Energistyrelsen
Att.: Lasse Hallundbæk
Mail: lshk@ens.dk

Dok. ansvarlig: PHA
Sekretær:
Sagsnr.: s2023-647
Doknr: d2023-19871-4.0
14-06-2023

Ekstern høring af Network Codes on sector-specific rules for cybersecurty aspects of cross-border electricity flows (NCCs) (ENS Id nr.: 3163352)

Green Power Denmark takker for muligheden for at kommentere på EU kommissionens udkast til sektorspecifik network code for cybersikkerhed for el-sektoren.

Green Power Denmark anerkender vigtigheden af, at der på tværs af Europa, på tværs af lande og på tværs af aktører, som ejer og driver elnet, produktions- og forbrugsanlæg og/eller som agerer som serviceleverandører til el-sektoren bør samarbejdes om opretholdes af en høj forsynings- og leveringssikkerhed i den europæiske el-system.

I forhold til udkastet til network code vil vi fra Green Power Denmarks side gerne pege på følgende temaer, som værende væsentlige for os, at der skabes mere klarhed omkring:

- Omfattede virksomheder og udpegning heraf
- Network coden bør holde fokus på ondsindet cyberaktivitet
- Videndeling bør gælde både for virksomheder og myndigheder
- Mere klarhed for virksomheder med grænseoverskridende aktivitet
- Netselskabernes omkostninger til håndtering af cybersikkerhed og risici forbundet hermed

Ovenstående temaer er uddybet i de følgende afsnit.

Omfattede virksomheder og udpegning heraf
Network coden definerer alene hvilken type af virksomheder, som er omfattet af network coden, men ikke hvilken størrelse af virksomheder/aktører, som er omfattet. Det er essentielt for det videre arbejde med network coden og implementeringen heraf, at der hurtigst muligt skabes klarhed om, præcist hvilke virksomheder som bliver omfattet af network coden og hvordan at virksomhederne bliver omfattet (læs: som ”high-impact” eller som ”critical impact”) samt hvorvidt der indføres en nedre tærskelværdi for, hvornår og hvorvidt en virksomhed er omfattet af network coden.

Network coden bør holde fokus på ondsindet cyberaktivitet
Artikel 17 og artikel 19 i network coden omhandler risikovurdering ud fra hhv. et EU- og et regionalt perspektiv. Disse to artikler kan læses sådan, at en risikovurdering skal dække alle typer af IT-hændelser, hvilket vi i Green Power Denmark finder uhensigtsmæssigt, idet et mere bredt sigte på IT-hændelser

allerede er en del af den risikovurdering, som må forventes at følge af NIS2-direktivet. Vores anbefaling er derfor, at network coden fokuserer på egentlig ondsindet cyberaktivitet, hvilket også var fokus for de tidligere udkast af network coden udarbejdet af ENTSO-E og DSO Entity.

Formålet med network coden er grænseoverskridende aktivitet og dermed bredere end NIS2 (hvor fokus er på virksomhedsniveau), hvorfor det i vores optik vil være uhensigtsmæssig dobbeltregulering, hvis network coden og NIS2 skal regulere de samme risici, hvis eneste forskel ellers er at network coden er grænseoverskridende. Network coden bør anskues som en "overligger" til NIS2.

Videndeling bør gælde både for virksomheder og myndigheder
I Green Power Denmark finder vi det ekstremt vigtigt, at myndigheder og virksomheder deler væsentlig hændelsesinformation med hinanden, særligt hvis der er tale om egentlig ondsindet cyberaktivitet. Deling af hændelsesinformation er efter vores bedste overbevisning den eneste måde, at virksomhederne kan agere proaktiv mod potentielle hændelser. Ligger myndighederne inde med relevant viden bør denne information derfor deles proaktivt.

I det udkast til network code, som ACER sendte til EU Kommissionen i juli 2022 var myndighedernes videndeling med "high-impact" og "critical impact"-enheder en del af udkastet til network code (artikel 40). Denne myndighedsopgave synes nu skrevet ud af EU Kommissionens udkast til ordlyd (artikel 37), hvilket i Green Power Denmarks optik efterlader branchen med en uhensigtsmæssig "envejs-kommunikation", hvor det kun er virksomhederne som forpligtiges til at rapportere hændelser til den nationale, kompetente myndighed, men ikke den anden vej (læs: at de kompetente myndigheder forpligtes til at dele deres information med virksomhederne), hvilket vi vurderer kan få omfattende konsekvenser, hvis relevant information ikke bibringes virksomhederne i rette tid.

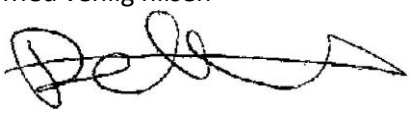
Derfor mener vi, at myndigheder også bør pålægges at dele relevant information med virksomhederne, evt. i anonymiseret form.

Virksomheder med grænseoverskridende aktivitet
I Green Power Denmarks medlemskreds har vi flere medlemmer, som har grænseoverskridende aktiviteter. For disse virksomheder er det vigtigt, at der snarest muligt skabes klarhed over, hvilke roller, opgaver og ansvar, som de enkelte medlemsstater tildeler til hvilke myndigheder eller andre nationale aktører. Dette gælder både ift. implementering af network coden og ift. NIS2.

Netselskabernes omkostninger til håndtering af cybersikkerhed og risici forbundet hermed
Med en ny kommende network code for cybersikkerhed bør det sikres, at netselskaberne kan få dækket de ekstraomkostninger, som implementering af network coden vil give anledning til.

I Green Power Denmark står vi naturligvis til rådighed for uddybende kommentarer til ovenstående.

Med venlig hilsen



Peter Kjær Hansen
pha@greenpowerdenmark.dk
Dir. tlf. +45 20 90 77 79