Bekendtgørelse om it-beredskab for el- og naturgassektorerne

Generelle bestemmelser

§ 1. Denne bekendtgørelse fastsætter regler for sikring af it-systemer, der er kritiske for produktion eller forsyning af elektricitet eller naturgas. Disse forsyningskritiske it-systemer skal sikres således, at forsyningen kan opretholdes og videreføres under ekstraordinære situationer, hvor it-systemernes drift trues.

§ 2. Denne bekendtgørelse finder anvendelse på bevillingspligtige virksomheder jf. elforsyningslovens §§ 10 og 19 samt for bevillingspligtige virksomheder jf. lov om naturgasforsyning § 10. Energinet.dk eller et af Energinet.dk helejet datterselskab er ligeledes omfattet af denne bekendtgørelse. Denne bekendtgørelse gælder ligeledes for balanceansvarlige virksomheder, der efter aftalte med Energinet.dk yder balancerende tjenester til energisystemet.

Stk. 2. Virksomheder omfattet af stk. 1. skal foretage de fornødne foranstaltninger for at sikre videreførelsen af el- og naturgasforsyningen i tilfælde af beredskabshændelser forårsaget af nedbrud i eller angreb på forsyningskritiske it-systemer.

Definitioner

§ 3. I denne bekendtgørelse anvendes følgende definitioner:

Balanceansvarlige virksomheder er virksomheder, der yder balancerende tjenester til energisystemet efter aftale med Energinet.dk. I denne bekendtgørelse forstås balanceansvarlige virksomheder som virksomheder, der har kontrol over fysiske anlæg til produktion, hvad enten denne kontrol udøves direkte eller gennem andre virksomheder.

Forsyning betegner den fysiske formidling af elektricitet eller naturgas fra producent til slutforbruger.

Forsyningskritiske processer er processer, der er nødvendige for forsyningen af en eller flere slutforbrugere. En forsyningskritisk proces foregår enten internt i en virksomhed eller i forbindelse med overlevering af energivarer eller ydelser mellem flere virksomheder.

It-sikkerhedstjeneste er en enhed, der kan varetage it-sikkerhedsmæssige opgaver for den enkelte virksomhed. En it-sikkerhedstjeneste leverer som minimum proaktive ydelser, der kan medvirke til at styrke it-sikkerheden ved ydelsesmodtageren, herunder informationer om it-sikkerhedstrusler og vejledning om vurdering og mitigering af sårbarheder. En it-sikkerhedstjeneste kan endvidere yde reaktive ydelser som anvendes ved nedbrud eller angreb på it-systemer, herunder assistance til akut skadesbegrænsning, bevisindsamling eller genopretning.

Cybersikkerhed er beskyttelse mod angreb på data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. Informationssikkerhed involverer organisering af it-sikkerhedsarbejdet, påvirkning af brugeradfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

Ikke kritiske it-systemer er it-systemer, der ikke styrer systemer eller processer, som kan påvirke forsyningen. Et sådan system er logisk adskilt fra kritiske it-systemer.

It-sikkerhed er en generel betegnelse for al sikkerhed i anvendelsen af it-systemer.

It-beredskab er de foranstaltninger, det arbejde og de processer, der skal forhindre, begrænse eller håndtere skader og forsyningssvigt som resultat af nedbrud, forstyrrelser eller angreb på el- og naturgassektorernes kritiske it-systemer.

Forsyningskritisk it-system er et it-system, der styrer eller i væsentligt omfang påvirker forsyningskritiske processer.

Logisk adgang er adgang til et it-systems funktionalitet via forbindelser til andre systemer eller netværk.

Koordinerende og operative forhold

§ 4. Alle virksomheder omfattet af § 2 er ansvarlige for egen it-sikkerhed. Alle virksomheder skal være i stand til at omsætte informationer om it-sikkerhedstrusler og konkrete it-varsler til nødvendige tiltag i egen organisation. Virksomheder i kategori 1 og 2 jf. § 7 skal sikre, at der er mulighed for it-sikkerhedsmæssig assistance til driftsorganisationen på alle tider af døgnet.

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 operative situationer, hvad enten disse afhængigheder skyldes aftale om it-assistance, it-driftsservice, el-forsyning eller andet. Beredskabsplanen skal tydeligt beskrive den operative ansvarsfordeling mellem virksomheden og dennes samarbejdsparter.

§ 5. Energinet.dk skal varetage de overordnede koordinerende opgaver i forbindelse med håndtering af beredskabshændelser, der omfatter flere virksomheder, eller hvor der er risiko for, at forsyningssikkerheden kompromitteres ved flere netvirksomheders kunder. Den koordinerende opgave medfører ikke, at Energinet.dk skal overtage det lokale operative ansvar ved en it-sikkerhedshændelse.

Stk. 2. Energinet.dk skal kunne bistå virksomheder omfattet af § 2 med kontaktoplysninger til andre virksomheder omfattet af § 2 eller relevante myndigheder i en akut situation.

Stk. 3. Energinet.dk skal kunne bistå virksomhederne med oplysninger om aktuelle driftstilstande m.v. af relevans for virksomhedernes håndtering af den pågældende situation.

Stk. 4. Energinet.dk skal etablere et formaliseret samarbejde om it-beredskabsforhold, der har til formål at fremme koordineringen af såvel planlægningen som udøvelsen af it-beredskabet. Samarbejdet kan foregå i sammenhæng med andet relevant beredskabsarbejde efter aftale med Energistyrelsen.

Stk. 5. Energinet.dk skal tilsikre at have det fornødne beredskab til håndtering af it-sikkerhedshændelser i egne systemer.

Stk. 6. Energinet.dk skal til enhver tid kunne modtage og videreformidle it-sikkerhedsvarsler og hændelsesoplysninger til virksomheder i el- og naturgassektorerne.

Organisatoriske forhold

§ 6. Enhver virksomhed omfattet af § 2 skal udpege en it-beredskabsansvarlig medarbejder, som er ansvarlig for at koordinere virksomhedens sikring af forsyningskritiske it-systemer, herunder risiko- og sårbarhedsvurdering af forsyningskritiske it-systemer. Den it-beredskabsansvarlige medarbejder kan varetage andre opgaver og funktioner i beredskabsarbejdet, såfremt det kan godtgøres, at dette personsammenfald ikke medfører interessekonflikter eller på anden måde begrænser virksomhedens mulighed for at varetage operative og planlægningsmæssig opgaver på betryggende vis.

Stk. 2. Virksomheden skal tilsikre, at it-beredskabsarbejde og det almene beredskabsarbejde koordineres, således at virksomhedens ledelse bibringes et samlet risikobillede, der repræsenterer kendte og mulige risici mod produktionen eller forsyningen af el eller naturgas.

Stk. 3. Virksomheden skal fire gange årligt koordinere mellem den ansvarlige for det almene beredskab (beredskabskoordinatoren), den it-beredskabsansvarlige og ledelsen. Virksomheden skal kunne dokumentere denne koordination.

Stk. 4. Personsammenfald mellem den it-beredskabsansvarlige, beredskabskoordinatoren og ledelsen skal undgås. Ved virksomheder placeret i kategori 3 jf. § 7 kan personsammenfald tillades. Tilsynsmyndigheden skal underrettes herom. Virksomheder i kategori 2 jf. § 7 kan ansøge tilsynsmyndigheden om tilladelse til et sådan personsammenfald. En sådan ansøgning skal begrundes med praktiske årsager og i øvrigt vurderes fagligt forsvarligt. Personsammenfald kan ikke tillades for virksomheder i kategori 1 jf. § 7.

Stk. 5. Alle virksomheder skal etablere en organisering af it-beredskabet, der tilsikrer, at virksomheden kan modtage it-sikkerhedsvarsler. Alle virksomheder skal på baggrund af egne risiko- og sårbarhedsvurderinger etablere den fornødne organisering, der kan iværksætte relevante tiltag ved modtagelse af et it-sikkerhedsvarsel.

Stk. 6. Energinet.dk skal kunne vejlede virksomhederne i forbindelse med etablering af procedurer for modtagelse af trusselsvurderinger og varsler.

Stk. 7. Virksomheder omfattet af § 2 er forpligtiget til at sikre, at leverandører af serviceydelser, der direkte eller indirekte har indflydelse på virksomhedens forsyningskritiske it-systemer, overholder de krav, som denne bekendtgørelse pålægger virksomheden. Virksomheden skal dokumentere, at relevante leverandører inddrages i beredskabsplanlægningen.

Kategorisering af virksomheder

§ 7. Virksomhederne inddeles i tre kategorier. De tre kategorier defineres ud fra deres betydning for det samlede el- eller naturgassystem på følgende måde:

1) Kategori 1: Virksomheder, der producerer eller forsyner energimængder af en størrelse, som anses for at være af væsentlig betydning for at opretholde el- eller naturgasforsyningen for de sammenhængende forsyningssystemer eller væsentlige dele af disse på nationalt niveau.

2) Kategori 2: Virksomheder, der producerer eller forsyner energimængder af en størrelse, som anses for at være af væsentlig betydning for at opretholde el- eller naturgasforsyningen eller væsentlige dele af disse på regionalt niveau.

3) Kategori 3: Øvrige virksomheder omfattet af § 2, der ikke er omfattet af kategori 1 eller 2.

Stk. 2. Ved nationalt niveau forstås et forsyningsområde med over 250.000 aftagere eller virksomheder, der håndterer energimængder over 600 MWh/h el eller over 100.000 Nm3/time gas.

Stk. 3. Ved regionalt niveau forstås et forsyningsområde med mellem 30.000 og 250.000 aftagere. 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, anses for at være af væsentlig betydning på regionalt niveau.

Stk. 4. Virksomheder, der ejer eller driver anlæg klassificeret af væsentlig betydning for den nationale eller regionale forsyning, vil blive indplaceret i den tilsvarende kategori, med mindre det kan godtgøres, at anlægget ikke anvender forsyningskritiske it-systemer.

Stk. 5. I tilfælde, hvor der er uoverensstemmelse mellem kategoriseringen ud fra antallet af aftagere og energimængde, samt i tvivlstilfælde kategoriseres virksomheder ud fra et forsigtighedsprincip i den kategori, der stiller mest omfattende krav til virksomhederne.

Stk. 6. Såfremt en virksomhed kan godtgøre at tilhøre en anden kategori efter stk. 1, skal dette meddeles tilsynsmyndigheden. Tilsynsmyndigheden reviderer årligt kategoriseringen efter stk. 1 - 3, senest den 1. februar. Virksomhederne underrettes herom.

Risiko- og sårbarhedsvurderinger

§ 8. Virksomheder omfattet af § 2 skal udarbejde en vurdering af relevante risici og sårbarheder, der kan påvirke virksomhedens forsyningskritiske it-systemer. Denne risiko- og sårbarhedsvurdering skal revideres minimum årligt og i det omfang, udviklingen gør det nødvendigt, herunder ved væsentlige ændringer af it-systemer eller trusselsbilledet. Virksomheden skal kunne dokumentere disse revisioner. Samtlige virksomheder skal udarbejde en risiko- og sårbarhedsvurdering pr. 1. september 2017. Denne risiko- og sårbarhedsvurdering skal fremsendes til Energinet.dk for at danne udgangspunkt for Energinet.dk's koordinering af beredskabsplanlægningen for sektorerne jf. § 11.

Stk. 2. Risiko- og sårbarhedsvurderinger skal udarbejdes i samråd mellem relevante personer i organisationen og skal integreres i virksomhedens samlede risikobillede jf. § 6. stk. 2. Den interne koordinering af beredskabsarbejdet jf. § 6 stk. 3, skal sikre denne integration.

Stk. 3. Risiko- og sårbarhedsvurderinger skal forevises ved tilsyn. Tilsynsmyndigheden kan pålægge virksomhederne at udføre risiko- og sårbarhedsvurderinger på baggrund af specifikke scenarier eller trusler, der anses for relevante for den pågældende virksomhed.

Stk. 4. Virksomheder i kategori 1 jf. § 7 skal årligt inden 1. maj fremsende en revideret risiko- og sårbarhedsvurdering til Energinet.dk. Virksomheder i kategori 2 og 3 jf. § 7, skal fremsende en revideret risiko- og sårbarhedsvurdering til Energinet.dk minimum hvert tredje år. Første revision fremsendes 1. maj 2018.

Stk. 5. Risiko- og sårbarhedsvurderinger jf. stk. 1. skal inddrage alle relevante trusler, herunder egne erfaringer fra øvelser og hændelser jf. §§ 12, 13 og 14 samt trusselsvurderinger fra Center for Cybersikkerhed og virksomhedens tilknyttede it-sikkerhedstjeneste jf. § 27.

Stk. 6. Energinet.dk skal årligt senest den 1. august udarbejde en vurdering af it-relaterede risici og sårbarheder for det sammenhængende elforsyningssystem henholdsvis det sammenhængende naturgasforsyningssystem. I vurderingerne skal indgå risici og sårbarheder afledt af sammenhænge med nabolandenes forsyningssystemer. Vurderingerne baseres bl.a. på virksomhedernes og Energinet.dk's vurderinger jf. stk. 1, samt planmateriale jf. § 9.

§ 9. Virksomhederne skal udarbejde planmateriale over egne forsyningskritiske it-systemers afhængigheder og sammenhænge. Planmaterialet skal beskrive virksomhedens placering i den samlede forsyningskæde, herunder identificere den driftskritiske kommunikation eller informationsudveksling, virksomheden har med andre aktører. Planmaterialet skal beskrive, hvilke systemer der betragtes som forsyningskritiske it-systemer, samt hvilke systemer de forsyningskritiske it-systemer er afhængige af.

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

Stk. 3. Alle virksomheder skal identificere informationsstrømme med styringskritisk relationer til andre virksomheder og Energinet.dk. For hver relation vurderes risici mht. tab og kompromittering af data eller kommunikation.

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

Stk. 5. Energinet.dk skal udarbejde planmateriale over information af forsyningskritisk karakter, der udveksles mellem Energinet.dk og andre virksomheder. Dette planmateriale skal præsentere et samlet overblik over de indbyrdes relationer for aktører i energisystemet for henholdsvis el- og gassystemet.

Stk. 6. Virksomheder, der indtager flere væsensforskellige opgaver i el- og naturgassystemet, skal udfylde planmateriale for hver opgave.

Beredskabsplanlægning

§ 10. Alle virksomheder skal udarbejde it-beredskabsplaner baseret på de i virksomheden udarbejdede it-risiko- og sårbarhedsvurderinger jf. § 8. Disse it-beredskabsplaner skal være en del af virksomhedens samlede beredskabsplanlægning, ligesom disse planer skal være koordineret med sektorberedskabsplanen som beskrevet i § 11.

Stk. 2. It-beredskabsplaner jf. stk.1 skal angive, hvordan virksomheden planlægger at håndtere en it-beredskabssituation. It-beredskabsplaner skal tilstræbes ikke at indeholde kritiske dele, der skal håndteres med fortrolighed, da dette vanskeliggør håndteringen af dokumenterne som beskrevet nærmere i § 21.

Stk. 3. It-beredskabsplanerne efter stk.1 skal som minimum indeholde:

1. Identificering af forsyningskritiske it-systemer og afhængighed af andre systemer.
2. Forebyggende foranstaltninger til at imødegå utilsigtede it-hændelser, herunder muligheder for segmentering af it-infrastruktur og alternative driftsformer. Hvis virksomheden anvender 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/Energistyrelsen samt virksomhedens tilknyttet it-sikkerhedstjeneste.
6. Beskrivelse af procedure 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.

Stk. 4. Beredskabsplanerne skal revideres senest 3 måneder efter gennemførelse af risiko- og sårbarhedsvurdering, samt ved væsentlige forandrede organisatoriske eller tekniske forhold. Beredskabsplanerne skal være versionsstyret med en kort beskrivelse af ændringer i forhold til tidligere planer. Energinet.dk skal vejlede virksomhederne i udarbejdelse af disse beredskabsplaner og skal sikre, at virksomhedernes beredskabsplaner i relevant omfang indeholder forhold af betydning fra Energinet.dk's sektorberedskabsplaner.

Stk. 5. Tilsynsmyndigheden kan pålægge en virksomhed at revidere sin it-beredskabsplan.

Stk. 6. Virksomheder, der i forbindelse med vagtordning, hjemmearbejdsplads eller på anden vis benytter ekstern opkobling til virksomhedens forsyningskritiske it-systemer, skal i beredskabsplanen beskrive procedurer for, hvordan it-sikkerhed sikres i disse forbindelser.

§ 11. Energinet.dk skal tilsikre, at it-sikkerhed indgår i sektorberedskabsplaner for både el- og naturgassektoren. Denne plan skal indeholde en beskrivelse af, hvordan Energinet.dk planlægger at håndtere en it-beredskabssituation, der berører flere virksomheder, herunder:

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

Stk. 2. Sektorberedskabsplaner skal foruden kravene i stk. 1 baseres på en vurdering efter § 8, stk. 6.

Stk. 3. Energinet.dk skal tilsikre, at relevante parter inddrages i udarbejdelsen af sektorberedskabsplaner. Virksomhederne skal i det formaliserede samarbejde om it-beredskabsforhold jf. § 5 stk. 4 have mulighed for at tilkendegive evt. ændringsforslag til sektorberedskabsplanlægningen.

§ 12. Virksomheder i kategori 2 og 3 jf. § 7, 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. En aftale om samordnet it-beredskab må ikke påvirke ansvaret for it-beredskabsplanlægningen, og den enkelte virksomhed er fortsat ansvarlig for planlægning og risikovurdering jf. §§ 8, 9, 10 og 11.

Stk. 2. Den operative struktur skal fremgå af virksomhedernes it-beredskabsplan jf. § 10, og planmateriale jf. § 9 skal være tilgængelig for den operativt ansvarlige part i operative situationer.

Stk. 3. Ansøgninger om samordnet it-beredskab skal fremsendes til Energistyrelsen. Ansøgningen skal suppleres med en skriftlig begrundelse samt en beskrivelse af konsekvenser ved samordnet it-beredskab, herunder vurdering af aftalens konsekvenser for det almene beredskabsarbejde. Denne beskrivelse skal inddrage de seneste risiko- og sårbarhedsvurderinger udarbejdet af de berørte virksomheder.

Stk. 4. Energistyrelsen træffer afgørelse på baggrund af en faglig vurdering af ansøgningens operative konsekvenser. Virksomhedens egen vurdering samt en faglig vurdering af de operative konsekvenser indhentet ved Energinet.dk skal lægges til grund for afgørelsen.

Øvelser, rapportering mv.

§ 13. Virksomheden skal sikre, at de medarbejdere, der indgår i håndteringen af it-beredskabet, løbende modtager den fornødne instruktion, uddannelse og træning i håndtering af it-sikkerhed.

Stk. 2. Virksomheden skal afholde it-sikkerhedsøvelser i anvendelse af egne it-beredskabsplaner jf. § 10 stk. 1. Virksomheder i kategori 1 jf. § 7 skal som minimum afholde én årlig it-beredskabsøvelse. Virksomheder i kategori 2 og 3 jf. § 7 skal tilsikre, at it-beredskabet trænes i forbindelse med det almene beredskabsarbejde i relevant omfang.

Stk. 3. Energinet.dk skal som minimum hvert tredje år afholde it-beredskabsøvelser, der træner anvendelse af sektorberedskabsplanen i it-beredskabssituationer jf. § 11.

Stk. 4. It-beredskabsøvelser skal indgå i virksomhedernes og Energinet.dk's 5-årige øvelsesplan. Det skal tilstræbes, at disse øvelser tager udgangspunkt i relevante trusler, sårbarheder eller erfaringer, således at øvelsernes realisme medvirker til at fremme bevidstheden om disse forhold i virksomheden.

Stk. 5. Energinet.dk skal udarbejde en vejledning, om hvilke typer af øvelser virksomhederne bør gennemføre og evaluere efter stk. 6 i løbet af en 5-årig periode. Tilsynsmyndigheden kan pålægge, at der øves specifikke scenarier eller elementer.

Stk. 6. Virksomheden og Energinet.dk skal udarbejde evaluering af hver afholdt øvelse. 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. Evalueringen fremsendes senest tre måneder efter øvelsen til tilsynsmyndigheden.

Stk. 7. Udover de øvelser, beskrevet i stk. 2 og stk. 3, skal virksomhederne dokumentere mindre interne øvelser, der træner virksomhedens it-sikkerhed. Fortegnelse over gennemførte mindre øvelser skal fremsendes til tilsynsmyndigheden én gang årligt.

Stk. 8. Virksomheden skal udarbejde og gennemføre awareness-tiltag med det formål løbende at oplyse og uddanne medarbejdere og relevante samarbejdsparter om it-sikkerhed. Virksomheder i kategori 1 jf. § 7 skal som minimum gennemføre awareness-tiltag årligt, mens virksomheder i kategori 2 og 3 skal gennemføre awareness-tiltag minimum hvert andet år.

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

Stk. 2. Energinet.dk 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.dk og den it-sikkerhedstjeneste, virksomheden er tilknyttet.

Stk. 4. Energinet.dk skal vurdere, om disse informationer skal videregives til Center for Cybersikkerhed, Energistyrelsen eller andre virksomheder i energisektorerne. Forpligtigelsen til at vurdere og videreformidle akutte hændelsesinformationer kan overdrages fra Energinet.dk til en it-sikkerhedstjeneste efter tilladelse fra Energistyrelsen.

Hændelser

§ 15. Virksomheden skal udarbejde en evaluering af større eller usædvanlige hændelser, der i væsentligt omfang aktiverer virksomhedens it-beredskab. Tilsvarende udarbejder Energinet.dk en evaluering af hændelser, som i væsentligt omfang har aktiveret el- eller naturgassektorens it-beredskab. Der udarbejdes som minimum evaluering på baggrund af følgende:

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

Tilsynsmyndigheden kan pålægge en virksomhed at udarbejde en sådan evaluering.

Stk. 2. Hændelsesevalueringen skal angive hændelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor. Hændelsesevalueringen skal indeholde en vurdering af, hvilke læringspunkter der er relevante at dele med andre virksomheder eller myndigheder. Denne evaluering erstatter ikke virksomhedernes pligt til omgående at underrette Energinet.dk jf. § 14.

Stk. 3. Evalueringen fremsendes senest tre måneder efter hændelsen til tilsynsmyndigheden.

Stk. 4. Hvis en hændelse jf. stk. 1 i væsentligt omfang har afprøvet konkrete forhold, som indgår i en planlagt øvelse i virksomhedens 5-årige øvelsesplan, jf. § 13, og hvis denne afprøvning vurderes at have samme værdi som en planlagt øvelse, kan tilsynsmyndigheden godkende, at den planlagte øvelse erstattes af den pågældende hændelse. En sådan godkendelse forudsætter, at der er udarbejdet en tilfredsstillende evaluering jf. stk. 1.

Sikringsforanstaltninger

§ 16. Enhver virksomhed skal sikre, at lokaliteter indeholdende forsyningskritiske it-systemer som datacentre m.m. beskyttes i henhold til deres kritikalitet for forsyningen på nationalt, regionalt eller lokalt niveau.

Stk. 2. Virksomheden skal sikre disse forsyningskritiske it-systemer mod uautoriseret adgang, såvel logisk som fysisk adgang.

Stk. 3. Beskyttelse jf. stk. 1 indebærer etablering af procedurer og forholdsregler i henhold til relevante regler for beskyttelse af tilsvarende fysiske installationer, der beskyttes af hensyn til deres betydning for den fysiske el- eller naturgasforsyningen nationalt, regionalt eller lokalt.

Leverandørstyring

§ 17. Virksomheden har selv ansvaret for de it-sikkerhedsmæssige aspekter i forbindelse med anvendelse af eksterne leverandører til såvel service, vedligeholdelse, drift, styring og overvågning af virksomhedens it-systemer. Virksomheder, der anvender en leverandør til at varetage forsyningskritisk it eller dele heraf, skal kunne dokumentere, at denne leverandør overholder kravene fastsat i denne bekendtgørelse.

Stk. 2. Virksomheden skal etablere procedurer for adgangsstyring af 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 kan forevises ved tilsyn. Der skal foretages en risikovurdering af serviceaftaler, der indeholder mulighed for fjernadgang til forsyningskritiske it-systemer.

Stk. 3. Virksomheden er ansvarlig for, at data, der af hensyn til forsyningen af el- eller naturgas og driften af forsyningskritiske it-systemer er følsomme, håndteres med den fornødne sikkerhed. Herunder forstås følsomme oplysninger som oplysninger, der kan anvendes til at få uberettiget adgang til forsynings- og driftskritiske systemer. Den fornødne sikkerhed omfatter;

1. at virksomheden i relation til leverandører bevarer ejerskab af data.
2. at adgangen til disse data logges, med mulighed for henføring til specifikke medarbejdere ved leverandører.
3. at disse data opbevares i lokaler, der er fysisk sikret mod uvedkommendes adgang.

Stk. 4. Virksomheder kan efterleve krav om dokumentation for leverandørstyring ved at anvende en ekstern it-revisor. Tilsynsmyndigheden kan dog forlange, at virksomhedens ledelse godtgør for overvejelser i relation til en sådan disposition.

Tilsyn

§ 18. Energinet.dk varetager opgaven som tilsynsmyndighed over for virksomhedernes overholdes af bestemmelser i denne bekendtgørelse. Energinet.dk skal ved varetagelse af denne tilsynsopgave tilsikre en tydelig adskillelse mellem varetagelsen af den overordnede koordinerende opgave efter § 5 og tilsynsopgaven efter denne bestemmelse. Energinet.dk skal ved udøvelse af tilsyn tilsikre, at den pågældende virksomhed bliver oplyst herom.

Stk. 2. Tilsynsmyndigheden fører tilsyn med virksomhederne jf. § 2, dog ikke Energinet.dk eller et af Energinet.dk helejet datterselskaber. Tilsynsmyndigheden gennemfører it-beredskabstilsyn ved virksomheder i kategori 1 jf. § 7 årligt. Ved resterende virksomheder gennemføres it-beredskabsstilsynet sammenfaldende med det tre-årlige beredskabstilsyn.

Stk. 3. Inden for den enkelte virksomhed kan tilsynet gennemføres ved brug af stikprøver, der vurderes at afspejle den samlede virksomhed i rimeligt omfang. Som en del af dette tilsyn skal tilsynsmyndigheden gennemgå virksomhedernes beredskabsplaner for at sikre, at planerne kan danne grundlag for en koordineret og effektiv håndtering af beredskabssituationer. Gennemgangen kan gennemføres gruppevist med et mindre antal selskaber ad gangen, såfremt dette findes forsvarligt.

Stk. 4. Tilsynsmyndigheden kan pålægge en virksomhed at foretage ændringer i it-beredskabsarbejdet foretaget efter denne bekendtgørelse, såfremt bekendtgørelsen ikke vurderes overholdt, eller såfremt dette vurderes at være nødvendigt for at opnå en koordineret og effektiv krisehåndtering. Tilsynsmyndigheden kan herunder pålægge en virksomhed at afholde øvelser efter § 13, stk. 2, og at nærmere angivne forhold skal indgå i sådanne øvelser.

Stk. 5. Tilsynsmyndigheden skal udarbejde en rapport om tilsynet med virksomheden. Rapporten skal forelægges virksomheden til kommentering inden færdiggørelse. Ved uenighed om faktuelle forhold skal denne uenighed indberettes for Energistyrelsen skriftligt.

Stk. 6. Tilsynsmyndigheden skal senest 1. maj fremsende en årlig redegørelse til Energistyrelsen om det gennemførte tilsynsarbejde jf. stk. 1-4 i det forløbne år.

§ 19. Energistyrelsen fører tilsyn med Energinet.dk's arbejde som virksomhed, som koordinerende virksomhed samt som tilsynsmyndighed for at sikre, at bestemmelserne i denne bekendtgørelse overholdes. Som en del af dette tilsyn skal Energistyrelsen gennemgå de risiko- og sårbarhedsvurderinger, planmateriale og beredskabsplaner, som Energinet.dk udarbejder jf. hhv. §§ 8, 9, 10 og 11, samt kategorisering jf. § 7 stk. 6 og redegørelse jf. § 18, stk. 6.

Stk. 2. Energistyrelsen kan pålægge Energinet.dk at ændre planmateriale og beredskabsplaner, som Energinet.dk udarbejder efter hhv. §§ 9 og 10, såfremt det ikke opfylder kraverne herfor, eller såfremt dette vurderes at være nødvendigt for at opnå en koordineret og effektiv krisehåndtering i relation til andre myndigheder.

Stk. 3. Energistyrelsen kan pålægge Energinet.dk at afholde øvelser jf. § 13, stk. 2 og 3, og at nærmere angivne forhold skal indgå i sådanne øvelser.

Stk. 4. Tilsynet jf. stk. 1 kan delvis baseres på de interne audit, som foretages af Energinet.dk, i det omfang, Energistyrelsen vurderer, at disse interne audit dækker de forhold, der omfattes af tilsynet.

Stk. 5. Energistyrelsen skal udarbejde en årlig rapport om tilsynet med Energinet.dk. Rapporten skal fremsendes til Energinet.dk til kommentering inden færdiggørelse.

Andre bestemmelser

§ 20. Energitilsynet kan jf. bekendtgørelsen om indtægtsrammer for netvirksomheder og regionale transmissionsvirksomheder omfattet af lov om elforsyning efter ansøgning forhøje reguleringsprisen for netvirksomheder, der har dokumenterede meromkostninger som følge af denne bekendtgørelses krav om tilmelding til en it-sikkerhedstjeneste jf. § 27.

Stk. 2. Dokumenterede meromkostninger til it-sikkerhedstjenesten som beskrevet i denne bekendtgørelses § 27 kompenseres i medfør af § 70, stk. 15, i lov om elforsyning.

§ 21. Følsomme oplysninger skal behandles med den fornødne fortrolighed, således at dette materiale ikke kommer uvedkommende i hænde. Materialet kan opbevares i elektronisk form og skal opbevares således, at uautoriseret adgang (såvel fysisk som logisk), ødelæggelse, ændring og offentliggørelse forhindres. Ved følsomme oplysninger forstås:

1. Oplysninger om konkrete risici- og sårbarheder udarbejdet jf. § 8.
2. Planmateriale og udarbejdet jf. § 9.
3. Kritiske dele af beredskabsplaner udarbejdet jf. §§ 10 og 11, indeholdende beskrivelse af, hvordan virksomheden eller sektoren agter at agere i givne beredskabssituationer.
4. Materiale af tilsvarende karakter, der af virksomheden eller Energinet.dk vurderes at være følsomt.

Stk. 2. Forsendelse af materiale om de i stk. 1 nævnte forhold skal ske på en måde, der sikrer fortrolighed og integritet af materialet.

Stk. 3. Hvis følsomt materiale kompromitteres, eller der er formodning om kompromittering, skal skadevirkningerne opgøres og vurderes. Denne opgørelse og vurdering fortages af Energistyrelsen under inddragelse af den pågældende virksomhed og Energinet.dk. Energistyrelsen afgør efter anbefaling fra Energinet.dk og Rigspolitiet, om der er behov for, at materialet eller dele af dette skal ændres. Energistyrelsen kan give pålæg herom til den pågældende virksomhed.

Stk. 4. Fortroligt materiale, der skal destrueres eller slettes grundet erstatning eller udløb, skal destrueres på behørig vis, således at konkrete beskyttelsesværdige informationer ikke kommer uvedkommende i hænde.

§ 22. Energinet.dk skal bidrage til udarbejdelse af sektorspecifikke trusselsvurderinger på vegne af el- og naturgassektorerne. Energistyrelsen udarbejder vejledning herom.

§ 23. Energistyrelsen kan efter ansøgning dispensere fra bestemmelser i denne bekendtgørelse, hvor sådanne bestemmelser i væsentligt omfang har mindre betydning eller reduceret effekt. Energinet.dk skal høres om sådanne ansøgninger.

Sanktioner og klagevejledning

§ 24. Såfremt en virksomhed ikke overholder bestemmelserne i denne bekendtgørelse, kan tilsynsmyndigheden påbyde virksomheden at foretage en it-revision af forsyningskritiske it-systemer ved en uafhængig revisor til afholdelse for virksomhedens egne midler. Virksomheden skal udarbejde en rapport på baggrund af denne it-revision. Denne rapport skal indeholde en tidsplan for udbedring af identificerede risici eller indsatsområder. Denne rapport skal billægges it-revisorens rapport og fremsendes til tilsynsmyndighedens godkendelse.

Stk. 2. Hvis en virksomhed groft eller gentagne gange undlader at efterkomme anbefalinger fremsat af et revisionsfirma efter en it-revision, jf. stk. 1, og herved kan bringe el- eller naturgasforsyningen i fare, kan Energistyrelsen pålægge virksomheden at gennemføre tiltag, som på baggrund af revisorens rapport skønnes nødvendige til opretholdelse af it-sikkerheden.

Stk. 3. Virksomheder, der pålægges nævnte tiltag jf. stk. 1 og 2, kan inden for 10 arbejdsdage klage til Energistyrelsen.

§ 25. Tilsynsmyndighedens afgørelser jf. § 7, stk. 6, § 9, stk. 4 og § 18 kan indbringes for Energistyrelsen. Klagen skal være indgivet skriftligt inden 4 uger efter, at afgørelsen er meddelt.

§ 26. Energistyrelsens afgørelser efter denne bekendtgørelse kan ikke indbringes for anden administrativ myndighed.

It-sikkerhedstjeneste

§ 27. Virksomheder omfattet af § 2 skal være tilmeldt en tjeneste, der yder varsler og informationer om relevante it- sikkerhedstrusler. Virksomheder i kategori 1 og 2 jf. § 7 skal endvidere være tilmeldt en tjeneste, der kan bistå virksomhederne med udredning og reetablering i akutte sikkerhedsmæssige situationer.

Stk. 2. Virksomhederne skal sikre, at oplysninger af sikkerhedsmæssig betydning for andre virksomheder i energisektorerne kan viderebringes til andre virksomheder omfattet af denne bekendtgørelses § 2. Virksomhederne skal sikre sig, at de oplysninger, der tilvejebringes gennem en it-sikkerhedstjeneste jf. stk. 1, skal kunne videreformidles til andre virksomheder uden forsinkelse, såfremt disse oplysninger vurderes at have betydning for forsyningen af el og naturgas.

Stk. 3. Virksomheden skal indsende sin kontrakt med en it-sikkerhedstjeneste til godkendelse ved Energistyrelsen senest den 1. september 2017 og ved ændringer herefter.

Stk. 4. Energistyrelsen kan inden for 8 uger fra fremsendelsen afvise en kontrakt på baggrund af formelle og indholdsmæssige forhold, der vurderes at forsinke, vanskeliggøre eller begrænse virksomhedens eller den samledes sektors evne til at håndtere en akut it-beredskabssituation jf. § 5 og § 6 eller it-beredskabsplanlægning jf. § 10 og § 11. Energistyrelsen kan bl.a. afvise kontrakter med it-sikkerhedstjenester på baggrund af kendskab til den pågældende it-sikkerhedstjenestes kompetenceniveau og ressourcer. Energistyrelsen kan søge faglig bistand til at foretage denne vurdering ved relevante offentlige myndigheder.

Stk. 5. Energistyrelsen kan anmode relevante parter om anbefaling om behovet for fastsættelse af nærmere regler for disse kontrakter.

Stk. 6. Energistyrelsen kan fastsætte nærmere minimumskrav til disse it-sikkerhedstjenester, herunder krav om certificering af centrale funktioner som f.eks. hændelseshåndtering (incident respons) og varslingsformidling. Energistyrelsen kan endvidere af hensyn til national sikkerhed stille krav om

sikkerhedsgodkendelse af medarbejdere ved disse it-sikkerhedstjenester. Disse regler kan differentiere for forskellige virksomhedskategorier jf. § 7.

Stk. 7. Såfremt flere virksomheder i energisektorerne indgår en fælleskontrakt med en it-sikkerhedstjeneste, skal kontrakten med it-sikkerhedstjenesten opbevares ved alle tilmeldte virksomheder. En it-sikkerhedstjeneste, der yder tjenester til flere virksomheder, skal af egen drift videreformidle væsentlige sikkerhedsmæssige oplysninger erkendt ved en virksomhed til andre tilmeldte virksomheder omfattet af § 2 i anonymiseret form.