

Energistyrelsen
Carsten Niebuhrs Gade 43
1577 København V

Sendt til: dcis-energi@ens.dk

Dok. ansvarlig: PHA
Sekretær: SLS
Sagsnr.: s2022-423
Doknr: d2022-312453-4.0
01-04-2022

Høringssvar vedr. cyber- og informationssikkerhedsstrategi for energisektorerne 2022-2025

Green Power Denmark takker for muligheden for at afgive høringssvar på udkast til ny cyber- og informationssikkerhedsstrategi for energisektorerne gældende for perioden 2022-2025.

Vores høringssvar og bemærkninger er opdelt i generelle bemærkninger efterfulgt af bemærkninger til de enkelte initiativer i høringsudkastet til strategien.

Generelle bemærkninger

Dialog med og inddragelse af branchen i udvikling af strategien

Green Power Denmark støtter og anerkender, at Energistyrelsen inddrager os som brancheorganisation og vores medlemmer i udviklingen af en cyber- og informationssikkerhedsstrategi for energisektorerne. Inddragelsen er et vigtigt udgangspunkt for at sikre, at strategien indeholder og behandler temaer og problemstillinger, som er relevante for både myndigheder og for branchen. Med inddragelse – både den, som allerede er sket, og også den, vi fortsat håber, vil ske – er der gode chancer for, at senere implementering kan ske målrettet og omkostningseffektivt. Inddragelse er også med til at sikre sektorernes medejerskab til strategien, herunder også den ledelsesmæssige fokus og opbakning.

Sikkerhed har en pris: Hvilket sikkerhedsniveau og hvilken robusthed skal energisektorerne stile efter?

Green Power Denmark ønsker at henlede Energistyrelsens opmærksomhed på, at cyber- og informationssikkerhed kommer med en pris, og at pris og kvalitet hænger sammen.

Green Power Denmark finder det derfor vigtigt, at Energistyrelsen inviterer sektorerne til en drøftelse af, hvilken sikkerhed og robusthed der ønskes i energisektorerne. I forhold til det aktuelle trussels- og situationsbillede i Europa og mod øst og i lyset af den løbende udvikling i cybertruslen og fortsat digitalisering af energisektorerne opfordrer vi til en nærmere, fælles drøftelse og analysearbejde af, hvilket sikkerhedsniveau og hvilken robusthed energisektorerne og andre samfundskritiske sektorer i Danmark skal stile efter.

I forhold til netselskabernes økonomiske rammer finder Green Power Denmark det vigtigt, at Energistyrelsen er tydelig på, hvilke økonomiske rammer et fremtidigt sikkerhedsarbejde ift. cyber- og informationssikkerhed skal udfoldes inden for. Det drejer sig om både muligheder og begrænsninger for den løbende trusselvurdering, indførelse af standardiserede ledelsessystemer, styrket sikkerhedsarkitektur, løbende netværksmonitorering, udbredelse af sikkerhedskultur og uddannelse af medarbejdere mv. Vi finder det også vigtigt, at Energistyrelsen sikrer, at netselskaberne kan foretage de nødvendige investeringer inden for cyber- og informationssikkerhed og kan få dækket deres omkostninger hertil i det omfang, at et givent sikkerhedsniveau og ønsket robusthed tilsiger dette.

Bemærkninger til de enkelte initiativer

Initiativ 1: Strategisk udvikling af EnergiCERT

Indledningsvis vil vi for god ordens skyld henlede opmærksomheden på, at EnergiCERT er et uafhængigt og uvildigt fagligt kompetencecenter, som er etableret som forening på privatretligt grundlag. EnergiCERT er etableret og udviklet med udgangspunkt i de tilsluttede virksomheders behov. Dette princip forventer vi også gælder og anerkendes fremadrettet.

Green Power Denmark er som medejer af EnergiCERT åben for løbende dialog med Energistyrelsen om EnergiCERT's fortsatte udvikling og herunder om Energistyrelsen kan være med til at sikre finansiering af eventuelle nye opgaver til EnergiCERT.

I initiativet foreslås oprettet et OT-observatørkorps. I Green Power Denmark stiller vi os tvivlende over for dette delinitiativ, idet vi ser et ikke-uvæsentligt overlap til den hændelsesrapportering og -evaluering, som energivirksomhederne allerede i dag er underlagt krav om jf. BEK 2646 og BEK 2647. Vi opfordrer i stedet til, at evt. ønske om øget videndeling og udbredelse af læring om hændelser og øvelser tænkes ind i initiativ 6 og 10 med udgangspunkt i den viden, som Energistyrelsens beredskabstilsyn ligger inde med historisk og i fremtiden.

Green Power Denmark bakker op om vigtigheden af det tværsektorielle DCIS-samarbejde, herunder indblik i og forståelse af sektorernes gensidige afhængigheder. Green Power Denmark indgår gerne i en nærmere dialog herom.

Initiativ 2: OT-sikkerhedsforum

Green Power Denmark anerkender, at der i dag er mangel på ekspertviden og kompetencer i relation til OT-sikkerhed. Af samme grund finder vi det vigtigt, at de sparsomme OT-kompetencer – på tværs af sektorer – som findes, fokuseres om det væsentlige. Green Power Denmark er bekendt med, at der i dag findes en række fora, arbejdsgrupper og udvalg. Herunder er det vigtigt at understrege, at OT-sikkerhed er kerneområdet for EnergiCERT, og derfor vil branchen foretrække at prioritere de sparsomme ressourcer på området i samarbejdet med EnergiCERT.

Vi ser derfor på nuværende tidspunkt ikke umiddelbart behov etablering af ét eller flere nye fora. Vi foreslår i stedet, at Energistyrelsen – gerne sammen med andre sektormyndigheder, herunder Center for Cybersikkerhed – beskriver og uddyber, hvilket behov I ser ift. jeres myndighedsrolle og sektoransvarsprincippet. Green Power Denmark indgår gerne i en efterfølgende drøftelse herom mhp. at bistå Energistyrelsen med viden og indsigt på OT-sikkerhedsområdet.

Initiativ 3: Risiko- og sårbarhedsvurderinger

Green Power Denmark bakker op om, at vurdering af risici og sårbarheder er grundlaget for, at energisektorens virksomheder kan arbejde ud fra en risikobaseret tilgang. Denne tilgang bør fastholdes fremadrettet.

Initiativ 4: Politikker for cyber- og informationssikkerhed

I Green Power Denmark noterer vi os, at der i initiativet står, at der *"... i de kommende år vil blive stillet mere omfattende krav i form af bl.a. lovgivning til energiselskabers virksomhedspolitikker på cybersikkerhedsområdet."*

Vi opfordrer Energistyrelsen til at sikre, at nye og mere omfattende krav sker ud fra en risikobaseret tilgang, at der sikres passende frister for implementering af disse nye krav, og at energiselskabernes økonomiske rammer levner plads til disse nye og mere omfattende krav. Det er samtidig vigtigt, at evt. nationale krav på området er afstemt i forhold til krav fra EU på området.

Initiativ 5: Krisestyring og videreførelse af forretningen

Green Power Denmark indgår gerne i en videre dialog om delinitiativerne nævnt herunder.

Initiativ 6: Øvelser

Green Power Denmark anerkender vigtigheden af, at energisektorerne er beredt på den dag, en cybersikkerhedshændelse indtræffer, hvad enten det er mindre/lokale, større regionale eller nationale sikkerhedshændelser. Afholdelse af øvelser udgør et vigtigt træningselement i den sammenhæng. Green Power Denmark bakker derfor op om nødvendigheden af afholdelse af øvelser, men henleder dog opmærksomheden på, at der allerede i dag er krav om løbende afholdelse af øvelser jf. BEK 2646 og BEK 2647, og at afholdelse af øvelser derfor allerede er en opgave, som virksomhederne gennemfører og lever op til. Der bør derfor ikke indføres et parallelt øvelses-setup.

Initiativ 7: Sektorberedskabsforanstaltninger

Green Power Denmark bakker op om udvikling af en fælles forståelse for kritikalitetsniveauer ved en cyberhændelse samt udvikling af cyberberedskabsforanstaltninger. Dog ser vi, at kritikalitet bør ses i sammenhæng med det enkelte energiselskabs risikovillighed og dermed en vurdering af sandsynlighed og konsekvens. Vi anbefaler derfor, at der i stedet arbejdes med beredskabsniveauer snarere end kritikalitetsniveauer. Vi opfordrer til, at udviklingen heraf sker i tæt dialog med os og vores medlemsvirksomheder, herunder EnergiCERT.

Initiativ 8: Cybersikkerhed i leverandørforhold

Green Power Denmark anerkender vigtigheden af leverandørsikkerhed. Vi bakker op om vigtigheden af et fokus på IoT/IIoT-udstyr, som er i direkte eller indirekte forbindelse med el- og energisystemet.

Initiativ 9: Uddannelse, kompetencer og adfærd

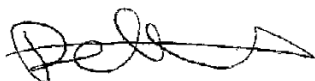
Green Power Denmark har allerede i dag stor fokus på uddannelse, kompetencer og rekruttering af tekniske eksperter til branchen og specialister inden for IT-, OT- og cybersikkerhed. Uddannelse af bestyrelsesmedlemmer og virksomhedsledelser er også et fokusområde for os. Vi indgår gerne i en dialog om de initiativer, vi til dato selv har gennemført, og hvordan vi i fællesskab fremadrettet kan målrette indsatsen. Vi opfordrer derfor til, at Energistyrelsen med strategien ikke lægger sig endeligt fast på, hvilke uddannelsesinitiativer der skal igangsættes.

Initiativ 10: Opsamling af og arbejde med viden og data

Green Power Denmark bakker op om dette initiativ. Vi opfordrer til, at arbejdet sker i tæt samarbejde med os og vores medlemsvirksomheder.

Green Power Denmark står naturligvis til rådighed for en uddybning af vores bemærkninger.

Med venlig hilsen

A handwritten signature in black ink, appearing to read 'Peter Kjær Hansen', with a long horizontal stroke extending to the right.

Peter Kjær Hansen
Afdelingschef Netanalyse

Green Power Denmark