



Klima-, Energi- og Forsyningsudvalget  
Christiansborg  
1240 København K

Ministeren

Dato  
23-01-2025

J nr. 2022 - 1944

Akt-id 581535

## Svar L 111 – spm. 4

Klima-, Energi- og Forsyningsudvalget har i brev af d. 9. januar 2025 stillet mig følgende spørgsmål om L 111 Forslag til lov om styrket beredskab i energisektoren, som jeg hermed skal besvare. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF)

### Spørgsmål 4

Det fremgår af høringsnotatet til lovforslaget - men desværre ikke af fremstillingen af lovforslaget - at lovforslaget indebærer en overimplementering af CER-direktivet og NIS2-direktivet. Der kan f.eks. henvises til høringssvarene fra Dansk E-mobility, Vestas og Green Power Denmark jf. L 111 – bilag 1 »Eksterne hørings-svar« side 27, 32, 91 og 460. Vil ministeren oversende en liste over krav, der går videre end de to EU-direktiver med en begrundelse for indførelsen af hvert af disse ekstra krav og en vurdering af hvert af disse krav i forhold til den byrde, der pålægges virksomhederne.

### Svar

Med lovforslaget og den udmøntende bekendtgørelse om modstandsdygtighed og beredskab i energisektoren, som er sendt i offentlig høring den 16. december 2024, foreslås der indført en række krav, som Klima-, Energi- og Forsyningsministeriet vurderer går videre end kravene i NIS 2- og CER-direktivet.

Der foreslås indført krav inden for 12 områder. Det bemærkes, at enkelte af disse områder i et vist omfang overlapper med NIS2- og CER-direktivet. Kravene foreslås indført med henblik på at øge energisektorens robusthed. Kravene er primært målrettet de mest forsyningskritiske virksomheder, som er tildelt niveau 4 og 5, og vurderes at være proportionale. De 12 områder er oplistet nedenfor, ligesom formålet er beskrevet.

#### 1. Alarmberedskab

Det foreslås, at virksomheder i niveau 4 og 5 skal have alarmer på deres forsyningskritiske anlæg, der sikrer, at virksomhederne i realtid kan opdage og regere

Klima-, Energi- og  
Forsyningsministeriet

Holmens Kanal 20  
1060 København K

T: +45 3392 2800  
E: kefm@kefm.dk

www.kefm.dk



på fx indbrud eller opdage visse former for spionage uanset bemanning af anlæget.

Formålet er, at virksomhederne har bedre forudsætninger for at opdage og reagere på fx spionage eller indbrud på anlæg i tide.

## *2. Netværkssikkerhed*

Der foreslås indført krav til virksomhedernes netværkssikkerhed. Virksomhedernes netværk skal være enten logisk eller fysisk segmenteret. Det betyder i praksis, at virksomhedens forsyningskritiske net- og informationssystemer isoleres fra andre net- og informationssystemer og udstyr, og at virksomheden bl.a. skal have dokumentation for netværkssegmenteringen. Krav om fysisk segmentering er afgrænset til virksomheder i niveau 4 og 5.

Formålet er bl.a. at sikre, at et cyberangreb ikke kan sprede sig og påvirke energiforsyningen.

## *3. Fjernadgang*

Der foreslås indført krav til virksomhedernes brug af fjernadgang. Virksomhederne skal sikre, at fjernadgange til virksomhedens net- og informationssystemer skal tildeles i en tidsbegrænset periode, så fjernadgange kun er åbne i tidsrum med et godkendt arbejdsbetinget behov for at tilgå et system, og at virksomheder skal udarbejde konkrete procedurer til at kunne opdage og håndtere cyberangreb mod fjernadgange til forsyningskritiske net- og informationssystemer.

Formålet er at sikre styring af fjernadgange, samt at der er procedurer for at kunne opdage og håndtere fx misbrug af fjernadgange.

## *4. Beskyttelse af mobile enheder og servere*

Der foreslås indført krav om, at virksomhederne skal forholde sig sikkerhed på mobile enheder og servere, fx PC, telefoner og tablet. Fx skal enheder være adgangskodebeskyttet, softwareopdateret og evt. beskyttet mod virus.

Formålet er at sikre et højt cybersikkerhedsniveau for mobile enheder og servere og minimere angrebsflader.

## *5. Kryptering*

Der foreslås indført krav om, at Energistyrelsen kan fastsætte nærmere regler for brug af kryptering ved autentificering, fx login.

Formålet er at sikre, at følsomme oplysninger bliver krypteret og beskyttet i forhold til både fortrolighed og integritet.



#### *6. Logs til reaktion på hændelser*

Der foreslås indført krav om, at virksomheder, skal have en logpolitik, der som minimum beskriver generering, lagring, analyse og anvendelse af logs. Desuden foreslås indført en hjemmel til, at Energistyrelsen kan fastsætte regler for systemunderstøttelse og regler om, hvor lang tid logs skal gemmes.

Formålet er at sikre, at virksomhederne har logs, som kan anvendes bl.a. ved cyberhændelser.

#### *7. Proaktiv monitorering af logs og redundans*

Der foreslås indført krav om, at virksomheder løbende skal monitorere logs og være i stand til at opdage uregelmæssigheder samt regelmæssigt teste om redundante systemer og backupløsninger er funktionelle.

Formålet er at sikre, at virksomhederne anvender logs aktivt, og har fx overblik over datatrafik på virksomhedens netværk.

#### *8. Geografisk placering af drift*

Der foreslås indført krav om, at virksomheder i niveau 4 og 5 skal placere servere og datacentre, der understøtter virksomhedens forsyningskritiske net- og informationssystemer, inden for EU/EØS/EFTA-lande eller i andre lande med en tilstrækkelighedsafgørelse fra EU.

Formålet med kravet er bl.a., at der for kritiske systemer ikke skabes afhængigheder, som kan sætte energiforsyningen under pres, fx i tilfælde af ændret geopolitisk situation.

#### *9. Risiko- og sårbarhedsvurderinger*

Der foreslås indført krav om, at virksomheden skal udarbejde risiko- og sårbarhedsvurderinger for indkøb, design og etablering af energiinfrastruktur. Virksomheder skal fx ved indgåelse af nye kontrakter og opstart af nye projekter relateret til energiforsyningen udarbejde risiko- og sårbarhedsvurderinger.

Formålet er bl.a., at virksomhederne forpligtes til en helhedsorienteret tilgang til styring af risici, sårbarheder og leverandører.

#### *10. Ledelsesansvar*

Der foreslås indført krav om, at virksomhedernes ledelse skal underskrive virksomhedens risiko- og sårbarhedsvurderinger, beredskabsplan, Energistyrelsens tilsynsrapport og efter relevans leverandørkontrakter.

Formålet er at sikre et tydeligt ledelsesansvar for sikkerhed og beredskab samt en helhedsorienteret tilgang til styring af risici, sårbarheder og leverandører.



#### *11. Beredskabsøvelser*

Der foreslås indført krav om at sikre, at forsyningskritiske leverandører inddrages eller deltager i beredskabsøvelser.

Formålet er at sikre, at virksomhederne forpligtes til en helhedsorienteret tilgang til styring af risici, sårbarheder og leverandører.

#### *12. Beredskabsrevision*

Der foreslås indført hjemmel til, at Energistyrelsen kan pålægge virksomheder at få foretaget ekstern revision af virksomhedens beredskab.

Formålet er, at Energistyrelsen kan reagere på væsentlige afvigelser og i særlige tilfælde kan pålægge virksomheden ekstern beredskabsrevision, hvor Energistyrelsen vælger revisor.

Med venlig hilsen

Lars Aagaard