseres ut fra antall innbyggere i forsyningsområdet til det enkelte selskap. Det er - og blir - stor forskjell mellom Statnett og Hafslund på den ene siden og f.eks. Luostejok kraftlag og Nore Energi på den andre siden. Denne forskjellen gjelder også muligheten til manuelt å overvåke, drifte og gjenopprette forsyningen hvis IKT-systemer skulle falle ut.

- Reguleringen – og ikke minst den statlige tilsynsvirksomheten – må være koordinert og kosteffektiv for bransjen det blir ført tilsyn med. Distriktsenergi har tidligere påpekt behovet for å samordne bedre tilsynsvirksomheten til DSBs Eltilsyn og NVE, og er fremover også opptatt av at staten må stokke sine bein godt i tilsyn med generell informasjonssikkerhet (NVE) og personvern (Datatilsynet). Vi forventer også at NVE i tilsynsvirksomheten aktivt følger opp leverandører av kritisk infrastruktur til hele bransjen, slik som Elhub, storleverandører av SCADA-tjenester og leverandører av kundesystemer og måledatainnsamlere som hele bransjen benytter seg av. Vi forventer spesielt at staten følger opp sikkerheten til systemer og selskaper som bransjen pålegges å knytte seg til, slik som Elhub.

- Like viktig som krav og tilsyn er det å bidra til kvalitets- og kompetanseløft i/til bransjen. Dette inkluderer også tiltak for å stimulere til utdanning av fremtidige IKT-eksperter til bransjen. Vi forstår det slik at NVEs fageksperter innen IKT-sikkerhet er opptatt av denne dimensjonen, og mener dette er noe som NVE bør oppmuntre og enda mer aktivt støtte opp om fremover.

- Vi forventer også at NVE som beredskapsmyndighet bidrar til gode rammebetingelser og trygghet for kvaliteten på kritiske tjenesteleveranser fra private selskaper. Meld. St. 38 (2016-2017) understreker viktigheten av egensikring og kompetanse innen hendelseshåndtering. Meldingen oppfordrer også til økt bruk av inntrengingstester for å avdekke sårbarheter og styrke sikkerheten. Vi merker oss at Nasjonal sikkerhetsmyndighet har etablert en kvaltetsordning for private leverandører som bistår med hendelseshåndtering ved IKT-hendelser. Vi ser dette prinsipielt som et positivt tiltak, og mener en slik ordning bør kunne utvides til også å omfatte bistand til sikkerhetstester av kritiske IKT-systemer i kraftforsyningen. Vi anser at alle

selskaper – fra de minste til de aller største – har nytte av slike tredjepartstester. Det er samtidig lite rasjonelt at alle selskaper må foreta nitidige undersøkelser i markedet på hvilke leverandører som driver seriøst, når der dette kan samordnes av en eller flere sentrale instanser.

Nedenfor kommenterer vi videre det vi oppfatter som **de vesentligste endringsforslagene** til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen. For enkelte av endringsforslagene mener vi at det er nødvendig å gå en runde til for å sikre en forsvarlig prosess og et rasjonelt regelverk.
Det er meget viktig at kravene er entydige og forutsigbare, samt at de administrative og økonomiske konsekvensene er tilstrekkelig belyst. Dette gjelder spesielt følgende endringsforslag som både er omfattende og – betinget av hvordan disse fortolkes – i betydelig grad utvider påleggene til bransjen i forhold til gjeldende beredskapsforskrift:

- **Forslag til ny § 6-9 om digitale informasjonssystemer**

På generelt grunnlag er Distriktsenergi opptatt av at medlemsbedriftene tar ansvar for å beskytte alle typer informasjonssystemer som inneholder personopplysninger og/eller sensitiv informasjon om kraftforsyningen.
Samtidig er vi opptatt av at nivået på beskyttelsen tilpasses virksomhetens størrelse og hvor mye sensitiv informasjon den enkelte virksomhet faktisk forvalter i forhold til å ivareta sikkerheten i kraftforsyningen som helhet.
Generelt mener vi at forslaget til ny § 6-9 vil skape stor usikkerhet om hva slags type tiltak som må implementeres, og hvor omfattende disse skal være. NVE viser til NSM sin veileder «NSMs grunnprinsipper for IKT-sikkerhet» som rettesnor for å etterleve kravene i bestemmelsen. Denne veilederen er svært omfattende, og meget ressurskrevende å følge helt ut. Vi stiller også spørsmål ved hvordan NVE tenker å følge opp bestemmelsen i tilsyn. Slik bestemmelsen i dag er formulert vil mye henge på hvordan denne fortolkes og anvendes i tilsyn.
Vi mener at bestemmelsen vil pålegge mange av våre medlemsbedrifter å implementere omfattende og ressurskrevende tiltak som ikke står i stil til hva bedriftene faktisk forvalter av informasjon og hvor kritiske de er for kraftforsyningen. Et eksempel gjelder punktene c) og d) i bestemmelsen som handler om å *sikre og oppdage* og *håndtere og gjenopprette*.
Sammenstilt oppfatter vi at disse kravene til å være tilnærmelsesvis lik bestemmelsen i § 7-14 c) om automatisk overvåking, logging, analyse og varsling ved unormal aktivitet i driftskontrollsystemet. Denne bestemmelsen gjelder med dagens regelverk for selskap med driftskontrollsystem i klasse 2, og som i den nye forskriften vil ha over 50 000 kunder. Når NVE foreslår at bestemmelsen skal gjelde for de virksomhetene som leverer eller produserer over 100 GWh energi i året, noe som tilsvarer et sted mellom 5 000 og 6 000 husholdninger, avhengig av type bolig, fremstår dette som krav til små bedrifter som er på linje med krav til virksomheter med driftskontrollsystem i klasse 2. Dette oppfatter vi som noe skjevt og vi kan ikke se at dette harmonerer med prinsippet om differensiering av kravene i forskriften som sådan.
Distriktsenergi mener at bestemmelsen bør deles opp og nivådeles slik det gjøres både i kapittel 5 og kapittel 7 i forskriften. Dette vil være i tråd med forskriftens oppbygging og

sørge for at pålagte sikkerhetstiltak er tilpasset virksomhetens funksjon og betydning for kraftforsyningen.

- **Forslag til endringer i § 7-12 om integrasjon mellom driftskontrollsystem og andre informasjonssystemer**

Integrasjon mellom driftskontrollsystem og øvrige informasjonssystem kan skje enten ved at systemene utveksler informasjon seg imellom, eller for eksempel ved at driftskontrollsystemet kun avgir informasjon uten å være i stand til å motta noe fra de systemene som driftskontrollsystemet har integrasjon mot.
Distriktsenergi er ikke uenig i at slike integrasjoner må sikres, men bestemmelsen fremstår som uklar, da det ikke er definert hva NVE mener med integrasjon. Det er heller ikke beskrevet i forarbeidene hva som menes med integrasjon. Dette vil medføre at våre medlemsbedrifter vil få store vanskeligheter med å tolke hva NVE faktisk mener med bestemmelsen, da definisjonen har innvirkning på sikkerhetstiltakene som må etableres.

Videre mener Distriktsenergi at denne bestemmelsen har en klar sammenheng med ny § 6-9, i den forstand at begrunnelsen for § 6-9 er at de fleste tilsiktede hendelser mot driftskontrollsystem har sitt opphav i administrative systemer. Vi mener da at kravet om sikring av *integrasjoner mellom driftskontrollsystem og andre informasjonssystem* og *sikring av digitale informasjonssystemer* bør være integrert, og at sikringen skal være tilsvarende driftskontrollsystemets klasse, jf. våre kommentarer til ny § 6-9. På denne måten ivaretas beredskapsforskriftens intensjon om differensiering av kravene basert på virksomhetenes funksjon og betydning for kraftforsyningen.
Ut over dette stiller vi spørsmål til enkelte av de andre bestemmelsene, som vi også forventer at NVE tar med i den videre bearbeidingen av endringsforslagene.

Særskilt om Kraft-CERT (ny § 3-6)
I den grad selskapene pålegges å varsle og/eller rapportere inn til Kraft-CERT må dette være formålstjenlig, staten må følge opp at leveransene utføres kosteffektivt og det må forventes at de som varsler og rapporterer også får noe av verdi tilbake.

Særskilt om pålegg om samarbeid med sikkerhetsmyndigheten (ny § 3-7)
Et pålegg om samarbeid med sikkerhetsmyndigheten (ny § 3-4) må være formålstjenlig. Vi legger til grunn at NVE er myndighet for alle tiltak som regulerer krav til forebyggende sikkerhet og beredskap. Vi oppfatter samtidig at man i begrepet «sikkerhetsmyndighet» i dette tilfellet mener Nasjonal sikkerhetsmyndighet. Det er svært viktig at dette beskrives og at det er forutsigbart hva som skal meldes til hvem, og videre hvem man skal forholde seg til i gitte situasjoner. Ansvarsforholdene må være entydige.
Vi regner med at man ikke trenger pålegg for å samarbeide med en statlig myndighet, og vi anerkjenner Nasjonal sikkerhetsmyndighet sin spesielle kompetanse innen IKT-sikkerhet. Et pålegg stiller imidlertid krav til tydelighet i forhold til *når* man er pliktig til å samarbeide, og *hva* samarbeidet faktisk innebærer. Det må samtidig forventes at et slikt samarbeid gir nytte tilbake til bransjen.
Vi peker på at det spesielt ved kritiske IKT-hendelser er behov for å gå opp kommunikasjons- og beslutningslinjene mellom den enkelte KBO-enhet, Kraftforsyningens distriktssjefer, NVE,

Kraft-CERT og Nasjonal sikkerhetsmyndighet. Skal samme informasjon til alle? Hva hvis rådene spriker? Hvem skal man forholde seg til? Det må i denne sammenhengen også legges vekt på at mange selskaper i bransjen samarbeider med private leverandører av tjenester for å fange opp og håndtere kritiske hendelser.

Særskilt om endring i § 6-2 om sensitiv informasjon
Generelt påpeker Distriktsenergi at kravene til beskyttelse av sensitiv informasjon er omfattende fra før. Det legges nå opp til at selskapene også skal skjerme hvor driftssentralene i klasse 2 og klasse 3 er. Dette kan på sikt også berøre enkelte av medlemsbedriftene våre. Vi har forståelse for at man skal beskytte beliggenheten til reserve driftssentraler, men stiller spørsmål ved om det er praktisk mulig effektivt å skjerme hvor de ordinære driftssentralene er. Vi er opptatt av at det skal være praktisk mulig – innenfor fornuftens grenser – å etterleve kravene, og stiller derfor spørsmål ved dette endringsforslaget. Vår innvending gjelder spesielt for driftssentraler i klasse 2.

Distriktsenergi har i tillegg til ovennevnte mottat innspill av mer teknisk karakter som vi her tar med i vårt høringssvar:

§6-9 Virksomheten skal minimum årlig gjennomføre sikkerhetsrevisjon av pålagte beskyttelsestiltak i det digitale informasjonssystemet

Kommentarer:

- Fotnote 12 side 41 viser til at «tiltak for sikkerhetsnivå kan være at avtale med IKT-leverandør sikrer at NVE gis tilgang til opplysninger fra f.eks tredjepartsrevisjon hos IKT-leverandøren der NVE finner det nødvendig som et ledd i tilsynet med virksomheten». Vi tolker dette dithen at tilgang til/innsyn i tredjeparts revisjoner er tilfredsstillende for å kunne demonstrere at sikkerhetsnivået opprettholdes eller forbedres.
- Vi anbefaler imidlertid at NVE tydeliggjør dette i veilederen for å unngå tvil.
- Vi viser til at de store skyleverandørene generelt har høy sikkerhet i sine tjenester ,- men at disse, bl.a. fra et sikkerhetsperspektiv, ikke aksepterer at kunder gjennomfører egne revisjoner. Dersom ikke tredjepartsrevisjonsrapport fra skyvleverandører aksepteres av NVE vil dette i praksis umuliggjøre å benytte store skyleverandører som Amazon, Google, Microsoft, noe som ville være uheldig fra et samfunnsøkonomisk perspektiv.
- Praksis om å akseptere tredjepartsrevisjonsrapporter fra skyleverandørene er akseptert hos datatilsynet.

Kap 9.7 Bryterfunksjonalitet i avanserte måle- og styringssystem (AMS) §6-10

Kommentarer:

- §6-10 a) Begrepet «adgangskontrollert sone» bør defineres mer nøyaktig. Begrepet kan tolkes fra å bety et kontorlandskap beskyttet av et nøkkelkort til en lukket nettverksone med separat tilgangskontroll.
- Begrepet kan videre tolkes dit at man mener et fysisk kontorlandskap med lukket nettverkskobling til informasjonssystemet for å sikre kilden til et kall. En slik tolkning vil medføre en betydelig merkostnad over dagens løsning hvor man beskytter datatrafikk over åpent internett ved hjelp av kryptering I henhold NSMs krav.
    - Forslag: Endre ordlyd til: «fysisk adgangskontrollert sone»

- §6-10 a) «kun nettselskap som har tillatelse til å utføre fjernstyring av bryterfunksjonalitet».
- Bestemmelsen er noe uklar. Vi tolker punktet slik at det er kun nettselskap som kan «initiere» fjernstyring av bryterfunksjonalitet, altså at leverandør kan bistå med dette såfremt det er «initiert» av nettselskapet. Dette bør tydeliggjøres i veilederen.
    - Forslag: Endre ordlyd til : «kun nettselskap som har tillatelse til å bestille å utføre fjernstyring av bryterfunksjonalitet»

Kap 10.9 Integrasjon mellom driftskontrollsystem og andre informasjonssystemer § 7-12

- § 7-12 begrepet «integrasjon» bør defineres mer nøyaktig eller endres tilbake til «sammenkoblet»
- Begrepet kan tolkes fra å bety fysisk kobling mellom to nettverkssoner for overføring av data begge veier til tunnelering av data en vei ved at en nettverksport åpnes for utgående trafikk. Det er sannsynlig at NVE mener kobling av nettverk (ikke tillat uten at andre systemer klassifiseres iht DMS). Tunnelering av data ut vil sannsynligvis være tillatt så lenge dataene ikke går direkte ut til åpen internett fra indre sone.
- Det bør være tydelig at «integrasjon» gjelder kun enveiskommunikasjon
- Er det bedre å beholde ordet «sammenkoblet»?
    - Forslag: Endre ordlyd til: «De deler av informasjonssystemet som er sammenkoblet med virksomhetens driftskontrollsystem skal sikres i henhold til til driftskontrollsystemets klasse»

Avslutning

Sikkerhet og beredskap er et kjerneområde for alle bedrifter i norsk energiforsyning. Distriktsenergi og våre medlemsbedrifter er opptatt av å opprettholde og videreutvikle den samlede kraftforsyningsberedskapen. Distriktsenergi er opptatt av at NVE viderefører sitt sterke engasjement om forebyggende sikkerhet og beredskap i energiforsyningen. Dette betyr også at staten samlet må tilrettelegge for at det gjennom den økonomiske rammereguleringen gis rom for å gjøre nødvendige investeringer, og at det stimuleres til FoU-aktiviteter. Vi er også opptatt av at det i reguleringen må gis rom til både å fortsette – og der dette er rasjonelt – utdype samarbeidsordninger mellom selskapene. Slikt samarbeid kan for eksempel gjelde felles driftssentralløsninger.
Distriktsenergi imøteser videre dialog, og stiller gjerne opp i både møter med NVE og i andre fora for å bidra til ytterligere felles løft for IKT-sikkerheten i vår bransje.

Mvh

Knut Lockert

Daglig leder
DistriktsEnergi