BEK nr 425 af 01/05/2018 (Gældende) | **Udskriftsdato: 28. februar 2019**

Ministerium: Energi-, Forsynings- og Klimaministeriet
Journalnummer: Energi-, Forsynings- og Klimamin., Energistyrelsen, j.nr. 2017-1546

Senere ændringer til forskriften
BEK nr 1367 af 28/11/2018

Bekendtgørelse om it-beredskab for el- og naturgassektorerne[1)]

I medfør af § 69, stk. 5, § 85 c, stk. 5 og 6, § 90 og § 92 i lov om elforsyning, jf. lovbekendtgørelse nr. 114 af 9. februar 2018, og § 15 b, stk. 5 og 6, § 52 og § 54 i lov om naturgasforsyning, jf. lovbekendtgørelse nr. 1157 af 6. september 2016, som ændret ved lov nr. 1755 af 27. december 2016, fastsættes efter bemyndigelse i henhold til § 4, stk. 1, i bekendtgørelse nr. 1512 af 15. december 2017 om Energistyrelsens opgaver og beføjelser, fastsættes:

Generelle bestemmelser

§ 1. Denne bekendtgørelse har til formål at fastsætte regler om it-beredskabet for it-systemer, der er kritiske for produktion eller forsyning af elektricitet eller naturgas. Disse forsyningskritiske it-systemer skal sikres, således at forsyningen og produktionen i videst muligt omfang kan opretholdes og videreføres i tilfælde af en it-sikkerhedshændelse.

§ 2. Denne bekendtgørelse finder anvendelse på:
1) Virksomheder, som er bevillingspligtige efter §§ 10 og 19 i lov om elforsyning.
2) Virksomheder, som er bevillingspligtige efter § 10 i lov om naturgasforsyning.
3) Energinet og et af Energinet's helejede datterselskaber.
4) Balanceansvarlige virksomheder.

Stk. 2. Virksomheder omfattet af stk. 1 skal foretage foranstaltninger for at minimere risikoen for forsyningsnedbrud og begrænse eventuelle konsekvenser af nedbrud i eller angreb på forsyningskritiske it-systemer.

Definitioner

§ 3. I denne bekendtgørelse forstås ved:
1) Balanceansvarlige virksomheder: Virksomheder, der yder balancerende tjenester til energisystemet efter aftale med Energinet, og som har styring over fysiske anlæg til produktion, hvad enten denne kontrol udøves direkte eller gennem andre virksomheder.
2) Forsyningskritiske processer: Processer, der er nødvendige for forsyning af en eller flere slutforbrugere.
3) It-sikkerhedstjeneste: En virksomhed, der varetager it-sikkerhedsmæssige opgaver for andre virksomheder.
4) It-beredskab: Foranstaltninger, processer og det arbejde, der skal forhindre, begrænse eller håndtere skader og forsyningssvigt som resultat af nedbrud, forstyrrelser eller angreb på el- og naturgassektorernes kritiske it-systemer.
5) It-sikkerhedshændelse: En hændelse, hvor et nedbrud i eller angreb på et forsyningskritisk it-system i væsentligt omfang aktiverer virksomhedens it-beredskab.
6) Forsyningskritisk it-system: Et it-system, der styrer eller i væsentligt omfang påvirker forsyningskritiske processer.

Koordinerende og operative forhold

§ 4. Virksomheder, jf. § 2, stk. 1, er ansvarlige for eget it-beredskab, herunder at omsætte informationer om it-sikkerhedstrusler og konkrete it-varsler til nødvendige tiltag i egen organisation.

Stk. 2. Virksomheder, der af geografiske eller tekniske årsager er afhængige af andre virksomheders it-systemer, skal sikre, at denne afhængighed ikke medfører komplikationer for virksomhedens håndtering af it-beredskabets operative og planlægningsmæssige opgaver.

Stk. 3. Virksomheder i kategori 1 og 2, jf. § 9, stk. 1, nr. 1 og 2, skal sikre, at der er mulighed for it-sikkerhedsmæssig assistance på alle tider af døgnet. Virksomhederne er ansvarlige for at vurdere, hvilken assistance der er relevant i den pågældende virksomhed.

§ 5. Energinet skal varetage de overordnede koordinerende opgaver i forbindelse med håndtering af it-beredskabshændelser, der omfatter flere virksomheder.

Stk. 2. Energinet skal etablere et formaliseret samarbejde om it-beredskabsforhold, der har til formål at fremme koordineringen af såvel planlægningen som udøvelsen af it-beredskabet.

Stk. 3. Energinet skal bistå virksomheder, jf. § 2, stk. 1, nr. 1, 2 og 4, med kontaktoplysninger til andre virksomheder eller relevante myndigheder i en akut situation.

Stk. 4. Energinet skal bistå virksomhederne med oplysninger om aktuelle driftstilstande m.v. til brug for virksomhedernes håndtering af it-beredskabshændelser.

Stk. 5. Energinet skal til enhver tid kunne modtage og videreformidle informationer af betydning for it-beredskabet for virksomheder, jf. § 2, stk. 1.

Organisatoriske forhold

§ 6. Virksomheder, jf. § 2, stk. 1, skal udpege en it-beredskabsansvarlig medarbejder, som er ansvarlig for at koordinere virksomhedens sikring af forsyningskritiske it-systemer, herunder risiko- og sårbarhedsvurdering.

Stk. 2. Virksomhederne skal sikre, at it-beredskabsarbejdet og det almene beredskabsarbejde koordineres, således at virksomhedens ledelse har et samlet risikobillede, der repræsenterer kendte og mulige risici mod produktionen eller forsyningen af elektricitet eller naturgas.

Stk. 3. Virksomhederne skal fire gange årligt koordinere mellem den ansvarlige for det almene beredskab (beredskabskoordinatoren), jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren, den it-beredskabsansvarlige og ledelsen. Virksomheden skal på Energinet's forlangende dokumentere denne koordination.

Stk. 4. Der må ikke være personsammenfald mellem den it-beredskabsansvarlige, beredskabskoordinatoren og ledelsen i virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1.

Stk. 5. Virksomheder placeret i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, kan ansøge Energinet om tilladelse til personsammenfald.

§ 7. Virksomheder, jf. § 2, stk. 1, nr. 1, 2 og 4, skal organisere it-beredskabet, således at det sikres, at virksomheden kan modtage it-sikkerhedsvarsler. Virksomhederne skal på baggrund af egne risiko- og sårbarhedsvurderinger etablere den fornødne organisering, der kan iværksætte relevante tiltag ved modtagelse af et it-sikkerhedsvarsel.

§ 8. Energinet skal vejlede virksomhederne i forbindelse med etablering af procedurer for modtagelse af trusselsvurderinger og varsler.

Kategorisering af virksomheder

§ 9. Virksomhederne, jf. § 2, stk. 1, inddeles i tre kategorier:

1) Kategori 1: Virksomheder, der producerer eller forsyner energimængder på nationalt niveau, der forvalter et forsyningsområde med over 250.000 slutforbrugere, eller virksomheder, der håndterer energimængder over 600 MWh/h elektricitet eller over 100.000 Nm3/time.

2) Kategori 2: Virksomheder, der producerer eller forsyner energimængder på regionalt niveau, der forvalter et forsyningsområde med mellem 30.000 og 250.000 slutforbrugere, eller virksomheder, der håndterer energimængder svarende mellem 100 MWh/h og 600 MWh/h elektricitet inden for en sammenhængende del af elsystemet eller mellem 10.000 Nm3/time og 100.000Nm3/time.
3) Kategori 3: Øvrige virksomheder, der ikke er omfattet af kategori 1 eller 2.

Stk. 2. Virksomheder, der ejer eller driver anlæg klassificeret som af væsentlig betydning for den nationale forsyning, jf. stk. 1, nr. 1, eller regionale forsyning, jf. stk. 1, nr. 2, tilhører tilsvarende kategori. Virksomheder, der driver eller ejer anlæg klassificeret af hensyn til el- eller naturgassektorens almene beredskab, vil således følge denne klassificering, med mindre det kan godtgøres, at anlægget ikke anvender forsyningskritiske it-systemer.

Stk. 3. I tilfælde, hvor der er uoverensstemmelse mellem kategoriseringen ud fra antallet af aftagere og energimængde, samt i tvivlstilfælde kategoriseres virksomheder i den kategori, der stiller mest omfattende krav til virksomhederne.

Stk. 4. Balanceansvarlige virksomheder placeres i kategori efter, hvilken energimængde de forvalter efter deres aftale med Energinet. Såfremt en balanceansvarlig virksomhed kan godtgøre, at en andel af den samlede produktions- eller forbrugskapacitet ikke kan styres, og derved ikke kan udgøre en risiko for forsyningen, kan denne mængde fratrækkes den balanceansvarlige virksomhedes samlede energimængde.

Stk. 5. Energinet træffer afgørelse om, hvilken kategori virksomhederne tilhører. Energinet reviderer årligt, og senest den 1. februar, kategoriseringen. Første gang senest den 1. august 2017. Virksomhederne, Energistyrelsen og Energitilsynet underrettes herom.

Risiko- og sårbarhedsvurderinger

§ 10. Virksomheder, jf. § 2, stk. 1, skal udarbejde en vurdering af relevante risici og sårbarheder, der kan påvirke virksomhedens forsyningskritiske it-systemer.

Stk. 2. Risiko- og sårbarhedsvurderinger skal indeholde alle relevante forhold, herunder egne erfaringer fra øvelser og hændelser, jf. §§, 19 og 22, samt trusselsvurderinger fra Center for Cybersikkerhed og den tilknyttede it-sikkerhedstjeneste, jf. § 25.

Stk. 3. Risiko- og sårbarhedsvurderinger skal udarbejdes med inddragelse af relevante personer i organisationen, herunder personer, men ikke begrænset til personer med ansvar for det almene beredskab og it-beredskabet. Risiko- og sårbarhedsvurderingen skal integreres i virksomhedens samlede risikobillede.

Stk. 4. Risiko- og sårbarhedsvurderingen skal opdateres, når nye risici, trusler eller sårbarheder erkendes samt ved væsentlige ændringer af it-systemer eller trusselsbilledet. Virksomhederne skal på Energinet's forlangende kunne dokumentere, hvordan og hvornår risiko- og sårbarhedsvurderingen er opdateret.

Stk. 5. Virksomheder skal første gang fremsende konklusionerne fra denne risiko- og sårbarhedsvurdering til modtagelse hos Energinet senest den 1. oktober 2017.

Stk. 6. Risiko- og sårbarhedsvurderinger skal forevises ved tilsyn.

Stk. 7. Virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1, skal årligt inden den 1. september fremsende konklusionerne fra en opdateret risiko- og sårbarhedsvurdering til Energinet. Virksomheder i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, skal fremsende konklusionerne fra en opdateret risiko- og sårbarhedsvurdering til Energinet minimum hvert tredje år. Første gang den 1. september 2018.

§ 11. Energinet skal årligt senest den 1. december udarbejde vurdering af it-relaterede risici og sårbarheder for det sammenhængende elforsyningssystem og det sammenhængende naturgasforsyningssystem. I vurderingerne skal indgå risici og sårbarheder afledt af sammenhænge med nabolandenes forsyningssystemer.

Planmateriale

§ 12. Virksomheder, jf. § 2, stk. 1, skal udarbejde planmateriale over egne forsyningskritiske it-systemer. Planmaterialet skal indeholde:

1) Beskrivelse af virksomhedens relation til transmissionsnettet, slutforbrugeren og andre virksomheder.
2) Identificering af den driftskritiske kommunikation eller informationsudveksling, virksomheden har med andre aktører.
3) Beskrivelse af forsyningskritiske it-systemer, herunder hvilke systemer de forsyningskritiske it-systemer er afhængige af.

Stk. 2. Planmaterialet skal opdateres ved ændringer i it-infrastrukturen.

Stk. 3. Virksomhederne skal identificere informationsstrømme med styringskritiske relationer til andre virksomheder og Energinet.

Stk. 4. Planmaterialet skal efter anmodning udleveres til Energinet. Virksomhederne skal ved udlevering af planmateriale vurdere materialets fortrolighed og tilsikre, at Energinet er bekendt med virksomhedens forventninger til håndtering af materialet. Energinet kan fastsætte krav til formen for dette planmateriale.

Stk. 5. Planmaterialet skal udfyldes for hver opgave for virksomheder, der indtager flere forskellige opgaver i el- og naturgassystemet.

§ 13. Energinet skal udarbejde planmateriale over information af forsyningskritisk karakter, der udveksles mellem Energinet og andre virksomheder. Planmaterialet skal indeholde et samlet overblik over de indbyrdes relationer for aktører i energisystemet for henholdsvis el- og gassystemet.

It-beredskabsplanlægning

§ 14. Virksomhederne, jf. § 2, stk. 1, skal udarbejde it-beredskabsplaner baseret på risiko- og sårbarhedsvurderingerne, jf. § 10.

Stk. 2. It-beredskabsplanerne skal indeholde følgende:
1) En identificering af forsyningskritiske it-systemer og afhængighed af andre systemer.
2) Beskrivelse af forebyggende foranstaltninger til at imødegå utilsigtede it-hændelser, herunder muligheder for segmentering af it-infrastruktur og alternative driftsformer. Anvendes fjernadgang til forsyningskritisk it-systemer, skal beredskabsplanen indeholde en plan for, hvordan angreb på disse systemer opdages og håndteres.
3) Beskrivelse af intern ansvars- og rollefordeling under krisestyring.
4) Beskrivelse af intern ansvarsplacering af systemansvar for forsyningskritiske it-systemer.
5) Beskrivelse af kommunikation med Energinet eller Energistyrelsen og virksomhedens tilknyttede it-sikkerhedstjeneste.
6) Beskrivelse af procedurer for etablering af alternativ drift ved nedbrud på forsyningskritiske it-systemer.
7) Plan for genoprettelse af forsyningskritiske it-systemer.
8) Plan for dokumentation og opfølgning på hændelser.
9) Beskrivelse af den operative ansvarsfordeling mellem virksomheden og dennes samarbejdsparter.

Stk. 3. It-beredskabsplanerne skal være en del af virksomhedens samlede beredskabsplanlægning.

Stk. 4. It-beredskabsplanerne skal være koordineret med sektorberedskabsplanen, jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren.

Stk. 5. It-beredskabsplanerne skal opdateres senest 3 måneder efter gennemførelse af en risiko- og sårbarhedsvurdering, jf. § 10, stk. 4.

Stk. 6. It-beredskabsplanerne skal være versionsstyret med en kort beskrivelse af ændringer i forhold til tidligere versioner.

Stk. 7. Virksomheder, der benytter ekstern opkobling til virksomhedens forsyningskritiske it-systemer, skal i beredskabsplanen beskrive procedurer for, hvordan it-sikkerhed sikres i disse forbindelser.

Stk. 8. Virksomhederne skal fremsende deres it-beredskabsplaner til Energinet ved opdatering, således at disse kan indgå i Energinets beredskabsplanlægning for hhv. el- og naturgassektoren.

§ 15. Virksomhedernes it-beredskabsplaner skal indgå i grundlaget for tilsynet, hvorfor de skal være modtaget af Energinet første gang senest den 1. januar 2018. Virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1, skal årligt inden den 1. september fremsende en opdateret beredskabsplan til modtagelse hos Energinet. Virksomheder i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, skal fremsende en opdateret beredskabsplan til modtagelse hos Energinet minimum hvert tredje år. Første gang den 1. september 2018.

Stk. 2. Energinet skal godkende virksomhedernes it-beredskabsplaner.

Stk. 3. Energinet skal vejlede virksomhederne i udarbejdelse af it-beredskabsplaner.

Stk. 4. Virksomhederne skal sikre, at it-beredskabsplanerne i relevant omfang indeholder forhold af betydning for sektorberedskabsplanen.

§ 16. Energinet skal sikre, at virksomhedernes it-beredskabsplaner indgår i sektorberedskabsplanerne for el- og naturgassektoren, jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren.

Stk. 2. Sektorberedskabsplanerne skal indeholde en beskrivelse af, hvordan Energinet planlægger at håndtere en it-beredskabssituation, der berører flere virksomheder, herunder:

1) Ansvarsfordelingen mellem virksomheder og Energinet.
2) Beskrivelse af kommunikationsveje og forholdsregler ved kompromittering af kommunikationsveje.
3) Krav Energinet i en it-beredskabssituation stiller til form, indhold og hyppighed af situationsrapporter fra virksomhederne til Energinet.
4) Hvorledes Energinet vil informere virksomhederne om it-beredskabssituationen, herunder form, indhold og hyppighed, således at Energinet kan tilsikre en samordnet situationsopfattelse hos virksomhederne i el- og naturgassektorerne.
5) En instruktion om anvendelse af specifik kryptering af informationer og driftsordre, hvis relevant.
6) Planer for segmentering af fælles it-infrastruktur eller driftsinfrastruktur i relevante scenarier, hvis relevant.

Stk. 3. Sektorberedskabsplanerne skal foruden kravene i stk. 2 baseres på en vurdering efter § 11. Sektorberedskabsplanerne til brug i it-beredskabssituationer skal revideres senest 3 måneder efter væsentlige ændringer i det samlede nationale risikobillede.

Stk. 4. Energinet skal sikre, at relevante parter inddrages i udarbejdelsen af sektorberedskabsplaner.

§ 17. Virksomheder i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, kan ansøge om at etablere samordnet it-beredskab, der medfører, at den operative håndtering af it-beredskabssituationer varetages i fællesskab eller af den ene part.

Stk. 2. Ansøgninger skal fremsendes til Energistyrelsen. Ansøgninger skal suppleres med en skriftlig begrundelse samt en beskrivelse af konsekvenser ved samordnet it-beredskab, herunder vurdering af aftalens konsekvenser for det almene beredskabsarbejde, jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren.

Øvelser, rapportering mv.

§ 18. Virksomheder, jf. § 2, stk. 1, skal sikre, at de medarbejdere, der indgår i håndteringen af it-beredskabet, løbende modtager den fornødne instruktion, uddannelse og træning i håndtering af it-beredskab.

§ 19. Virksomheder, jf. § 2, stk. 1, skal afholde it-beredskabsøvelser med udgangspunkt i egne it-beredskabsplaner, jf. § 14 stk. 1.

Stk. 2. It-beredskabsøvelser skal indgå i virksomhedernes øvelsesplan, jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren, og tage udgangspunkt i relevante trusler, sårbarheder eller erfaringer.

Stk. 3. Virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1, skal minimum afholde én årlig it-beredskabsøvelse. Virksomheder i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, skal sikre, at it-beredskabet i lighed med andre elementer i virksomhedens beredskabsplan øves.

Stk. 4. Virksomhederne skal dokumentere mindre interne øvelser, der træner virksomhedens it-sikkerhed. Dokumentationen af mindre øvelser skal fremsendes til Energinet én gang årligt.

Stk. 5. Energinet skal som minimum hvert tredje år afholde it-beredskabsøvelser, der træner anvendelse af sektorberedskabsplanen i it-beredskabssituationer, jf. § 16. Første øvelse skal senest være gennemført den 1. januar 2019.

Stk. 6. Virksomhederne henholdsvis Energinet skal udarbejde en evaluering af hver afholdt it-beredskabsøvelse. Øvelsesevalueringen skal angive øvelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor. Evalueringen skal indeholde en vurdering af, hvilke læringspunkter der er relevante at dele med andre virksomheder eller myndigheder.

Stk. 7. Virksomhedernes øvelsesevalueringer efter stk. 3 og stk. 4 fremsendes senest tre måneder efter øvelsen til Energinet. Energinets øvelsesevalueringer efter stk. 3-5 fremsendes senest tre måneder efter øvelsen til Energistyrelsen.

Stk. 8. Energinet skal udarbejde en vejledning, om hvilke typer af øvelser virksomhederne kan gennemføre og evaluere.

§ 20. Virksomheder, jf. § 2, stk. 1, skal udarbejde og gennemføre awareness-tiltag om it-sikkerhed, herunder formidle oplysninger om hvordan it-sikkerheden skal varetages af den berørte gruppe af medarbejdere eller eksterne.

Stk. 2. Virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1, skal minimum gennemføre awareness-tiltag årligt.

Stk. 3. Virksomheder i kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, skal gennemføre awareness-tiltag minimum hvert andet år.

Hændelser

§ 21. It-sikkerhedshændelser, der i væsentlig grad reducerer virksomhedens funktionalitet eller funktionaliteten af andre dele af el- og naturgassektoren, skal omgående meddeles Energinet.

Stk. 2. Energinet skal omgående underrette Energistyrelsen, såfremt it-sikkerhedshændelsen er af betydning for el- eller naturgasforsyningen på nationalt niveau.

Stk. 3. Såfremt en it-sikkerhedshændelse vurderes at have indflydelse på andre virksomheders eller myndigheders it-beredskab, skal væsentlige informationer omgående videregives til Energinet og til den it-sikkerhedstjeneste, virksomheden er tilknyttet.

Stk. 4. Energinet skal vurdere, om information om hændelser skal videregives til Center for Cybersikkerhed, Energistyrelsen eller andre virksomheder i el- eller naturgassektorerne.

Stk. 5. Forpligtigelsen til at vurdere og videreformidle akutte hændelsesinformationer, kan overdrages fra Energinet til en it-sikkerhedstjeneste efter tilladelse fra Energistyrelsen.

Stk. 6. Energinet skal underrette Center for Cybersikkerhed om it-sikkerhedshændelser i el- og naturgassektorerne, der har konsekvenser for forbrugerene. Energinet kan til denne underretning anvende en af Erhvervsstyrelsen dertil indrettet internetbasseret portal under iagttagelse af § 29. Underretningen skal som minimum indeholde en beskrivelse af:

1) Hændelsen.
2) Hændelsens konsekvenser, omfang og varighed.
3) Hvorvidt hændelsen vurderes at have væsentlige konsekvenser for tjenester i andre sektorer eller andre EU- eller EØS-lande.

Stk. 7. Energinet kan efter høring af den meddelende virksomhed i stk. 1 oplyse offentligheden om den konkrete hændelse, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse. Den meddelende virksomhed kan efter tilladelse fra Energinet, når de konkrete forhold tilsiger det, varetage oplysningen af egne kunder.

§ 22. Virksomheder, jf. § 2, stk. 1, skal udarbejde en evaluering af hændelser, der i væsentligt omfang aktiverer virksomhedens it-beredskab. Der skal minimum udarbejdes en evaluering på baggrund af følgende situationer:

1) Hændelser, der har aktiveret virksomhedens it-beredskab.

2) Hændelser, der har afstedkommet behov for manuel drift eller på anden måde har udgjort en risiko for væsentlig reduktion i it-styring af driften.
3) Hændelser, der har krævet bistand til situationsudredning, udbedring eller reetablering af systemer eller funktionalitet i virksomhedens it-systemer, f.eks. fra en it-sikkerhedstjeneste, Center for Cybersikkerhed eller Energinet.
4) Hændelser, der vurderes at kunne give anledning til læring ved andre virksomheder.

Stk. 2. Hændelsesevalueringen skal angive hændelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor samt en vurdering af, hvilke læringspunkter der er relevante at dele med andre virksomheder eller myndigheder.

Stk. 3. Hændelsesevalueringen fremsendes senest tre måneder efter hændelsen til Energinet henholdsvis Energistyrelsen.

Stk. 4. Har en hændelse i væsentligt omfang afprøvet konkrete forhold, som indgår i en planlagt øvelse i virksomhedens øvelsesplan, jf. § 19, stk. 2, kan Energinet godkende, at den planlagte øvelse erstattes af den pågældende hændelse.

Sikringsforanstaltninger

§ 23. Virksomheder, jf. § 2, stk. 1, skal sikre, at den fysiske opbevaring af forsyningskritiske it-systemer beskyttes i forhold til deres kritikalitet for forsyningen på nationalt, regionalt eller lokalt niveau. Således skal den fysiske beskyttelse af disse systemer ske på lige vilkår med fysiske anlæg af tilsvarende kritikalitet i medfør af regler for det almene beredskab.

Stk. 2. Virksomhederne skal sikre forsyningskritiske it-systemer mod uautoriseret adgang. Sikringen skal ske imod logisk såvel som fysisk adgang.

Leverandørstyring

§ 24. Virksomheder, jf. § 2, stk. 1, har ansvar for it-sikkerheden i forbindelse med anvendelse af eksterne leverandører af virksomhedens it-systemer.

Stk. 2. Virksomhederne skal etablere procedurer for adgangsstyring for leverandører af forsyningskritiske it-systemer eller dele heraf. Såfremt der er behov for fjernadgang til forsyningskritiske it-systemer, skal procedurer for denne fjernadgang beskrives i kontrakter, der på anmodning skal forevises ved tilsyn.

Stk. 3. Virksomhederne er ansvarlige for, at data, der er følsomme af hensyn til forsyningen af elektricitet eller naturgas og driften af forsyningskritiske it-systemer, håndteres med den fornødne sikkerhed. Den fornødne sikkerhed omfatter minimum:
1) at virksomhederne i relation til leverandører bevarer ejerskab af data,
2) at adgangen til disse data logges, med mulighed for henføring til specifikke medarbejdere ved leverandører og
3) at disse data opbevares i lokaler, der er fysisk sikret mod uvedkommendes adgang.

It-sikkerhedstjeneste

§ 25. Virksomheder, jf. § 2, stk. 1, skal være tilmeldt en proaktiv it-sikkerhedstjeneste, der yder vejledning om vurdering og mitigering af sårbarheder. Den proaktive it-sikkerhedstjeneste skal endvidere give informationer og varsle om relevante it-sikkerhedstrusler.

Stk. 2. Virksomheder i kategori 1 og 2, jf. § 9, stk. 1, nr. 1 og 2, skal foruden tjenesten, jf. stk. 1, være tilmeldt en reaktiv it-sikkerhedstjeneste, der bistår virksomheden ved nedbrud eller angreb på it-systemer, herunder assistance til akut skadesbegrænsning, bevisindsamling og reetablering i akutte sikkerhedsmæssige situationer.

Stk. 3. Virksomhederne skal sikre, at oplysninger, der har en sikkerhedsmæssig betydning for andre virksomheder i energisektorerne, kan viderebringes til andre virksomheder.

Stk. 4. Oplysninger, der tilvejebringes gennem en it-sikkerhedstjeneste, skal kunne videreformidles til andre virksomheder uden forsinkelse, såfremt disse oplysninger vurderes at have betydning for forsyningen af elektricitet eller naturgas.

Stk. 5. Virksomhederne skal indsende kontrakt med en it-sikkerhedstjeneste samt opgørelse af kontraktens omkostninger til godkendelse ved Energistyrelsen senest den 1. oktober 2017. Ved ændringer i kontrakten skal denne senest 2 måneder efter ændringen indsendes til fornyet godkendelse ved Energistyrelsen.

Stk. 6. Energistyrelsen kan inden for 8 uger fra modtagelsen afvise en kontrakt på baggrund af formelle og indholdsmæssige forhold, der vurderes at forsinke, vanskeliggøre eller begrænse virksomhedens eller den samlede sektors evne til at håndtere en akut it-beredskabssituation eller it-beredskabsplanlægning, jf. § 14 og § 16.

Stk. 7. Hvis flere virksomheder i el- eller naturgassektorerne indgår en fælles kontrakt med en it-sikkerhedstjeneste, skal kontrakten opbevares hos alle tilmeldte virksomheder.

Stk. 8. Virksomhederne skal sikre i deres kontrakt med en it-sikkerhedstjeneste, der yder tjenester til flere virksomheder, at it-sikkerhedstjenesten af egen drift videreformidler væsentlige sikkerhedsmæssige oplysninger erkendt ved en virksomhed, til andre tilmeldte virksomheder.

Tilsyn

§ 26 Energinet fører tilsyn over for virksomhederne, jf. § 2, stk. 1, nr. 1, 2 og 4, om overholdelsen af §§ 4, 6, 7, 10, 12, 14, 15, 18-25 og § 29.

Stk. 2. Energinet gennemfører it-beredskabstilsyn for virksomheder i kategori 1, jf. § 9, stk. 1, nr. 1, årligt.

Stk. 3. For virksomheder omfattet af kategori 2 og 3, jf. § 9, stk. 1, nr. 2 og 3, gennemføres it-beredskabstilsynet sammenfaldende med det tre-årlige beredskabstilsyn, jf. bekendtgørelser om beredskab for elsektoren og naturgassektoren.

Stk. 4. Energinet skal udarbejde en rapport om tilsynet. Rapporten skal forelægges virksomheden til kommentering inden færdiggørelse. Ved uenighed om faktuelle forhold skal uenigheden skriftligt indberettes for Energistyrelsen.

Stk. 5. Energinet skal senest den 1. maj fremsende en årlig redegørelse til Energistyrelsen om forrige års gennemførte tilsynsarbejde.

§ 27. Energistyrelsen fører tilsyn med Energinet's arbejde som virksomhed, jf. § 2, stk. 1, nr. 3, som koordinerende virksomhed samt som tilsynsmyndighed, jf. § 26, stk. 1.

Stk. 2. Energistyrelsen skal årligt udarbejde en rapport om tilsynet med Energinet. Rapporten skal fremsendes til Energinet til kommentering inden færdiggørelse.

Andre bestemmelser

§ 28. Energitilsynet kan, jf. bekendtgørelse om indtægtsrammer for netvirksomheder, efter ansøgning forhøje omkostningsrammen midlertidigt for netvirksomheder, der har dokumenterede meromkostninger som følge af krav om tilmelding til en it-sikkerhedstjeneste, jf. § 25, stk. 1.

Stk. 2. Omkostningsrammen og det samlede forrentningsgrundlag i reguleringsåret kan for netvirksomheder omfattet af kategori 1-3 forhøjes med netvirksomhedens omkostninger til it-sikkerhedstjenestens ydelser om relevant varsling og information. Omkostningsrammen og det samlede forrentningsgrundlag i reguleringsåret kan endvidere for netvirksomheder omfattet af kategori 1 og 2 forhøjes med netvirksomhedens omkostninger til it-sikkerhedstjenestens ydelser om udredning og reetablering i akutte sikkerhedsmæssige situationer. Netvirksomhedens kontrakt med it-sikkerhedstjenesten skal indgås på markedsmæssige vilkår, jf. § 46 i lov om elforsyning.

Stk. 3. En netvirksomhed kan efter reglerne i bekendtgørelse om indtægtsrammer for netvirksomheder én gang årligt ansøge Energitilsynet om en forhøjelse af omkostningsrammen og det samlede forrent-

ningsgrundlag i reguleringsåret for det år, hvor de dokumenterede meromkostninger er afholdt, jf. stk. 1 og 2. Ansøgningen skal være bilagt Energistyrelsens godkendelse af netvirksomhedens kontrakt med it-sikkerhedstjenesten, jf. § 25, stk. 5, og den skal indeholde en redegørelse for, hvordan priser og vilkår i kontrakten er fastsat. Muligheden for at få godkendt en forhøjelse af omkostningsrammen og det samlede forrentningsgrundlag i reguleringsåret bortfalder, såfremt Energitilsynet ikke har modtaget en ansøgning rettidigt, jf. bekendtgørelse om indtægtsrammer for netvirksomheder.

§ 29. Følsomme oplysninger skal behandles med fortrolighed.

Stk. 2. Ved følsomme oplysninger forstås:

1) Oplysninger om konkrete risici- og sårbarheder, jf. § 10.
2) Planmateriale, jf. §§ 12 og 13.
3) Kritiske dele af beredskabsplaner, jf. §§ 14 og 16, indeholdende beskrivelse af, hvordan virksomheden eller sektoren vil agere i givne beredskabssituationer.
4) Materiale af tilsvarende karakter, der af virksomheden eller Energinet vurderes at være følsomt.

Stk. 3. Forsendelse og håndtering af følsomt materiale skal ske på en måde, der sikrer fortrolighed og integritet af materialet.

Stk. 4. Følsomt materiale, som ikke længere benyttes, skal destrueres.

§ 30. Energinet skal bidrage til udarbejdelse af sektorspecifikke trusselsvurderinger på vegne af el- og naturgassektorerne. Energinet skal i denne forbindelse stille en medarbejder til rådighed for Center for Cybersikkerhed.

Stk. 2. Medarbejderen skal forrette tjeneste efter anvisning fra Center for Cybersikkerhed.

Stk. 3. Energinet skal sikre, at denne medarbejder har de fornødne kompetencer og viden påkrævet for at kunne udarbejde relevante sektorspecifikke trusselsvurderinger.

Stk. 4. Energinet skal sikre, at medarbejderen modtager informationer relevant for arbejdet.

§ 31. Virksomhederne skal efter anmodning give Energinet og Energistyrelsen oplysning om alle forhold af relevans for beredskabsarbejdet, herunder oplysninger til brug for det i § 9, stk. 1 og stk. 2 nævnte klassificering. Energinet skal tilsvarende oplyse Energistyrelsen om alle forhold af relevans for beredskabsarbejdet.

§ 32. Energistyrelsen kan efter ansøgning dispensere fra bestemmelser i denne bekendtgørelse, hvor ansøgeren har godtgjort at en dispensation fra den konkrete bestemmelse i væsentligt omfang har mindre betydning eller reduceret effekt for it-beredskabet.

Håndhævelse og klageadgang

§ 33. Energinet kan i forbindelse med deres tilsynsvirksomhed udstede påbud, jf. § 85 d, stk. 1, i lov om elforsyning og § 47 b, stk. 1, i lov om naturgasforsyning, for manglende overholdelse af §§ 4, 6, 7, 10, 12, 14, 15, 18-25 og 29.

Stk. 2. Energistyrelsen kan udstede påbud om it-revision og gennemførelse af tiltag fra en sådan it-revision efter indstilling fra Energinet, ved manglende overholdelse af påbud udstedt efter stk. 1.

§ 34. Energistyrelsen kan i forbindelse med deres tilsyn med Energinet udstede påbud, jf. § 85 d, stk. 1, i lov om elforsyning og § 47 b, stk. 1, i lov om naturgas forsyning, for manglende overholdelse af §§ 4-6 og 8, § 9, stk. 5, §§ 10-14, § 15 stk. 2 og 3, §§ 16, 18-26 og 29-30.

Stk. 2. Energistyrelsen kan udstede påbud overfor Energinet om it-revision og gennemførelse af tiltag fra en sådan it-revision, ved manglende overholdelse af påbud udstedt efter stk. 1 jf. § 85 c, stk. 2 og 3, i lov om elforsyning, og § 15 b, stk. 2 og 3, i lov om naturgasforsyning.

§ 35. Afgørelser truffet af Energinet, jf. § 9, stk. 5, § 12, stk. 4, § 15, stk. 2, § 22, stk. 4 og § 33 stk. 1, kan ikke påklages til Energistyrelsen eller anden administrativ myndighed.

Stk. 2. Afgørelser efter stk. 1 kan dog påklages til Energistyrelsen for så vidt angår retlige spørgsmål.

Stk. 3. Klagen skal være indgivet skriftligt inden 4 uger efter, at afgørelsen er meddelt til pågældende.

§ 36. Energistyrelsens afgørelser, jf. § 17, § 21, stk. 5, § 25, stk. 6, § 31, § 33, stk. 2 og §§ 34 og 35, kan ikke indbringes for anden administrativ myndighed.

Stk. 2. Afgørelser efter stk. 1 kan dog påklages til Energiklagenævnet for så vidt angår retlige spørgsmål.

Stk. 3. Klagen skal være indgivet skriftligt inden 4 uger efter, at afgørelsen er meddelt til pågældende.

Ikrafttrædelse

§ 37. Bekendtgørelsen træder i kraft den 9. maj 2018.

Stk. 2. Bekendtgørelse nr. 515 af 23. maj 2017 om it-beredskab for el-og naturgassektorerne ophæves.

Energi-, Forsynings- og Klimaministeriet, den 1. maj 2018

Lars Christian Lilleholt

/ Martin Hansen

[1)] Bekendtgørelsen indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EU-Tidende 2016, nr. L 194, s. 1.