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 eller dupleres således at forsyningen kan opretholdes og videreføres under ekstraordinære situationer, hvor it-systemernes drift trues, hvad enten truslen skyldes bevidste eller utilsigtede handling eller naturfænomener.

§ 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 for virksomheder, der grundet kommercielle kontrakter har kontrol med fysisk infrastruktur, der forsyner, lagrer eller producerer el eller naturgas.

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 eller angreb på forsyningskritiske it-systemer.

Definitioner

§ 3. I denne bekendtgørelse forstås ved:

Balanceansvarlige virksomheder er virksomheder, der yder balancerende tjenester til energisystemet efter aftale med Energinet.dk.

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.

CSIRT (Computer Security Incident Response Team) er en enhed, der kan varetage it-sikkerhedsmæssige opgaver af såvel proaktiv som reaktiv karakter, herunder leverer informationer om it-sikkerhedstrusler og vejledning om vurdering og mitigering af sårbarheder. Begrebet CSIRT anvendes i denne bekendtgørelse alene om kommercielle it-sikkerhedsydelser.

Cybersikkerhed yder 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 gennem beskrevne procedurer og planer 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 er ansvarlige for egen it-sikkerhed. Virksomheder i kategori 1 og 2 i henhold til § 7, skal tilsikre, at virksomheden kan omsætte informationer om it-sikkerhedstrusler og konkrete it-varsler til at iværksætte de nødvendige tiltag i egen organisation. Dette krav medfører, at virksomheden i sine beredskabsplaner skal beskrive en procedure 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.

Stk. 2. Energinet.dk skal tilsikre at have det fornødne beredskab til håndtering af it-sikkerhedshændelser i egne systemer.

Stk. 3. Energinet.dk skal til enhver tid kunne modtage og videreformidle it-sikkerhedsvarsler og hændelsesoplysninger til virksomheder i el- og naturgassektorerne.

Stk. 4. Energinet.dk skal ikke overtage det lokale operative ansvar ved en it-sikkerhedshændelse, men skal kunne bistå virksomhederne med driftsoplysninger og kommunikation til myndighederne.

Stk. 5. Energinet.dk skal kunne bistå virksomheder omfattet af § 2 med kontaktoplysninger til andre virksomheder omfattet af § 2 eller relevante myndigheder, der kan bidrage til håndteringen af en akut situation.

Organisatoriske forhold

§ 6. Enhver virksomhed efter § 2, stk. 1, skal fastlægge det organisatoriske ansvar for sikring af de it-systemer, der anvendes til styring af virksomhedens produktion eller forsyning af el eller naturgas.

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

Stk. 3. Virksomheden skal udpege en it-beredskabskoordinator, der er ansvarlig for risiko- og sårbarhedsvurdering af de forsyningskritiske it-systemer.

Stk. 4. Virksomheden skal fire gange årligt koordinere mellem den ansvarlige for det almene beredskab (beredskabskoordinatoren), it-beredskabskoordinatoren og ledelsen. Dette kan eksempelvis ske gennem etablering af et internt beredskabsudvalg.

Stk. 5. Personsammenfald mellem it-beredskabskoordinatoren, beredskabskoordinatoren og ledelse skal undgås så vidt muligt. For en virksomhed placeret i kategori tre efter § 7, skal tilsynsmyndigheden underrettes ved personsammenfald. Virksomheder i kategori to efter § 7, skal ansøge tilsynsmyndigheden om tilladelse til et sådan personsammenfald. En sådan ansøgning skal begrundes med, at et personsammenfald er nødvendigt af praktiske årsager og i øvrigt er fagligt forsvarligt. Personsammenfald kan ikke tillades i virksomheder kategoriseret i kategori et efter § 7.

Stk. 6. Alle virksomheder skal etablere en organisering af it-beredskabet, der tilsikrer, at virksomheden kan modtage it-sikkerhedsvarsler. Alle virksomheder skal udarbejde forholdsregler, der sikrer, at den fornødne organisering og relevante tiltag kan iværksættes ved modtagelse af et it-sikkerhedsvarsel. Energinet.dk skal kunne vejlede virksomhederne i forbindelse med etablering af procedurer for modtagelse af trusselsvurderinger og varsler.

Stk. 7. Virksomheder omfattet af denne bekendtgørelse efter § 2, er forpligtiget til at sikre, at leverandører af forsyningskritiske serviceydelser 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 et: 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 to: 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 tre: Øvrige virksomheder, der ikke er omfattet af kategori 1 eller 2, men som er omfattet af § 2.

Stk. 2. 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. 3. Virksomheder, der ejer eller driver anlæg klassificeret af væsentlig betydning for den nationale eller regionale forsyning efter gældende regler, vil blive indplaceret i den tilsvarende kategori, med mindre det kan godtgøres, at anlægget ikke drives af it-systemer.

Stk. 4. Såfremt en virksomhed kan godtgøre at tilhøre en anden kategori efter stk. 1, skal dette meddeles tilsynsmyndigheden. Tilsynsmyndigheden reviderer årligt kategoriseringen efter stk. 1 og 2, senest den 1. februar. Virksomhederne underrettes herom.

Risiko- og sårbarhedsvurderinger

§ 8. Virksomheder efter § 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-systemet eller trusselsbilledet. Virksomheden skal skriftligt dokumentere disse revisioner.

Stk. 2. Risiko- og sårbarhedsvurderinger skal udarbejdes i samråd mellem kompetente personer i organisationen og skal integreres i virksomhedens samlede risikobillede efter § 6. stk. 2. Den interne koordinering af beredskabsarbejdet efter § 6 stk. 4 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.

Stk. 4. Virksomheder i kategori et efter § 7, skal årligt inden 1. maj, fremsende en revideret risiko- og sårbarhedsvurdering til Energinet.dk. Virksomheder i kategori to og tre efter § 7 skal fremsende en revideret risiko- og sårbarhedsvurdering til Energinet.dk minimum hvert tredje år, første gang 1. maj 2017.

Stk. 5. Risiko- og sårbarhedsvurderinger efter stk. 1. skal inddrage alle relevante trusler, herunder egne erfaringer fra øvelser og hændelser efter §§ 13, 14 og 15, samt trusselsvurderinger fra Center for Cybersikkerhed og den tilknyttede CSIRT-tjeneste.

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 sammenhænge med nabolandenes forsyningssystemer. Vurderingerne baseres bl.a. på virksomhedernes og Energinet.dk's vurderinger efter stk. 1, samt planmateriel efter § 9.

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

Stk. 2. Dette planmateriale skal opdateres ved ændringer i it-infrastrukturen.

Stk. 3. Energinet.dk skal udarbejde planmateriale over de driftskritisk informationsudvekslinger, der er 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. 4. Alle virksomheder skal på baggrund af de identificerede indbyrdes relationer, for hver relation vurdere risici mht. tab og kompromittering af data eller kommunikation. Dette planmateriale skal efter anmodning kunne udleveres til Energinet.dk. Energinet.dk kan fastsætte krav til formen for dette planmateriel.
Stk. 5. Virksomheder, der indtager flere væsensforskellige opgaver i el- og naturgassystemet, skal udfylde planmateriel for hver opgave.

§ 10. 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, ødelæggelse, ændring og offentliggørelse forhindres. Ved følsomme oplysninger forstås:

1. Oplysninger om konkrete risici- og sårbarheder udarbejdet efter § 8.
2. Planmateriale og udarbejdet efter § 9
3. Kritiske dele af beredskabsplaner udarbejdet efter §§ 11, 12 og 13, 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. 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, og kan give pålæg herom til den pågældende virksomhed.

Stk. 3. Fortroligt materiale, der skal destrueres eller slettes grundet erstatning eller udløb, skal destrueres på behørig vis, således at konkrete beskyttelsesværdige informationer ikke kommer uvedkommende til hænde.

Beredskabsplanlægning

§ 11. Alle virksomheder skal udarbejde it-beredskabsplaner baseret på de i virksomheden udarbejdede it-risiko- og sårbarhedsvurderinger efter § 8. Disse it-beredskabsplaner skal være en del af virksomhedens samlede beredskabsplanlægning, ligesom disse planer skal være koordineret med sektorberedskabsplanen, som beskrevet i § 12.

Stk. 2. It-beredskabsplaner efter stk.1 skal angive, hvordan virksomheden planlægger at håndtere en it-beredskabssituation. Formålet hermed er at sikre, at situationen normaliseres hurtigst muligt, og herved reducere konsekvenserne af hændelsen.

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

1. En identificering af forsyningskritiske it-systemer og afhængighed af andre systemer.
2. Forebyggende foranstaltninger til at imødegå utilsigtet it-hændelse, 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. Intern ansvars- og rollefordeling under krisestyring.
4. Intern ansvarsplacering af systemansvar for forsyningskritiske it-systemer.
5. Beskrivelse af kommunikation med Energinet/Energistyrelsen samt tilknyttede CSIRT.
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 årligt og senest 3 måneder efter gennemførsel 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.

Stk. 5. Tilsynsmyndigheden kan pålægge virksomheden at revidere sin it-beredskabsplan. Energinet.dk skal vejlede virksomhederne i udarbejdelse af disse beredskabsplaner.

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

§ 12. 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 fra flere regioner, 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 drifts infrastruktur i relevante scenarier.

§ 13. Virksomheder i kategori 2 og 3 kan indgå samarbejdsaftaler, der medfører, at den operative håndtering af it-beredskabssituationer varetages i fællesskab eller af den ene part. En sådan aftale påvirker ikke ansvaret for it-beredskabsplanlægningen, og den enkelte virksomhed er fortsat ansvarlig for planlægning og risikovurdering efter §§ 8, 9, 11 og 12. Den operative struktur skal fremgå af virksomhedernes it-beredskabsplan efter § 11 og § 12, og planmateriel efter § 9, skal være tilgængelige for den operativt ansvarlige part i operative situationer.

Stk. 2. Ansøgninger om samordnet beredskab skal fremsendes til Energistyrelsen. Ansøgningen skal suppleres med en skriftlig begrundelse, samt en beskrivelse af mulige sikkerhedsmæssige konsekvenser ved samordnet beredskab. Denne beskrivelse skal inddrage de seneste risiko- og sårbarhedsvurderinger udarbejdet af de berørte virksomheder.

Stk. 3. 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.

§ 14. 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 efter § 11 stk. 1. Virksomheder i kategori et efter § 7, skal som minimum afholde én årlig it-beredskabsøvelse.

Virksomheder i kategori to og tre efter § 7, skal tilsikre, at it-beredskab trænes i forbindelse med det almene beredskabsarbejde i relevant omfang.

Stk. 3. Energinet.dk skal minimum hvert tredje år afholde it-beredskabsøvelser, der træner anvendelse af sektorberedskabsplanens procedurer for it-beredskabssituationer efter § 12.

Stk. 4. It-beredskabsøvelser skal indgå i virksomhedernes og Energinet.dk's 5-årige øvelsesplan efter gældende regler.

Stk. 5. Energinet.dk skal udarbejde en vejledning, om hvilke øvelser virksomhederne skal 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 en evaluering om hver afholdt øvelse. Øvelsesevalueringen skal angive øvelsens forløb, opnåede erfaringer samt planlagt opfølgning og tidsplan herfor. Endvidere skal evalueringen 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. Denne evaluering erstatter ikke virksomhedernes pligt til omgående at underrette Energinet.dk efter § 15.

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 kan fremsendes til tilsynsmyndigheden én gang årligt.

Stk. 8. Virksomheden skal dokumentere, hvilke awareness-tiltag, der gennemføres med det formål løbende at oplyse og uddanne medarbejdere og eksterne samarbejdsparter og it-medarbejdere om it-sikkerhed i den daglige betjening af driftssystemer og kontorsystemer. Virksomheder i kategori et efter § 7, skal som minimum gennemføre awareness-tiltag årligt for alle personalegrupper, mens virksomheder i kategori to og tre skal gennemføre awareness-tiltag for it-medarbejdere årligt og andre medarbejdere som minimum hvert andet år.

§ 15. It-sikkerhedshændelser der i væsentlig grad reducerer virksomhedens funktionalitet eller funktionaliteten af andre dele af el- og naturgassektoren, skal omgående meddeles Energinet.dk. Energinet.dk skal omgående underrette Energistyrelsen, såfremt it-sikkerhedshændelsen er af betydning for el- eller naturgasforsyningen på nationalt niveau. Som eksempler kan nævnes, at nedbrud på anlæg m.m. af betydning for den nationale eller regionale forsyning omgående skal rapporters til Energinet.dk.

Stk. 2. Såfremt en it-sikkerhedshændelse vurderes at have indflydelse på andre virksomheders eller myndigheders it-beredskab, skal væsentlige informationer omgående viderebringes til Energinet.dk og den CSIRT virksomheden er tilknyttet. Energinet.dk skal vurdere, om disse informationer skal viderebringes til Center for Cybersikkerhed, Energistyrelsen samt andre virksomheder i energisektorerne. Denne forpligtigelse til at vurdere og videreformidle akutte hændelsesinformationer kan overdrages fra Energinet.dk til en CSIRT-tjeneste, efter tilladelse fra Energistyrelsen.

Hændelser

§ 16. 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 CSIRT, Forsvarets Center for Cybersikkerhed eller Energinet.dk.
- Hændelser der vurderes at kunne give anledning til læring eller ændrede proaktive handlinger ved andre virksomheder.

- Ved tvivl om behovet for hændelsesevaluering kan virksomhederne rådføre sig med Energinet.dk.

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 endvidere 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 efter § 15.

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

Stk. 4. Hvis en hændelse efter stk. 1 i væsentligt omfang har afprøvet konkrete forhold, som indgår i en planlagt øvelse i virksomhedens 5-årige øvelsesplan, jf. § 14, 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 efter stk. 1.

Sikringsforanstaltninger

§ 17. En virksomhed skal sikre, at lokaliteter indeholdende forsyningskritiske it-systemer beskyttes i henhold til disse forsyningskritiske systemers kritikalitet for forsyningen på nationalt, regionale eller lokalt niveau.

Stk.2 Beskyttelse efter stk. 1 indebærer etablering af procedurer og forholdsregler, jf. gældende bestemmelser.

Stk. 3 Virksomheden skal sikre forsyningskritiske it-systemer i stk. 1 mod uautoriseret adgang såvel logisk adgang som fysisk adgang.

Leverandørstyring

§ 18. Virksomheden bærer det fulde ansvar for de it-sikkerhedsmæssige aspekter i forbindelse med anvendelse af ekstern leverandører til såvel service, vedligeholdelse, drift, styring og monitering af virksomhedens it-systemer. Virksomheder der anvender en leverandør til styring af egen it-sikkerhed, skal kunne dokumentere, at denne leverandør efterlever kravene i denne bekendtgørelse.

Stk. 2. Virksomheden skal etablere procedurer for adgangsstyring af leverandører af forsyningskritiske it-systemer. 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 er følsomme, håndteres med den fornødne sikkerhed. Herunder forstås følsomme oplysninger som oplysninger, der kan anvendes til at få uberettiget adgang til forsyningskritiske it-systemer og kritiske driftssystemer. Den fornødne sikkerhed omfatter:

1. at virksomheden i relation til leverandører bevarer ejerskab af disse 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 af styring af leverandører ved at anvende en ekstern it-revisor. Tilsynsmyndigheden kan dog forlange, at virksomhedens ledelse godtgøre for overvejelser i relation til en sådan disposition.

Tilsyn

§ 19. Energinet.dk varetager opgaven som tilsynsmyndighed overfor virksomhedernes efterlevelse af reglerne i denne bekendtgørelse efter § 1. Tilsynsmyndigheden fører tilsyn med virksomhederne efter § 2, dog ikke Energinet.dk eller et helejet datterselskab. Tilsynsmyndigheden gennemfører it-beredskabstilsyn

ved virksomheder i kategori et efter § 7 årligt. Ved resterende virksomheder gennemføres it-beredskabsstilsynet sammenfaldende med det tre-årlige beredskabstilsyn.

Stk. 2. 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.

Stk. 3. Tilsynsmyndigheden kan pålægge en virksomhed at ændre dens planmateriale efter § 11 og andre dele af dens beredskabsarbejde, såfremt det ikke opfylder reglerne herfor, 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 § 14, stk. 2, og at nærmere angivne forhold skal indgå i sådanne øvelser.

Stk. 4. Tilsynsmyndigheden skal udarbejde en rapport om tilsynet med den enkelte virksomhed. Rapporten skal forelægges virksomheden til kommentering inden færdiggørelse. Ved uenighed om faktuelle forhold skal denne uenighed indberettes for Energistyrelsen skriftligt.

Stk. 5. Tilsynsmyndigheden skal fastsætte en tidsplan for sit tilsyn med virksomhedernes it-beredskabsarbejde. Tilsynsmyndigheden foretager tilsyn med hver virksomhed i kategori et efter § 7 årligt og for resterende virksomheder mindst hvert tredje år.

Stk. 6. Tilsynsmyndigheden skal senest 1. maj fremsende en årlig redegørelse til Energistyrelsen om dets tilsynsarbejde efter stk. 1-5 i det forløbne år.

§ 20. Energistyrelsen fører tilsyn med Energinet.dk's arbejde som virksomhed, overordnede som koordinerende virksomhed samt som tilsynsmyndighed for at sikre, at det opfylder reglerne i denne bekendtgørelse. Som en del af dette tilsyn skal Energistyrelsen gennemgå de risiko- og sårbarhedsvurderinger, planmateriel og beredskabsplaner, som Energinet.dk udarbejder efter hhv. §§ 8, 9, 11 og 12, samt kategorisering efter § 7 stk. 4 og redegørelse anført i § 19, stk. 6.

Stk. 2. Energistyrelsen kan pålægge Energinet.dk at ændre planmateriale og beredskabsplaner, som Energinet.dk udarbejder efter hhv. §§ 9 og 11, såfremt det ikke opfylder reglerne 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 efter § 14, stk. 2 og 3, og at nærmere angivne forhold skal indgå i sådanne øvelser.

Stk. 4. Tilsynet efter 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

§ 21. Energitilsynet kan efter ansøgning forhøje reguleringsprisen for netvirksomheder, der har dokumenterede meromkostninger som følge af denne bekendtgørelse efter reglerne i bekendtgørelsen om indtægtsrammer for netvirksomheder og regionale transmissionsvirksomheder omfattet af lov om elforsyning.

Stk. 2. Dokumenterede meromkostninger til proaktive varslingstjeneste som beskrevet i denne bekendtgørelses § 5, kompenseres i medfør af § 70, stk. 7, 2. pkt. i lov om elforsyning. Kompensationen kan beregnes ved brug af standardiserede forudsætninger, jf. stk. 3.

Stk. 3. Energitilsynet kan fastsætte standardiserede forudsætninger for forhøjelse af reguleringsprisen som følge af dokumenterede meromkostninger.

Stk. 4. Øgede driftsomkostninger som følge af udgifter til kompetenceudvikling af egne medarbejder afholdes inden for den hidtidige indtægtsramme.

Stk. 5. Netvirksomheder kan alene ansøge Energitilsynet om kompensation for dokumenterede meromkostninger, jf. stk. 1, én gang årligt for meromkostninger i det foregående regnskabsår. Retten til at få godkendt en indtægtsrammeforhøjelse som følge af meromkostningerne bortfalder, såfremt ansøgningen ikke foreligger i Energitilsynet senest den 31. maj i regnskabsaflæggelsesåret.

Stk. 6. Omkostninger ved virksomhedernes beredskabsarbejde inden for it-sikkerhedsområdet afholdes af virksomhederne selv.

§ 22. Energinet.dk skal bidrage til udarbejdelse af sektorspecifikke trusselsvurderinger i regi af Center for Cybersikkerhed på vegne af el- og naturgassektorerne. Energistyrelsen udarbejder i samarbejde med Center for Cybersikkerhed en 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 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 ved 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 revisors rapport skønnes nødvendige til opretholdelse af it-sikkerheden.
Stk. 3. Virksomheder, der pålægges nævnte tiltag efter stk. 1 og 2, kan indenfor 10 arbejdsdage klage til Energistyrelsen. Energistyrelsen kan træffe endelig afgørelse.

§ 25. Tilsynsmyndighedens afgørelser efter § 7, stk. 4, § 9, stk. 4 og § 19 kan indbringes for Energistyrelsen. Klage 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.

CSIRT

§ 27. Virksomheder efter § 2 skal være tilmeldt en tjeneste, der yder varsler og informationer om relevante it-sikkerhedstrusler. Virksomheder i kategori 1 og 2 efter § 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 bekendtgørelse efter § 2. Virksomhederne skal derfor sikre sig, at de oplysninger, der tilvejebringes gennem en CSIRT-tjeneste efter stk. 1., skal kunne videreformidles til andre virksomheder uden forsinkelse, såfremt disse oplysninger vurderes at have sikkerhedsmæssig betydning for forsyningen af el og naturgas af mere end 30.000 forbrugere.

Stk. 3. Virksomheden skal indsende sin kontrakt med en CSIRT-tjeneste til godkendelse ved Energistyrelsen senest 1. juli 2017, og ved ændringer herefter. 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 efter § 4 og § 5 eller it-beredskabsplanlægning efter § 11 og § 12. Energistyrelsen kan afvise kontrakter med CSIRT-tjenester på baggrund af kendskab til den pågældende CSIRT-tjenestes kompetenceniveau og ressourcer. Energistyrelsen kan søge faglig bistand til at foretage denne vurdering ved relevante offentlige myndigheder, herunder Center for Cybersikkerhed.

Stk. 4. Energinet.dk skal den 1. november hvert år afgive anbefaling til Energistyrelsen om behovet for fastsættelse af nærmere regler for disse kontrakter.

Stk. 5. Energistyrelsen kan fastsætte nærmere minimumskrav til disse CSIRT-tjenester, herunder krav om certificering af centrale funktioner som f.eks. hændelseshåndtering (incident respons) og varslingsformidling. Energistyrelsen kan endvidere stille krav om sikkerhedsgodkendelse af CSIRT og herunder CSIRT-medarbejder af hensyn til national sikkerhed. Disse regler kan differentiere mellem forskellige virksomhedskategorier efter § 7.

Stk. 6. Såfremt flere virksomheder i energisektorerne indgår en fælleskontrakt med en CSIRT-tjeneste, skal kontrakten med CSIRT-tjenesten opbevares ved alle tilmeldte virksomheder. En CSIRT-tjeneste, 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.