



Til høringsparterne på vedlagte liste

Kontor/afdeling
Beredskab

Dato
16-12-2024

J nr. 2024 - 6493

Høring over udkast til bekendtgørelse om modstandsdygtighed og beredskab i energisektoren

Energistyrelsen sender hermed udkast til bekendtgørelse om modstandsdygtighed og beredskab i energisektoren i høring.

Energistyrelsen skal venligst anmode om eventuelle høringssvar **snarest muligt** og **senest torsdag den 23. januar 2025 kl. 13.00.**

Høringssvaret bedes sendt enten pr. mail til beredskab@ens.dk eller som post til Center for beredskab, Carsten Niebuhrs Gade 43, 1577 København, med angivelse af journalnummer **2024 - 6493**.

Bekendtgørelsen ventes udstedt med hjemmel i lov om styrket beredskab i energisektoren, som i øjeblikket er under behandling i Folketinget¹. Loven forventes at træde i kraft den 1. marts 2025 under forudsætning af, at lovforslaget vedtages. Bekendtgørelsens udstedelse er betinget af, at Folketinget vedtager lovforslaget.

Baggrund

Klimaforandringer, den grønne omstilling på energiområdet og teknologiske udviklinger har de seneste år ændret rammerne for energisektorens beredskabsarbejde. Derfor er der behov for at opdatere eksisterende beredskabsregulering, så energisektoren som helhed er modstandsdygtig overfor relevante risici, hvad enten de er naturlige eller menneskeskabte, hændelige eller tilsigtede.

Denne bekendtgørelse konsoliderer eksisterende bekendtgørelser for alment beredskab og it-beredskab for henholdsvis el-, naturgas- og oliesektoren². Bekendtgørelsen implementerer samtidig en række tiltag til at styrke modstandsdygtighed og beredskab i energivirksomheder, herunder foranstaltninger som følger af NIS 2- og CER-direktiverne.

Koordinering med Ministeriet for Samfundssikkerhed og Beredskab

Ministeriet for Samfundssikkerhed og Beredskab har med den kongelige resolution af 29. august 2024 overtaget det overordnede ansvar for implementeringen af NIS 2- og CER-

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

Niels Bohrs Vej 8
6700 Esbjerg

T: +45 3392 6700
E: ens@ens.dk

www.ens.dk

¹ Fremsatte lovforslag findes på [Folketingets hjemmeside](https://www.folketinget.dk).

² Bekendtgørelse nr. 2646 af 28/12/2021 om beredskab for elsektoren, bekendtgørelse nr. 821 af 14/08/2019 om beredskab for naturgassektoren, bekendtgørelse nr. 424 af 25/04/2018 om beredskab for oliesektoren og bekendtgørelse nr. 2647 af 28/12/2021 om it-beredskab for el- og naturgassektoren.



direktiverne fra Forsvarsministeriet. Implementeringen af direktiverne i Danmark sker ved, at Ministeriet for Samfundssikkerhed og Beredskab fremsætter to hovedlovforslag, der implementerer henholdsvis NIS 2- og CER-direktiverne for størstedelen af de sektorer, der er omfattet af henholdsvis NIS 2- og CER-direktivernes anvendelsesområde. Energisektoren omfattes ikke af hovedlovforslagene. For energisektoren implementeres NIS 2- og CER-direktiverne i stedet særskilt gennem L 111 om forslag til lov om styrket beredskab i energisektoren, som blev fremsat for Folketinget den 4. december 2024. For at sikre en vis ensartethed og koordination mellem reglerne i hovedlovforslagene og reguleringen i energisektoren, er kravene i L 111 om forslag til lov om styrket beredskab i energisektoren indtil ressortomlægningen koordineret med Forsvarsministeriet og herefter med Ministeriet for Samfundssikkerhed og Beredskab.

Det følger af bl.a. §§ 6 og 8 i L 111 forslag til lov om styrket beredskab i energisektoren, at den nærmere fastsættelse af krav vedrørende beredskabsplanlægning, passende organisatoriske foranstaltninger og cybersikkerhedsforanstaltninger skal ske efter forhandling med ministeren for samfundssikkerhed og beredskab. Formålet med forhandlingen er bl.a. at sikre, at der ikke fastsættes modstridende krav i relation til NIS 2-direktivet for henholdsvis energisektoren og de øvrige sektorer, der er omfattet af direktivet. Det bemærkes, at forhandlingerne med ministeren for samfundssikkerhed og beredskab om relevante bestemmelser i udkastet til bekendtgørelse endnu ikke er afsluttet. Det kan derfor ikke udelukkes, at der kan forekomme justeringer i udkastet til bekendtgørelse efter den offentlige høring.

Implementering af NIS 2- og CER-direktiverne i energisektoren

Energistyrelsen vurderer det hensigtsmæssigt, at foranstaltninger efter NIS 2- og CER-direktiverne implementeres i energisektoren med én bekendtgørelse, som også konsoliderer eksisterende regler for beredskab. Det skyldes, at et effektivt beredskab forudsættes af en holistisk tilgang, hvorfor virksomheders organisatoriske beredskab, fysiske sikkerhed og cybersikkerhed skal spille sammen på tværs af organisationen.

Nuværende regler om beredskab, fysisk sikring og cybersikkerhed efter eksisterende bekendtgørelser overlapper på flere områder med NIS 2- og CER-direktiverne. Derfor konsolideres eksisterende bekendtgørelser så vidt muligt i henhold til direktiverne, hvilket indebærer en række sproglige præciseringer og juridiske korrektioner. Præciseringer af eksisterende regler skal også sikre, at foranstaltninger implementeres på den måde, hvorved det er intention, da et forholdsvis stort fortolkningsrum i nuværende regler har medført, at virksomheders foranstaltninger ikke altid bidrager positivt til energisektorens modstandsdygtighed og beredskab.

Dertil indføres nye regler om en række foranstaltninger, som supplerer NIS 2- og CER-direktiverne, og som er særligt rettet mod yderligere at højne energisektorens modstandsdygtighed og beredskab. Behovet herfor skal ses i forhold til, at energisektoren er en særlig kritisk sektor, hvor hændelser kan skabe kaskadeeffekter i andre kritiske sektorer i samfundet, som er afhængig af en stabil energiforsyning.



Energistyrelsen skal gøre opmærksom, at der er en række europæiske og internationale regelværk og forpligtelser, som virksomheder i energisektoren skal efterleve sideløbende med reglerne i denne bekendtgørelse, herunder netværkskoden om cybersikkerhed inden for elsektoren (NCCS).

Energistyrelsen skal også gøre opmærksom på, at høringen af denne bekendtgørelse sker parallelt med høringen af udkast til bekendtgørelse om Energistyrelsens gebyrer efter lov om styrket beredskab i energisektoren. Bekendtgørelse om udvidet baggrundskontrol og sikkerhedsgodkendelse i energisektoren som bl.a. implementerer foranstaltninger om passende medarbejderstyring efter CER-direktivets artikel 13, stk. 1, litra e. Der afventes en endelig høringsdato herpå.

Indhold

Nedenstående afsnit har fokus på hovedpunkterne i den nye bekendtgørelse, herunder væsentlige ændringer af eksisterende regler for virksomheder omfattet af bekendtgørelse nr. 2646 af 28/12/2021 om beredskab for elsektoren, bekendtgørelse nr. 821 af 14/08/2019 om beredskab for naturgassektoren, bekendtgørelse nr. 424 af 25/04/2018 om beredskab for oliesektoren og bekendtgørelse nr. 2647 af 28/12/2021 om it-beredskab for el- og naturgassektoren.

Niveauinddeling af virksomheder og klassificering af anlæg

Bekendtgørelsen lægger op til, at Energistyrelsen niveauinddeler virksomheder og klassificerer anlæg ud fra en femtrinsskala, hvor niveau 5-virksomheder og klasse 5-anlæg anses som mest kritiske for energiforsyningen (§§ 4-9). Niveau 1-virksomheder omfatter mindre virksomheder, som vurderes relevante for forsyningssikkerheden på lokalt niveau, mens niveau 5-virksomheder omfatter virksomheder af betydning for energiforsyningen på internationalt niveau. Dette er en ændring af eksisterende regler for el- og naturgassektoren, hvor Energistyrelsen kategoriserer virksomheder og klassificerer anlæg i tre kategorier, og hvor virksomheder i kategori 1 og anlæg i klasse 1 anses som mest kritiske for energiforsyningen.

Ovenstående bestemmelser gør det muligt i bekendtgørelsen at præcisere bestemmelser, som sikrer proportionalitet mellem omfanget af lovpligtige foranstaltninger og virksomheders forsyningsmæssige kritikalitet. Niveau 1-virksomheder omfattes eksempelvis udelukkende af bestemmelser om at have et grundlæggende beredskab i form af en beredskabsplan og et operationelt kontaktpunkt (§ 5).

Energistyrelsen afgør virksomheders og anlægs kritikalitet ud fra den samlede mængde af energi, som en virksomhed eller et anlæg producerer eller håndterer, ud fra tærskelværdierne i bekendtgørelsens bilag 1 og 2. For virksomheder med anlæg, vil virksomhedens niveau ofte modsvare anlæggenes klassificering, medmindre virksomhedens anlæg tilsammen producerer eller håndterer en energimængde, som falder inden for tærskelværdierne til en højere niveauinddeling. Energistyrelsen kan endvidere placere virksomheder og anlæg i et



højere trin, hvis virksomheden eller anlægget er leverandører til slutbrugere, der udgør kritisk infrastruktur i andre sektorer (§ 4, stk. 5, og § 6, stk. 5).

Energistyrelsen niveauiddeler virksomheder og klassificerer anlæg hvert tredje år eller ved væsentlige ændringer, som eksempelvis fusioner eller når anlæg tages i eller ud af drift permanent, hvilket virksomheder skal melde ind til Energistyrelsen (§ 9). Energistyrelsen skal gøre opmærksom på, at der internt vil blive arbejdet på at indhente oplysninger, som virksomheder allerede indberetter til Energistyrelsen i andre sammenhænge, fx i forbindelse med ansøgninger om bevillinger.

Organisatorisk beredskab

Bekendtgørelsen lægger op til en videreførelse af eksisterende regler for organisatorisk beredskab, som de finder anvendelse for el- og naturgassektoren. Det indebærer, at virksomheder skal foretage beredskabsplanlægning, hvor der først skal udarbejdes et planlægningsgrundlag i form af fortegnelser over anlæg, systemer og informationsstrømme (§§ 14-17) samt en risiko- og sårbarhedsvurdering (ROS) relateret til virksomhedens evne til at levere sine tjenester (§ 18). Virksomheder skal på denne baggrund udarbejde beredskabsplaner til at kunne håndtere hændelser og styre kriseindsatsen (§ 19), som skal sendes til Energistyrelsen sammen med konklusionerne fra deres ROS i henhold til faste tidsintervaller (§ 107). Beredskabsplanerne skal indeholde procedurer af operativ karakter for håndtering af hændelser, og er med til at implementere CER-direktivets artikel 13, stk. 1, litra c og d.

Energistyrelsen skal bemærke, at der i bekendtgørelsen ikke skelnes mellem alment beredskab og it-beredskab, hvilket indebærer, at præcisering af indholdet i beredskabsplaner (§ 19) retter sig mod hændelser på såvel anlæg som i net- og informationssystemer. Dette vil være en ændring for virksomheder omfattet af eksisterende regulering for el- og naturgassektoren, hvor alment beredskab og it-beredskab har været reguleret i hver sin bekendtgørelse. Hensigten er at fremme et beredskab, der planlægges og udføres på koordineret vis på tværs af organisationen.

Energistyrelsen finder det også hensigtsmæssigt at ændre eksisterende regler om sikringsplaner samt planmateriale for forsyningskritiske it-systemer og informationsstrømme således, at disse ikke indgår som en del af virksomheders beredskabsplaner, men i stedet præciseres som en særskilt planlægningsaktivitet i form af fortegnelser (§§ 14-17). Det skal hertil bemærkes, at § 9 fra BEK 424 om beredskab for oliesektoren udgår.

Bekendtgørelsen lægger op til, at virksomheder skal øve deres beredskabsplaner i henhold til en femårig øvelsesplan (§ 20), hvilket er en videreførelse af eksisterende praksis for el- og naturgassektoren og en justering af den nuværende treårige øvelsesperiode for oliesektoren. Øvelsesplaner kan gælde for en kortere tidsperiode, så længe virksomheden kommer igennem alle relevante øvelseselementer i bekendtgørelsens bilag 4 i løbet af en femårig periode.



Virksomheder i niveau 3-5 skal som minimum gennemføre øvelser på årlig basis, mens virksomheder i niveau 2 som minimum skal foretage øvelser hvert andet år. Energistyrelsen finder det hertil hensigtsmæssigt at præcisere regler om øvelser således, at virksomheder med forsyningskritiske systemer skal øve genetablering af disse systemer på årlig basis.

Bekendtgørelsens §§ 20-23 om øvelser og øvelsesplaner understøtter implementering af CER-direktivets artikel 13, stk. 1, litra f, og er en videreførelse af eksisterende bekendtgørelser med enkelte præciseringer og justeringer. Det bemærkes, at § 19, stk. 4, i BEK 2647 om it-beredskab for el- og naturgassektoren udgår.

Bekendtgørelsen lægger op til, at virksomheder hertil skal udpege faste personer til at koordinere beredskabsplanlægningen på tværs af det klassiske beredskab, cyberberedskab og fysisk sikring forankret på anlæg (§ 11). Dette er en videreførelse og præcisering af eksisterende regler for el- og naturgassektoren, om end den it-beredskabsansvarlige og sikringsansvarlige omdøbes til henholdsvis en cyberkoordinator og sikringskoordinator.

For at have en effektiv risiko- og beredskabskultur forudsættes det, at der i virksomheden er en høj sikkerhedsbevidsthed. Medarbejdere er ofte første forsvarslinje, når det kommer til forebyggelsen af hændelser, hvorfor manglende sikkerhedsbevidsthed om eksempelvis usikre links i mails eller påvirkningsforsøg kan gøre virksomheder sårbare over for især cyberangreb.

Bekendtgørelsen lægger derfor op til, at virksomheder skal gennemføre årlige awareness-tiltag, som fremmer og opretholder medarbejderes kendskab til såvel beredskabsplaner, fysisk sikkerhed og cybersikkerhed (§ 26). Virksomheder skal også sikre, at medarbejdere, som udfører opgaver inden for virksomhedens organisatoriske beredskab, fysiske sikring og cybersikkerhed, opretholder de nødvendige kompetencer, herunder også ledelsen (§§ 24 - 26). Med bestemmelserne implementeres CER-direktivets artikel 13, stk. 1, litra f, og NIS 2-direktivets artikel 21, stk. 2, litra g.

Nye krav til risikostyring

Bekendtgørelsen indeholder bestemmelser rettet mod at fremme en risikostyringskultur, hvilket indebærer at virksomheder gennemfører risikovurderinger og foranstaltninger til styring af risici, som står i forhold til de foreliggende risici. Ansvar for herfor ligger i vid udstrækning hos virksomhederne selv, hvorfor virksomheder efter de nye regler skal have en politik for risikostyring til at formalisere rammerne for styring af risici, der kan forstyrre eller forhindre leveringen af virksomhedens tjenester (§ 18).

Politikken skal bl.a. beskrive de risikovurderingsmetoder, virksomheder anvender til at risikovurdere sikkerheden i net- og informationssystemer og den fysiske sikkerhed på anlæg. Det skal hertil bemærkes, at bekendtgørelsen ikke eksplicit forholder sig til anvendte risikovurderingsmetoder, da virksomheder i energisektoren anvender forskellige standarder for risikostyring.



Politikken implementerer NIS 2, artikel 21, stk. 2, litra a, som primært sigter på at beskytte net- og informationer og disses fysiske miljø, om end Energistyrelsen vurderer det hensigtsmæssigt at udvide politikken indhold til også at skulle inkludere metoder for kritiske enheders risikovurdering, som følger af CER-direktivets artikel 12. På denne måde er risikopolitikken med til at fremme en holistisk tilgang til risikostyring, hvormed der forebygges silotænkning i virksomheders sikkerheds- og beredskabsarbejde.

Risikovurderinger af forsyningskritiske projekter

Bekendtgørelsen lægger op til nye regler om risikostyring i forbindelse med projekter af betydning for forsynings sikkerheden. Antallet og kompleksiteten af projekter, som kan påvirke virksomheders evne til at levere deres tjenester, er steget markant i takt med den grønne omstilling og den stigende digitalisering af energisektoren. Derfor indføres nye bestemmelser om risikovurderinger af projekter, så virksomheden træffer foranstaltninger til at styre risici (§ 25), og så Energistyrelsen bliver bekendt med de risici, der er forbundet med projekterne (§ 26).

De nye regler indebærer, at virksomheder ved opstart af projekter udarbejder og vedligeholder en risikovurdering med det formål, at virksomheden tidligst muligt og løbende forholder sig til og håndterer sikkerhedsmæssige risici forbundet til projektet.

Nye krav til forsyningskædesikkerhed

Eksisterende bekendtgørelser indeholder allerede regler om leverandørstyring i energisektoren, herunder at virksomheder i forhold til deres leverandører skal bevare ejerskab for forsyningskritiske og fortrolige data samt have procedurer for leverandørers fjernadgange til forsyningskritiske systemer. Alle eksisterende regler videreføres i den nye bekendtgørelse.

Dertil indføres nye regler om, at virksomheder skal have procedurer til at sikre forsyningskædesikkerhed for så vidt angår de produkter og tjenester, der anvendes i leveringen af deres tjenester (§ 29). Virksomheder skal i denne forbindelse have metoder til at sikre, at risikovurderinger af eksempelvis et net- og informationssystem, som virksomheden anskaffer, forholder sig til relevante leverandørrisici. Virksomheder skal hertil forholde sig til, om en leverandør har passende foranstaltninger, der står i forhold til de foreliggende risici, så vidt angår de leverede produkter og tjenester.

Virksomheder skal på denne baggrund rette krav til sikkerhed og beredskab i forbindelse med indgåelse af en leverandøraftale (§ 30), hvor virksomheder bl.a. skal sikre, at foranstaltninger til at styre risici samt rapporteringsforpligtelser, som bekendtgørelsen pålægger virksomheden, i relevant omfang indgår som leverandørkrav. Bekendtgørelsen lægger samtidig op til, at virksomheder skal forholde sig til, hvordan deres leverandører over for virksomheden kan dokumentere efterlevelse af de krav, som der stilles i leverandøraftalen (§ 30).

Det skal bemærkes, at der kan være tilfælde, hvor det ikke er muligt at stille direkte krav til en leverandør, som eksempelvis ved serviceaftaler for systemer og ydelser, virksomheder



erhverver som færdige løsninger. I disse tilfælde forventes det, at virksomheder forholder sig til det sikkerhedsniveau, som leverandøren udbyder, herunder kvaliteten af eventuelt integrerede foranstaltninger i systemet. Dette er med til at implementere NIS 2, artikel 21, stk. 3.

Bestemmelserne i §§ 29-32 er med til at implementere NIS 2-direktivets artikel 21, stk. 2, litra d, der tilsigter at virksomheder skal have foranstaltninger til at sikre forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende et leverandørforhold.

Energistyrelsen skal bemærke, at nye regler om leverandørkontrakter efter § 30-32 ikke vil have bagudvirkende effekt. Virksomheder skal derfor først forholde sig til de nye kontraktregler, når eksisterende aftaler skal genforhandles.

Energistyrelsen er hertil bevidst om, at det kan være en udfordring for virksomheder at stille leverandørkrav efter bekendtgørelsen for så vidt angår især industrielle kontrolsystemer, hvortil der er begrænsede system- og serviceleverandører. Det forventes, at virksomheder på sigt vil blive hjulpet på vej af anden supplerende regulering herom, herunder Cyber Resilience Act. Virksomheder skal dog fortsat forholde sig til leverandørrisici i leveringen af deres tjenester i kraft af deres procedurer forsyningskædesikkerhed i leverandørforhold (§ 29).

Ledelsens ansvar

Bekendtgørelsen lægger op til, at virksomheders risikoaccept og beredskab fastlægges af virksomhedens ledelse, som bl.a. skal forholde sig til og godkende risiko- og sårbarhedsvurderinger samt beredskabsplaner og tilsynsrapporter (§ 10), hvorfor ledelsen også skal opbygge og fastholde de nødvendige kompetencer til at træffe disse beslutninger (§ 24). Bestemmelserne implementeres NIS 2-direktivets artikel 20, stk. 1 og 2.

Dertil videreføres eksisterende regler for el- og naturgassektoren, hvor ledelsen i dag skal koordinere med beredskabskoordinatoren og den it-beredskabsansvarlige fire gange årligt, så ledelsen har et samlet overblik over de risici, som beredskabsplaner skal baseres på.

Energistyrelsen anerkender, at det kan blive en udfordring for større og komplekse virksomheder at implementere nye regler om ledelsesansvar. Energistyrelsen skal derfor bemærke, at ledelsen anses for at være de personer, som kan gøres ansvarlige over for topledelsen, bestyrelsen eller ejerne for beslutninger i henhold til bestemmelserne i denne bekendtgørelse, og som derudover har beføjelser til at tildelte økonomi, personale og andre ressourcer til at udføre opgaverne.

Nye krav til klimasikring og fysisk sikring af anlæg

Bekendtgørelsen lægger op til, at der indføres nye regler for klimasikring og fysisk sikring af forsyningskritiske anlæg i energisektoren (§§ 36-43), så virksomheder i højere grad bliver i stand til at forebygge, opdage og reagere på mistænkelig aktivitet eller hændelser i realtid. Bestemmelserne er med til at implementere CER-direktivets artikel 13, stk. 1, litra a-c, om end



Energistyrelsen finder det hensigtsmæssigt at præcisere reglerne for især den fysiske sikring (§ 37 og § 38).

I dag gælder regler om fysisk sikring kun for de mest forsyningskritiske anlæg i el-, naturgas- og olie-sektoren, såfremt anlægget er ubemandet, hvilket ikke vurderes tilstrækkeligt i forhold til at sikre en modstandsdygtig energisektor. Derfor skal der fremover foretages fysisk sikring af alle anlæg i klasse 3-5, hvilket omfatter styret adgangskontrol, sikring til at forsinke og besværliggøre fysisk indtrængen på anlæg samt elektronisk overvågning til at opdage forsøg på indtrængen, herunder forsøg på sabotage, indbrud og tyveri. Virksomheder med anlæg i klasse 4 og 5 skal dertil have elektronisk overvågning til at verificere forsøg på indtrængen.

Energistyrelsen skal bemærke, at der i bekendtgørelsen udelukkende opstilles kriterier for, hvad den fysiske sikring skal kunne understøtte samt placeringen af den fysiske sikring. Der vil være metodefrihed i forhold til sikringsforanstaltningernes udformning, hvorfor typen af eksempelvis overvågnings- og alarmløsninger vil afhænge af virksomheders egne risikovurderinger.

De nye krav til klimasikring og fysisk sikring af anlæg indebærer, at virksomheder forventes at investere i yderligere sikringsforanstaltninger for at kunne efterleve de nye regler. Der forventes derfor at være omstillingsomkostninger forbundet med især klimasikring af anlæg, hvilket følger af CER-direktivet. Det forventes dog også, at flere virksomheder i energisektoren allerede har eller er ved at implementere de nødvendige tiltag til at kunne efterleve reglerne for den fysiske sikring.

Det følger af bekendtgørelsens § 124, at virksomheder skal have implementeret eller være i gang med at implementere klimasikring af anlæg i klasse 2-5 inden marts 2026, mens virksomheder skal have implementeret eller være i gang med at implementere øvrig fysisk sikring inden marts 2027.

Nye krav til cybersikkerhed

Bekendtgørelsen lægger op til, at der indføres nye regler til at understøtte sikkerheden i net- og informationssystemer, som virksomheder anvender i leveringen af deres tjenester, jf. § 8 i lov om styrket beredskab.

Minimumsimpliciteringen af NIS 2-direktivet indebærer, at foranstaltninger, som følger af direktivet, omfatter alle de net- og informationssystemer, som virksomheder anvender i leveringen af deres tjenester. Dette er en ændring fra eksisterende regulering, hvor regler for cybersikkerhed udelukkende finder anvendelse på forsyningskritiske it-systemer.

Foranstaltninger rettet mod at understøtte sikkerheden i net- og informationssystemer medvirker til at implementere NIS 2-direktivets artikel 21. Øvrige supplerende foranstaltninger til at højne cybersikkerheden i energisektoren finder anvendelse på forsyningskritiske net- og informationssystemer, forstået som operationelle teknologier (OT), industrielle



kontrollsystemer og informationsteknologier (IT) med mulighed for direkte at påvirke styringskritiske funktioner i et produktionsmiljø.

Det følger af NIS 2-direktivets artikel 21, stk. 2, litra i, at væsentlige og vigtige enheder skal implementere foranstaltninger til at forvalte aktiver, hvilket Energistyrelsen anser som en forudsætning for at kunne styre risici for sikkerheden i net- og informationssystemer. Derfor indføres nye regler om styring af hardware- og softwareaktiver, som indgår i eller kan tilgå virksomheders net- og informationssystemer (§ 48). Aktivstyringen skal bl.a. understøtte virksomheders evne til at identificere enheder på netværket (§ 69) og til at identificere sårbarheder (§ 47).

Virksomheder skal dertil sikre, at aktiverne hærdes (§ 46) og konfigureres på sikker vis (§ 49), så angrebsfladen for cyberangreb mod energisektoren mindskes til mindst muligt. Samtidig indføres nye EU-regler om anvendelsen af multifaktorautentifikation (§ 53) og kryptering (§ 60 og § 61), sammen med regler om adgangsstyring til at understøtte grundlæggende cyberhygiejnepraksisser i energisektoren. Bestemmelserne i §§ 52, 54 og 55 er med til at implementere NIS 2- direktivets artikel 21, stk. 2, litra g-j.

Dertil videreføres nuværende regler for fjernadgange, hvor virksomheder omfattet af eksisterende regulering skal have en række procedurer til at styre fjernadgange, som udgør en væsentlig angrebsvinkel for cyberangreb mod energisektoren. Reglerne præciseres således, at fjernadgange kun må være åbne i det tidsrum, hvor der er et behov, (§ 55, stk. 2), ligesom mobile enheder, som kan tilgå forsyningskritiske systemer, ikke må anvendes til privat brug.

Bekendtgørelsen viderefører også eksisterende regler for sårbarhedsstyring, som i dag gælder for el- og naturgassektoren, hvor virksomheder bl.a. skal videreformidle oplysninger af sikkerhedsmæssig betydning for energisektoren. Nuværende regler opdateres i henhold til NIS 2-direktivets artikel 21, stk. 2, litra e, så virksomheder skal tage stilling til, om sårbarheder bør offentliggøres (§ 47). Videreformidlingen af sårbarheder skal sikre, at kritiske sårbarheder for energisektoren, som potentielt eksisterer hos mange virksomheder, belyses, så virksomheder kan reagere med rettidig omhu.

De nye og præciserede regler om cybersikkerhed i energisektoren kan indebære, at virksomheder, som ikke allerede har foranstaltninger til at understøtte implementeringen af de nye regler, vil skulle foretage investeringer i nye løsninger, som kan understøtte eksempelvis aktiv- og sårbarhedsstyring eller adgangs- og identitetsstyring for henholdsvis deres IT- og OT-miljøer.

Bekendtgørelsen lægger op til, at virksomheder i niveau 4 og 5 skal placere servere og datacentre, som har relation til forsyningskritiske systemer, inden for EU/EØS-jurisdiktion (§ 50). På denne måde er adgang til og drift af forsyningskritiske systemer kun underlagt EU/EØS-regulering, hvilket skal medvirke til at forebygge afhængigheder, der kan sætte energiforsyningen under pres i tilfælde af eksempelvis geopolitiske ændringer.



Bekendtgørelsen lægger endvidere op til, at virksomheder skal foretage netværkssegmentering, så produktionsmiljøet med forsyningskritiske systemer isoleres fra andre interne netværk. Netværk skal segmenteres ved brug af en demilitariseret zone (DMZ) til at skabe en sikker mellemzone mellem produktionsmiljøet og øvrige netværk. Dette skal reducere risikoen for, at et angreb mod administrative systemer kan få indvirkning på forsyningskritiske processer på anlæg. For virksomheder i niveau 4 og 5 gælder det, at segmenteringen skal ske fysisk, hvilket indebærer, at forsyningskritiske systemer placeres på separate fysiske lokationer eller adskilte zoner inden for samme facilitet. Nye regler om netværkssegmentering indebærer, at virksomheder, som ikke allerede har segmenteret produktionsmiljøet, vil skulle foretage investeringer herom.

Det følger af NIS 2-direktivets artikel 21, stk. 2, litra b, at virksomheder har foranstaltninger til kunne håndtere hændelser. Det forudsætter, at der indføres regler om etablering af logning og monitorering i virksomheders net- og informationssystemer og netværksinfrastruktur, så virksomheder kan identificere og reagere på eventuelle hændelser (§§ 64-70). Energistyrelsen vurderer det hertil hensigtsmæssigt at præcisere reglerne for virksomheder i niveau 4 og 5, herunder at virksomhederne skal kunne reagere på uregelmæssigheder i realtid.

Bekendtgørelsen viderefører eksisterende regler om it-sikkerhedstjenesten (§§ 33-25), som i dag gælder for el- og naturgassektoren. It-sikkerhedstjenesten er en intern eller udliciteret funktion, som foretager eksempelvis monitorering af logs samt bistår virksomheders risikostyring med nyeste oplysninger om relevante cybertrusler og sårbarheder. Reglerne for it-sikkerhedstjenesten præciseres, så it-sikkerhedstjenesten bidrager til energisektorens beredskab efter hensigten. Det skal hertil bemærkes, at § 25, stk. 5 og 6, udgår fra BEK 2747 om it-beredskab for el- og naturgassektoren.

Erhvervsøkonomiske konsekvenser

Nye regler for organisatorisk beredskab, fysisk sikkerhed og cybersikkerhed, som følger af bekendtgørelsen, vil medføre erhvervsøkonomiske konsekvenser for både monopolvirksomheder og private virksomheder. Erhvervsstyrelsens område for Bedre Regulering og Energistyrelsen har derfor foretaget en vurdering af de erhvervsøkonomiske konsekvenser for erhvervslivet. Erhvervsstyrelsens vurdering af de administrative konsekvenser er dog ikke færdigafsluttet, hvorfor der for nuværende ikke er et endeligt samlet estimat. Derfor eftersendes samlede tal for bekendtgørelsens erhvervsøkonomiske konsekvenser for erhvervslivet.

Ikrafttrædelse

Bekendtgørelsen forventes at træde i kraft fra 1. marts 2025. I bekendtgørelsen er der enkelte overgangsbestemmelser for større foranstaltninger, som eksempelvis fysisk sikring og netværkssegmentering. Dette fremgår af kapitel 21, § 124.



Øvrige oplysninger

Udkastet til bekendtgørelse er sendt i høring hos de høringsparter, der fremgår af vedlagte høringsliste.

Der tages i bekendtgørelsen forbehold for lovtekniske ændringer.

Der vil blive afholdt tre sektormøder for omfattede virksomheder fra energisektoren. Disse afholdes henholdsvis den 10. januar 2025 kl. 9.00 til 12.00 samt den 13. januar 2025 kl. 12.30 til 15.30 i Energistyrelsen, Carsten Niebuhrs Gade 43

1577 København V. Tilmelding kan ske via: [Sektormøde: Lov om styrket beredskab i energisektoren \(den 10. januar\) | Energistyrelsen](#) og [Sektormøde: Lov om styrket beredskab i energisektoren \(den 13. januar\) | Energistyrelsen](#).

Der vil ligeledes blive afholdt et arrangement i Energistyrelsen, Niels Bohrs Vej 8D 6700 Esbjerg den 15. januar kl 13.30 til 16.30. Tilmelding kan ske via: [Sektormøde: Lov om styrket beredskab i energisektoren \(den 15. januar\) | Energistyrelsen](#).

Deltagelsen er forbeholdt de berørte virksomheder.

Eventuelle spørgsmål til udkastet til bekendtgørelse kan rettes til beredskab@ens.dk.

De modtagne høringssvar vil blive offentliggjort på Høringsportalen. Ved afgivelse af høringssvar samtykkes til offentliggørelse af høringssvaret, herunder afsenders navn og mailadresse. Det bemærkes, at høringssvar vil blive oversendt til Folketingets Klima-, Energi- og Forsyningsudvalg.

Med venlig hilsen

Jesper Rode Tholstrup
Kontorchef i Energistyrelsen, Center for Beredskab