energiavirasto
energimyndigheten

Anvisning för aktörer som övervakas av Energimyndigheten om iakttagande av cybersäkerhetslagen

1721/040002/2025

Cybersäkerhetslagen inom energisektorn

ANVISNING FÖR AKTÖRER SOM ÖVERVAKAS AV ENERGIMYNDIGHETEN OM IAKTTAGANDE AV CYBERSÄKERHETSLAGEN

1721/040002/2025

Energiavirasto
Energimyndigheten
Lintulahdenkuja 2 A
FI-00530 Helsinki
Puhelin 029 505 0000
S-posti kirjaamo@energiavirasto.fi
Internet www.energiavirasto.fi

1721/040002/2025

Innehåll

Versionshistoria

Version	Datum	Viktigaste ändringar
1	8.4.2025	Första versionen
2	11.4.2025	Hänvisningen till elbilar har tagits bort från avsnittet om laddningsoperatörer. Den svenska översättningen har ändrats för att motsvara lagens översättning.
3	1.10.2025	Tillägg om småskalig elproduktion och Energimyndighetens tolkning att enbart elproduktion som är småskalig kan anses vara ringa.

1 Bakgrund

1.1 Allmänt om cybersäkerhetslagen och NIS2-direktivet

Cybersäkerhetslagen (124/2025) innehåller bestämmelser om riskhantering och anmälan om incidenter i fråga om cybersäkerhet. Cybersäkerhetslagen är en nationell lag genom vilken cybersäkerhetsdirektivet, dvs. NIS2-direktivet (EU) 2022/2555, har verkställts[1].

Syftet med NIS2-direktivet är att säkerställa en enhetlig hög nivå på cybersäkerheten i hela Europeiska unionen. NIS2-direktivet har ersatt det tidigare direktivet om nät- och informationssäkerhet (NIS1-direktivet), vars tillämpningsområde i Finland har omfattat elnätsinnehavare och innehavare av överföringsnät för naturgas inom energisektorn. I och med NIS2-direktivet gäller cybersäkerhetsskyldigheterna en större grupp än tidigare och är mer detaljerade än tidigare. Ändringarna i elmarknadslagen (588/2013) och naturgasmarknadslagen (587/2017) som gjordes i och med NIS1-direktivet har upphävts. På el- och naturgasnätsinnehavarna tillämpas skyldigheterna i cybersäkerhetslagen på samma sätt som på andra företag som omfattas av lagen.

Cybersäkerhetslagen är en gemensam allmän lag som gäller alla branscher. Inom energisektorn omfattas aktörer inom el, fjärrvärme och fjärrkyla, gas, olja och vätgas av lagstiftningen.

Observera: Energimyndigheten och Säkerhets- och kemikalieverket (Tukes) är tillsynsmyndigheter inom energisektorn. Denna anvisning gäller endast aktörer inom energisektorn som övervakas av Energimyndigheten. De aktörer som Tukes övervakar ska bekanta sig med Tukes anvisningar om cybersäkerhetslagen.

1.2 Anvisningens mål och karaktär

I denna anvisning har vi samlat information om efterlevnaden av cybersäkerhetslagen för de aktörer inom energisektorn som Energimyndigheten övervakar. Andra aktörer bör vända sig till den NIS2-myndighet som övervakar aktörstypen i fråga. I denna anvisning har man till exempel inte beaktat eventuella undantag som gäller andra sektorer.

Energimyndigheten uppdaterar denna anvisning efter behov. Den mest aktuella versionen publiceras på Energimyndighetens webbplats (https://energiavirasto.fi/sv/cybersakerhet) och i anvisningarna för VERTTI-tillsynsuppgiftssystemet.

Aktörerna måste själva identifiera om de omfattas av cybersäkerhetslagen. Aktörer som omfattas av lagen ska på eget initiativ anmäla sig till den myndighet som övervakar den till aktörsförteckningen, dit aktören anmäler basuppgifter om företagets verksamhet och kontaktuppgifter. Den första anmälan ska göras senast

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

8.5.2025. De aktörer som Energimyndigheten övervakar anmäler uppgifterna till VERTTI-tillsynsuppgiftssystemet, där man loggar in med Suomi.fi-fullmakt. Före anmälan ska aktörerna noggrant bekanta sig med denna anvisning och anvisningarna för ifyllande i VERTTI-tillsynsuppgiftssystemet (kapitel 6).

Med denna anvisning får de aktörer som Energimyndigheten övervakar utöver tillämpningsområdet för cybersäkerhetslagen en allmän uppfattning om skyldigheterna enligt cybersäkerhetslagen, inklusive riskhantering, anmälan om incidenter (NIS-anmälan) samt Energimyndighetens tillsyn över aktörerna.

Energimyndigheten ger denna anvisning som en rekommendation. Anvisningen hänvisar dock till juridiskt bindande skyldigheter som föreskrivs i cybersäkerhetslagen. Bestämmelser om rättsliga skyldigheter finns dessutom i andra lagar, såsom eventuella genomförandeakter från kommissionen och eventuella separata myndighetsföreskrifter. Denna anvisning är inte ett uttömmande presentation av cybersäkerhetslagen eller NIS2-direktivet, men den stöder aktörerna i fullgörandet av sina skyldigheter enligt cybersäkerhetslagen och NIS2-direktivet.

2 Lagstiftning som berör ärendet

2.1 Cybersäkerhetslagen

Cybersäkerhetslagen har publicerats i lagwebbtjänsten Finlex: https://finlex.fi/sv/lagstiftning/forfattningssamling/2025/124

3 Tillämpningsområde

3.1 Allmänt om tillämpningsområdet och myndigheternas behörighetsfördelning

Cybersäkerhetslagen tillämpas på juridiska och fysiska personer som bedriver sådan verksamhet som avses i bilaga I eller II till lagen eller som är sådana aktörer som avses i de nämnda bilagorna. För att ovan nämnda aktör ska omfattas av cybersäkerhetslagen ska den vara tillräckligt stor eller så ska dess verksamhet oberoende av storlek anses vara kritisk. Företag som omfattas av cybersäkerhetslagen kallas aktörer.

I 3 § i cybersäkerhetslagen föreskrivs om definitionen av aktör, det vill säga vilka aktörer som omfattas av lagens tillämpningsområde. I paragrafens 1 mom. föreskrivs om en allmän definition av en aktör som är tudelad i fråga om arten eller typen av aktörens verksamhet och aktörens storlek. I 2 och 3 mom. föreskrivs om specialfall där aktören omfattas av lagens tillämpningsområde oberoende av dess storlek. I fråga om vissa aktörer föreskrivs om begränsningar av lagens tillämpningsområde i 4 §. I fråga om internationella aktörer föreskrivs om jurisdiktion och territorialitet i 6 §[2].

[2] Se RP 57/2024 rd. Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet), s. 149.

I detta kapitel behandlas vad företaget ska beakta när det utreder om företaget omfattas av tillämpningsområdet för cybersäkerhetslagen och till vilken tillsynsmyndighet företaget ska anmäla sig till aktörsförteckningen. I kapitel 3.2 behandlas vilken typ av verksamhet som hör till lagens tillämpningsområde. I kapitlen 3.3 och 3.4 specificeras när ett företag som bedriver verksamhet som nämns i bilagan till lagen omfattas av lagens tillämpningsområde. I kapitel 3.5 behandlas aktörer som med stöd av CER-direktivet[3] har förklarats kritiska och huruvida dessa omfattas av cybersäkerhetslagen.

De aktörer som omfattas av tillämpningsområdet indelas i viktiga och väsentliga aktörer. Medelstora företag är viktiga entiteter. Väsentliga aktörer är aktörer som överskrider definitionen av ett medelstort företag, alltså stora företag, kritiska entiteter enligt CER-direktivet och andra aktörer som oberoende av storlek definierats som väsentliga aktörer. Mer information om indelningen i viktiga och väsentliga aktörer finns i kapitel 3.6.

Inom energisektorn omfattas aktörer inom el, fjärrvärme och fjärrkyla, gas, olja och vätgas av lagen. Energimyndigheten och Säkerhets- och kemikalieverket (Tukes) är tillsynsmyndigheter inom energisektorn. Tillsynsmyndigheten beror på den verksamhet som aktören bedriver. I kapitel 3.2 specificeras närmare vem som är tillsynsmyndighet för varje verksamhet som omfattas av lagen och till vilken myndighet aktören då ska anmäla sig till aktörsförteckningen.

Ett flerbranschföretag kan vara en aktör som övervakas av flera myndigheter, om företaget bedriver flera verksamheter enligt bilagan till lagen och verksamheterna övervakas av olika myndigheter. Så är fallet till exempel om företaget är elproducent (tillsynsmyndighet Energimyndigheten), fjärrvärmedistributör (tillsynsmyndighet Energimyndigheten) och operatörer av oljeledningar (tillsynsmyndighet Säkerhets- och kemikalieverket). På motsvarande sätt kan företaget också bedriva flera verksamheter som omfattas av lagen, men alla dessa verksamheter övervakas av samma myndighet. Till exempel ett företag som endast bedriver fjärrvärmedistribution och elproduktion är en aktör som endast övervakas av Energimyndigheten.

En aktör enligt cybersäkerhetslagen ska anmäla sig separat till alla myndigheter som övervakar den i aktörsförteckningen (cybersäkerhetslagen 41 §, se kapitel 4.1 och 6).

3.2 Verksamhet eller aktör inom energisektorn som omfattas av tillämpningsområdet

Enligt 3 § i cybersäkerhetslagen tillämpas lagen på juridiska och fysiska personer (aktörer) som bedriver verksamhet enligt bilaga I eller II eller är sådana aktörer som avses i nämnda bilagor. Inom energisektorn omfattas aktörer inom el, fjärrvärme och fjärrkyla, gas, olja och vätgas av lagen.

[3] Europaparlamentets och rådets direktiv om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG
(CER-direktivet).

Cybersäkerhetslagen är en allmän lag som omfattar flera verksamhetsområden. I denna anvisning behandlas endast aktörer som bedriver verksamhet inom energisektorn och i synnerhet aktörer som övervakas av Energimyndigheten. Företag som bedriver annan verksamhet ska kontrollera tillämpningsområdet i cybersäkerhetslagen och hos den myndighet som övervakar verksamheten i fråga.

Med tanke på definitionen av aktör är det inte av betydelse vilken juridisk form aktören har, utan endast huruvida aktören bedriver sådan verksamhet som avses i paragrafen eller är en sådan typ av aktör som avses i paragrafen samt uppfyller storleksvillkoret enligt 1 mom. eller omfattas av undantaget från tillämpningen enligt 2 eller 3 mom. oberoende av aktörens storlek.[4]

Med bedrift av verksamhet avses i huvudsak den aktör i vars namn den verksamhet som nämns i bilagan faktiskt bedrivs.[5] Om aktören till exempel genom avtal har ordnat service, driftsövervakning eller annan operativ verksamhet för någon annan aktör, betraktas denna aktör som tjänsteproducent i förhållande till den aktör i vars namn verksamheten bedrivs. Elproduktion bedrivs till exempel av den instans i vars namn el produceras (säljs vidare). Nedan i kapitel 3.3.2 i denna anvisning behandlas hur lagens tillämpningsområde bestäms till exempel i fråga om aktieägare och företag i koncernform. Energimyndigheten betonar att aktören ska sörja för riskhanteringen för tjänsteproducenterna (se 9 § 2 mom. i cybersäkerhetslagen. 4 punkten och kapitel 4.2-4.3 i denna anvisning).

Finlands cybersäkerhetslag tillämpas i regel på aktörer som är etablerade i Finland (6 § 1 mom. i cybersäkerhetslagen).[6] Tillämpningsområdet för finsk lag omfattar en aktör som är etablerad i Finland i sin helhet, dvs. också de av aktörens funktioner som finns till exempel i en annan medlemsstat eller i tredjeländer. Om verksamhet som omfattas av tillämpningsområdet för NIS 2-direktivet i Finland bedrivs eller tjänster tillhandahålls av en aktör som är etablerad i en annan EU-medlemsstat, omfattas aktören i regel och på motsvarande sätt av lagstiftningen och laglighetsövervakningen i etableringsstaten.[7]

Inom energisektorn omfattas aktörer inom el, fjärrvärme och fjärrkyla, gas, olja och vätgas av cybersäkerhetslagen. Energimyndigheten och Säkerhets- och kemikalieverket (Tukes) är tillsynsmyndigheter inom energisektorn. Energimyndigheten övervakar följande aktörer:

- nätinnehavare av el och naturgas
- distributörer av fjärrvärme och fjärrkyla

[4] RP 57/2024 rd., s. 149.

[5] Observera: Cybersäkerhetslagen omfattar laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn.

[6] Enligt 6 § 1 mom. i cybersäkerhetsdirektivet tillämpas lagen på aktörer som är etablerade i Finland, om inte något annat föreskrivs i lag eller följer av Europeiska unionens lagstiftning eller internationella förpliktelser som är bindande för Finland. I 2-3 mom. i bestämmelsen i fråga specificeras vissa aktörer på vilka tillämpas principer som avviker från 1 mom. Avvikelserna omfattar inte verksamhet eller aktörstyper inom energisektorn.

[7] RP 57/2024 rd., s. 162.

- operatörer för anläggningar för överföring av vätgas
- leverantörer av el och naturgas, dvs. säljare, inklusive återförsäljare
- elproducenter
- laddningsoperatörer
- nominerade elmarknadsoperatörer
- andra parter på elmarknaden som erbjuder aggregering, efterfrågeflexibilitet eller lagring av energi

I tabellen nedan presenteras verksamhet och aktörer enligt bilagan till cybersäkerhetslagen samt den myndighet som övervakar dessa. Tabellen omfattar endast aktörer inom energisektorn, dvs. företag som också bedriver annan verksamhet, ska kontrollera att lagen omfattas av cybersäkerhetslagen.

Verksamhet eller aktör inom energisektorn som omfattas av lagen	**Observationer om aktören**	**Tillsynsmyndighet**
El		
Elföretag enligt 3 § 1 mom. 21 punkten i elmarknadslagen (588/2013) som bedriver elleverans enligt 11 punkten i momentet	Med elleverans avses elförsäljning till kunder eller återförsäljning. Med kund avses såväl grossist som slutförbrukare av el. Elföretag som bedriver elleverans är elförsäljare och återförsäljare. Detaljförsäljning är verksamhet som omfattas av lagen.[8] Cybersäkerhetslagens tillämpningsområde omfattar till exempel inte de balansansvariga parter som definieras i artikel 2.14 i förordning (EU) 2019/943 i denna roll. Om det företag som är	Energimyndigheten

[8] Enligt Energimyndighetens utlåtande (3603/040003/2024) är tillhandahållandet av en laddningstjänst för elfordon inte detaljförsäljning med el eller elleverans. Tillämpningsområdet för cybersäkerhetslagen omfattar dock separat laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn.

	balansansvarig part dock bedriver sådan annan verksamhet som nämns i bilagan till lagen (till exempel elleverans) hör det till lagens tillämpningsområde.	
Distributionsnätsinnehavare som avses i 3 § 1 mom. 10 punkten i elmarknadslagen	Distributionsnätsinnehavare inklusive innehavare av slutna distributionsnät samt högspänningsdistributionsnät	Energimyndigheten
Stamnätsinnehavare enligt 7 § i elmarknadslagen		Energimyndigheten
Producenter som avses i 3 § 1 mom. 15 punkten i elmarknadslagen	Cybersäkerhetslagen tillämpas inte på aktörer vars verksamhet är sporadisk och ringa. Som sporadisk och ringa verksamhet anses till exempel produktion av el huvudsakligen för eget bruk med hjälp av en solpanel eller vindgenerator, där en kvantitativt liten överproduktion tidvis matas in i elnätet.[9] Enligt Energimyndighetens tolkning kan produktion anses vara ringa endast om den klassificeras som småskalig elproduktion. Denna gräns är vid tidpunkten för anvisningens publicering högst två megavoltampere.[10]	Energimyndigheten
Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU)		Energimyndigheten

[9] Cybersäkerhetslagen 4 § 5 mom. och RP 57/2024 rd., s. 158.
[10] Elmarknadslagens 3 § 14 punk. I regeringens proposition (RP 45/2025 rd) föreslås att gränsen för småskalig produktion sänks från två megavoltampere till under en megavoltampere.

2019/943 om den inre marknaden för el		
Parter på elmarknaden enligt 3 § 1 mom. 37 punkten i elmarknadslagen som tillhandahåller aggregering enligt 3 § 1 mom. 21 a punkten i elmarknadslagen, efterfrågeflexibilitet enligt 30 a punkten eller energilagring enligt 21 c punkten		Energimyndigheten
Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn		Energimyndigheten
Fjärrvärme och fjärrkyla		
Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i punkt 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 om främjande av användningen av energi från förnybara energikällor	Tillämpningsområdet omfattar operatörer av fjärrvärme eller fjärrkyla, det vill säga distributörer av fjärrvärme och fjärrkyla. Operatörer av fjärrvärme eller fjärrkyla som inte alls bedriver distribution skulle uteslutas från tillämpningsområdet.[11]	Energimyndigheten
Gas		
Distributionsnätsinnehavare som avses i 3 § 1 mom. 10 punkten i naturgasmarknadslagen (587/2017)	Distributionsnätsinnehavare inklusive innehavare av slutna distributionsnät	Energimyndigheten

[11] RP 57/2024 rd., s. 152.

Överföringsnätsinnehavare som avses i 3 § 1 mom. 9 punkten i naturgasmarknadslagen		Energimyndigheten
Naturgasleverantörer som avses i 3 § 1 mom. 14 punkten i naturgasmarknadslagen	Med leverans av naturgas avses försäljning och återförsäljning av naturgas och kondenserad naturgas till kunder. Med kund avses en grossist och en slutförbrukare av naturgas samt ett naturgasföretag som köper naturgas. Naturgasleverantörer är detaljförsäljare, shippers och traders.	Energimyndigheten
Innehavare av en lagringsanläggning som avses i 3 § 1 mom. 20 punkten i naturgasmarknadslagen		Tukes
Innehavare av en behandlingsanläggning för kondenserad naturgas som avses i 3 § 1 mom. 22 punkten i naturgasmarknadslagen		Tukes
Naturgasföretag som avses i 3 § 1 mom. 18 punkten i naturgasmarknadslagen	Distributionsnätsinnehavare, överföringsnätsinnehavare och naturgasleverantörer hör dock till de aktörer som Energimyndigheten övervakar.	Tukes
Operatörer av raffinaderier och bearbetningsanläggningar för naturgas		Tukes
Olja		
Operatörer av oljeledningar		Tukes

Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja		Tukes
Centrala lagringsenheter enligt definitionen i punkten 2 f i rådets direktiv 2009/119/EG om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter		Tukes
Vätgas		
Operatörer för anläggningar för produktion och lagring av vätgas		Tukes
Operatörer för anläggningar för överföring av vätgas		Energimyndigheten

Mer information om den verksamhet som ingår i bilagorna till cybersäkerhetslagen finns i cybersäkerhetslagen: https://finlex.fi/sv/lagstiftning/forfattningssamling/2025/124

Cybersäkerhetslagen tillämpas inte på aktörer vars verksamhet enligt bilaga I eller II är sporadisk och ringa (4 § 5 mom. i cybersäkerhetslagen). Huruvida verksamheten är sporadisk och ringa ska bedömas i förhållande till verksamhetens varaktighet, huvudsakliga syfte och omfattning samt till antalet personer eller kunder som är beroende av verksamheten. Som sporadisk och ringa verksamhet anses till exempel produktion av el huvudsakligen för eget bruk med hjälp av en solpanel eller vindgenerator, där en kvantitativt liten överproduktion tidvis matas in i elnätet.[12] Enligt Energimyndighetens tolkning är elproduktion som inte kan klassificeras som småskalig elproduktion inte heller att betrakta som ringa.

Energimyndigheten betonar att det ovanstående är ett undantag och att det ska tolkas snävt. Undantaget motiveras i regeringens proposition så att det behövs för att lagens tillämpningsområde inte i strid med lagens syfte ska utvidgas till att på grund av ringa eller tillfällig verksamhet som avses i bilaga I eller II i sin helhet

[12] RP 57/2024 rd., s. 158–159.

omfatta en juridisk eller fysisk person vars verksamhet annars uppfyller eller överskrider definitionen av en medelstor aktör, men som i övrigt inte skulle omfattas av lagens tillämpningsområde.[13]

I cybersäkerhetslagen föreskrivs också att lagen inte tillämpas på verksamhet eller tjänster som tillhandahålls för tryggande av försvaret, den nationella säkerheten, allmän ordning och säkerhet eller förebyggande av brott, brottsutredning och väckande av åtal (4 § 1–2 mom. i cybersäkerhetslagen).

3.3 Aktörer som omfattas av tillämpningsområdet på basis av storleksklass

3.3.1 Allmänt om fastställande av storleksklass

Ovan i kapitel 3.2 beskrivs hurdan verksamhet som omfattas av cybersäkerhetslagen. För att en aktör inom energisektorn ska omfattas av cybersäkerhetslagen krävs dock utöver en viss verksamhet att företaget är tillräckligt stort eller att dess verksamhet annars anses vara kritisk. I detta kapitel 3.3 behandlas hur aktörens storlek bestämmer om aktören omfattas av lagen. I kapitlen 3.4 och 3.5 behandlas aktörer som omfattas av cybersäkerhetslagen oberoende av storleken.

För att en aktör som bedriver sådan verksamhet som nämns i kapitel 3.2 ska omfattas av lagen ska den uppfylla eller överskrida de villkor för medelstora företag som anges i artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG. Artikel 3.4 i bilagan till rekommendationen tillämpas inte vid definitionen av aktör. Kommissionens rekommendation finns här: EUR-Lex - 32003H0361 - SV - EUR-Lex.

En ytterligare förutsättning är att aktören tillhandahåller tjänsten eller bedriver sin verksamhet inom Europeiska unionen (se även kapitel 3.2).

Aktören ska identifiera om den uppfyller definitionen av medelstort företag eller om den överskrider tröskelvärdena för definitionen av medelstort företag. Detta har betydelse för om aktören är en viktig eller väsentlig aktör enligt 27 § i cybersäkerhetslagen. Viktiga och väsentliga aktörer behandlas närmare i kapitel 3.6.

I kommissionens rekommendation fastställs maximistorleken för mikroföretag, små företag och medelstora företag. Företag som överskrider definitionen av ett medelstort företag är stora företag. I denna anvisning går vi i stora drag igenom hur aktören definierar sin storlek enligt kommissionens rekommendation. Det har också publicerats en användarhandledning för kommissionens rekommendation som innehåller åskådliga exempel på definitionen av aktörens storlek. Användarhandledningen finns här: Användarhandledning om definitionen av SMF-företag (europa.eu)

Aktören uppfyller definitionen av ett medelstort företag när det överskrider ramvillkoren för definitionen av ett litet företag, men inte överskrider de maximitröskelvärden som fastställts för små och medelstora företag. Aktören uppfyller således definitionen av en medelstor aktör om den har minst 50 anställda eller om dess

[13] RP 57/2024 rd., s. 159.

årliga omsättning och balansräkning överstiger 10 miljoner euro. Om aktören har färre än 50 anställda, men både omsättningen och balansräkningen överstiger 10 miljoner euro, uppfyller aktören definitionen av en medelstor aktör. Om aktören har färre än 50 anställda, och antingen omsättningen eller balansräkningen, men inte båda, överskrider 10 miljoner euro, uppfyller aktören inte definitionen av en medelstor aktör.

Aktören överskrider definitionen av ett medelstort företag när den överskrider maximitröskelvärdena för definitionen av små och medelstora företag i kommissionens rekommendation. Aktörer som överskrider tröskelvärdena är stora företag som har minst 250 anställda eller vars årliga omsättning överstiger 50 miljoner euro och balansräkningen är över 43 miljoner euro. Om aktören har färre än 250 anställda, men både den årliga omsättningen och balansräkningen överstiger tröskelvärdena i fråga, överskrider aktören definitionen av en medelstor aktör.

Vid bedömningen av huruvida storlekskriterierna uppfylls och överskrids är det viktigt att beakta att tröskelvärdena enligt kommissionens rekommendation avviker till exempel från tröskelvärdena enligt bokföringslagen (1336/1997).

Bedömningen görs aktörsspecifikt och definitionen tolkas enligt rättssubjekt.

För att aktören ska kunna fastställa om den uppfyller eller överskrider ovan nämnda tröskelvärden ska den granska vilka uppgifter som ska beaktas och bedömas mot tröskelvärdena. I uppgifterna om personalen, omsättningen och balansräkningen ska omfattningen av aktörens verksamhet beaktas i sin helhet, inte endast i fråga om den verksamhet som avses i bilagan till cybersäkerhetslagen.[14] Om en aktör bedriver verksamhet inom flera olika näringsgrenar och endast en del av verksamheten utgörs av sådan verksamhet som avses i bilagan till cybersäkerhetslagen, ska aktörens verksamhet som helhet beaktas vid bedömningen av storleken. Bedömningen av huruvida gränsen överskrids bör alltså inte begränsas till den verksamhet som avses i bilagan eller till exempel kapitel 3.2. Följaktligen ska omsättningen, balansräkningen och antalet anställda bedömas för hela aktören, vilket omfattar också annan verksamhet än sådan som avses i bilagan. Ett undantag från detta är dock den begränsning som föreskrivs senare i kapitel 3.3.3 och cybersäkerhetslagens 4 § 6 mom. i det fall att verksamhet som avses i bilagan till lagen bedrivs av en kommun.[15]

Det viktigaste är att aktören kan fastställa om den uppfyller eller överskrider ovan nämnda tröskelvärden, utreda om det är ett fristående företag, ett partnerföretag eller ett anknutet företag enligt kommissionens rekommendation. Om företaget har partnerföretag eller anknutna företag, ska företaget lägga till dessa företags uppgifter i sina egna uppgifter när det bedömer om tröskelvärdena uppfylls eller överskrids. Mer information om samkörning av uppgifter finns i kapitel 3.3.2 i denna anvisning och i kommissionens användarhandledning: Användarhandledning om definitionen av SMF-företag (europa.eu).

[14] Se RP 57/2024 rd., s. 196.
[15] RP 57/2024 rd., s. 150.

Enligt artikel 3.1 i bilagan till kommissionens rekommendation är ett företag fristående om

- det är helt självständigt, dvs. det har ingen delaktighet i andra företag, och
- inget annat företag har delaktighet i företaget

  eller

- företaget kontrollerar mindre än 25 % av kapital- eller röstandelen (det som är högre beaktas) i ett eller flera andra företag, och/eller
- utomstående inte har en kapital- eller röstandel som överstiger 25 % (det som är högre beaktas) i företaget

  eller

- det inte är anknutet till ett annat företag via en fysisk person i den mening som avses i artikel 3.3.

I artikel 3.2 a–d i bilagan till kommissionens rekommendation nämns fyra undantag, varvid företaget kan anses vara fristående även om ovan nämnda tröskelvärde på 25 procent skulle uppnås eller överskridas om det är fråga om vissa typer av investerare och dessa inte ensamma eller tillsammans står i ett sådant förhållande till företaget som avses i punkt 3.

Om företaget är fristående använder det endast uppgifter om antalet anställda och penningvärden i sitt bokslut för att fastställa om det uppfyller tröskelvärdena för storlekskriterierna. Om aktören inte är ett fristående företag ska aktören beakta partnerföretags och anknutna företags uppgifter vid beräkningen av uppfyllandet av tröskelvärdena.

I artikel 4 i rekommendationen föreskrivs om de uppgifter som behövs för att beräkna personalstyrkan och de finansiella beloppen samt referensperioden. I fråga om uppfyllandet av storlekskriterierna granskas den senaste avslutade och föregående räkenskapsperioden. Om aktörens årliga uppgifter växlar mellan och överskrider de tröskelvärden som granskas, anses aktören uppnå och förlora sin ställning i storlekskategorin när överskridningen eller underskridningen upprepas under två på varandra följande år.

I den användarhandledningen som publicerats på kommissionens rekommendation finns åskådliggörande exempel på hur aktörens storlek fastställs. Användarhandledningen innehåller också information om till exempel sammanslagningars eller företagsförvärvs konsekvenser. Användarhandledningen och kommissionens rekommendation finns här: Användarhandledning om definitionen av SMF-företag (europa.eu)

3.3.2 Koncernföretag samt partnerföretag och anknutna företag

Aktörer som inte uppfyller definitionen av fristående företag i kapitel 3.3.1 ovan ska vara noggranna med vilka uppgifter de ska beakta vid bedömningen av storlekskriterierna enligt kommissionens rekommendation. Traditionellt gäller detta i synnerhet aktörer som hör till koncernstrukturen, men också andra som har olika ägarförhållanden eller andra kopplingar till andra företag.

Uppfyllandet av kriterierna ska granskas separat för varje rättsubjekt. Därför är de också separata aktörer till exempel i koncernstrukturen, då moder- och dotterbolaget är separata juridiska personer. Att dotterbolaget i ett sådant fall omfattas av tillämpningsområdet innebär därför inte automatiskt att också moderbolaget gör det, om moderbolaget inte självständigt uppfyller definitionen av aktör.[16]

Definitionerna av partnerföretag och anknutna företag finns i artikel 3 i bilagan till kommissionens rekommendation och de åskådliggörs med exempel i den ovan länkade användarhandledningen.

I artikel 6 i bilagan till kommissionens rekommendation föreskrivs det om fastställande av uppgifter om företag som har partnerföretag eller anknutna företag. En aktör som inte är ett fristående företag ska beakta andra företags uppgifter vid bedömningen av om tröskelvärdena uppfylls. Ett partnerföretag ska till exempel lägga till en andel av sin partners personalstyrka och finansiella uppgifter till sina egna uppgifter när det fastställer om tröskelvärdena uppfylls eller överskrids. Denna andel avspeglar den andel av aktierna eller röstetalet (beroende på vilken som är större) som innehas av någon annan. Om aktören däremot har till exempel majoriteten av aktieägarnas röstetal i ett annat företag, är det fråga om ett anknutet företag och 100 procent av dess uppgifter ska läggas till i aktörens uppgifter när uppfyllandet av tröskelvärdena fastställs.

Enligt 3 § 5 mom. i cybersäkerhetslagen tillämpas inte artikel 3.4 i bilagan till kommissionens rekommendation på aktören. Momentet i fråga innebär att eftersom nämnda punkt inte tillämpas kan även ett offentligt ägt företag betraktas som ett företag som inte uppfyller eller överskrider den tröskel som avses i 1 mom. 2 punkten.[17]

I den användarhandledningen som publicerats på kommissionens rekommendation finns åskådliggörande exempel på hur aktörens storlek fastställs. Användarhandledningen innehåller också information om till exempel sammanslagningars eller företagsförvärvs konsekvenser. Användarhandledningen och kommissionens rekommendation finns här: Användarhandledning om definitionen av SMF-företag (europa.eu)

3.3.3 Kommunen som verksamhetsutövare eller företagets ägare

Cybersäkerhetslagen tillämpas på kommuner som avses i kommunallagen (410/2015) endast i fråga om verksamhet som avses i bilagan till lagen (4 § 6

[16] RP 57/2024 rd., s. 150.
[17] RP 57/2024 rd., s. 158.

mom. i cybersäkerhetslagen). Till skillnad från vad som anges ovan i kapitel 3.3.1 för andra aktörer ska kommunerna inte beakta dess storleksuppgifter när den bedömer kommunens verksamhet i sin helhet. När det bedöms om kommunens verksamhet omfattas av tillämpningsområdet, ska vid fastställandet av storlekskriteriet endast den verksamhet som avses i bilagan till lagen beaktas, men inte kommunens personal, balansräkning eller omsättning i övrigt.[18]

Som konstaterats i föregående kapitel tillämpas inte artikel 3.4 i bilagan till kommissionens rekommendation på aktören med stöd av 3 § 5 mom. i cybersäkerhetslagen. Eftersom nämnda punkt inte tillämpas kan även ett offentligt ägt företag betraktas som ett företag som inte uppfyller eller överskrider den tröskel som avses i 1 mom. 2 punkten. I motsats till vad som sägs i kommissionens rekommendation, de begränsningar av äganderätten eller rösträtten som gäller offentliga organ inte tillämpas.[19]

3.4 Aktörer oberoende av storlek

Såsom anges ovan i kapitlen 3.2 och 3.3 ska aktören utreda om den bedriver verksamhet som omfattas av cybersäkerhetslagen och om den uppfyller eller överskrider storlekskriterierna i kommissionens rekommendation för att omfattas av tillämpningsområdet för cybersäkerhetslagen. Det finns dock två undantag som gäller aktörer inom energisektorn i det storleksbaserade tillämpningsområdet som beskrivs här, varvid aktören kan omfattas av lagens tillämpningsområde oberoende av dess storlek. I detta kapitel behandlas undantagskriterier enligt 3 § 3 mom. i cybersäkerhetslagen. I följande kapitel 3.5 behandlas den andra undantagsgrunden i anslutning till CER-direktivet[20].

I 3 § 3 mom. i cybersäkerhetslagen föreskrivs att vissa aktörer omfattas av lagen oavsett storlek, det vill säga även när aktören inte uppfyller storlekskravet i kapitel 3.3. Sådana aktörer är aktörer som bedriver verksamhet eller som har en aktörstyp som avses i bilaga I eller II till lagen och som uppfyller ett eller flera av kriterierna i 3 § 3 mom. 1–4 punkten. Lagen tillämpas på en sådan aktör, oavsett storlek, som bedriver verksamhet enligt bilagor eller som är en sådan aktör som avses i nämnda bilagor, om

1) aktören tillhandahåller en tjänst som är väsentlig för att upprätthålla kritiska samhälleliga eller ekonomiska funktioner och som inte tillhandahålls av andra aktörer,

2) en störning av den tjänst som aktören tillhandahåller skulle ha en betydande påverkan på allmän ordning, allmän säkerhet eller folkhälsa,

---

[18] RP 57/2024 rd., s. 159.

[19] RP 57/2024 rd., s. 150 och 158.

[20] Europaparlamentets och rådets direktiv om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG
(CER-direktivet).

3) en störning av den tjänst som aktören tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser, eller

4) aktören är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i en medlemsstat i Europeiska unionen som är beroende av denna aktör.

Närmare bestämmelser om de kriterier som nämns ovan får utfärdas genom förordning av statsrådet (3 § 4 mom. i cybersäkerhetslagen). Enligt regeringens proposition om cybersäkerhetslagen är aktörer som kriterierna gäller aktörer som bedriver verksamhet av särskilt slag och skulle på grund av verksamhetens särskilda art undantagsvis omfattas av lagens skyldigheter oberoende av deras storlek. Med beaktande av de kriterier som avses i 3 mom. 1–4 punkten och arten av artikel 2.2 b-e i NIS2-direktivet, kan det utifrån de uppgifter som ett enskilt företag har tillgång till visa sig vara osäkert om företaget uppfyller kriterierna i 1–4 punkten. Det är därför nödvändigt att precisera kriterierna genom förordning av statsrådet för att förtydliga rättsläget i fråga om när en enskild aktör uppfyller det kriterium som avses i 3 mom. 1–4 punkten. Härigenom preciseras unionsrättsaktens förpliktande tillämpningsområde.[21]

Ovan nämnda förordning av statsrådet har inte utfärdats när denna anvisning publicerades. Energimyndigheten anvisar således att aktörerna ska vänta på statsrådets förordning för att säkerställa en enhetlig tolkning av undantagskriterierna. Om aktören på det sätt som presenteras i kapitel 3.3 på grund av sin storlek omfattas av tillämpningsområdet för cybersäkerhetslagen, ska aktören anmäla sig till Energimyndigheten som en aktör som ska övervakas. När kriterierna för aktörer oberoende av storlek har preciserats genom förordning av statsrådet, ska en aktör som uppfyller kriterierna anmäla sig eller uppdatera sin anmälan i NIS2-aktörsförteckningen. Närmare information om anmälan till NIS2-aktörsförteckningen finns i kapitel 4.1 och 6 i denna anvisning.

3.5 CER-aktörer

NIS2-direktivet tillämpas på aktörer som med stöd av CER-direktivet definierats som kritiska aktörer oberoende av deras storlek. Kritiska aktörer enligt CER-direktivet definieras för första gången 2026. Energimyndigheten uppdaterar anvisningen i takt med att det nationella genomförandet av CER-direktivet framskrider.

3.6 Viktig eller väsentlig aktör?

De aktörer som omfattas av cybersäkerhetslagen delas in i två kategorier: viktiga och väsentliga aktörer. Aktören ska meddela i aktörsförteckningen som upprätthålls av tillsynsmyndigheten om den är en viktig eller väsentlig aktör.

Medelstora företag är viktiga aktörer (kapitel 3.3).

[21] RP 57/2024 rd., s. 157.

Väsentliga aktörer är aktörer som överskrider definitionen av ett medelstort företag, alltså stora företag (kapitel 3.3), kritiska aktörer enligt CER-direktivet (kapitel 3.5) och andra aktörer som oberoende av storlek definierats som aktörer som omfattas av lagen (kapitel 3.4).

Skyldigheterna i cybersäkerhetslagen gäller viktiga och väsentliga aktörer lika mycket, men Energimyndigheten övervakar dessa på olika sätt. Tillsynen riktas till väsentliga aktörer. Energimyndigheten kan dock inrikta tillsynen också på viktiga aktörer om det finns grundad anledning att misstänka att aktören i fråga inte har iakttagit cybersäkerhetslagen, föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS2-direktivet (cybersäkerhetslagen 27.1 §).

4 Skyldigheter

4.1 Anmälan till aktörsförteckningen

Aktören ska anmäla sig till den aktörsförteckning som upprätthålls av Energimyndigheten (cybersäkerhetslagen 41 §). Om en aktör övervakas av flera myndigheter, ska aktören anmäla sig separat till alla aktörsförteckningar som upprätthålls av de myndigheter som övervakar aktören.

Aktören ska göra den första anmälan till aktörsförteckningen senast en månad efter att lagen har trätt i kraft dvs. senast 8.5.2025 eller en månad efter att kriterierna för aktören enligt 3 § uppfylls.

En aktör som Energimyndigheten övervakar ska anmäla sig till NIS2-aktörsförteckningen som upprätthålls i VERTTI-tillsynsuppgiftssystemet. I kapitel 6 i denna anvisning finns närmare anvisningar om anmälan till VERTTI-tillsynsuppgiftssystemet.

Aktörerna ska utan dröjsmål anmäla ändringar i de uppgifter som avses i 41 §. Ändringar i de uppgifter som räknas upp i 41 § 2 mom. i cybersäkerhetslagen ska anmälas till Energimyndigheten inom två veckor. Sådana uppgifter är bland annat aktuella kontaktuppgifter, IP-adressområden och information om aktören är en viktig eller väsentlig aktör.

Energimyndigheten ska lämna uppgifter om aktörsförteckningen till den gemensamma kontaktpunkten vid Traficoms Cybersäkerhetscenter. Den gemensamma kontaktpunkten har till uppgift att göra de anmälningar som avses i artikel 3.5 i NIS2-direktivet till Europeiska kommissionen, NIS-samarbetsgruppen och Europeiska unionens cybersäkerhetsbyrå. Cybersäkerhetscentrets CSIRT-enhet har dessutom rätt att få uppgifter ur den aktörsförteckning som Energimyndigheten upprätthåller. Information som är relevant för CSIRT-enhetens uppgifter är särskilt aktörernas kontaktuppgifter och IP-adresser.[22]

[22] RP 57/2024 rd., s. 208.

4.2 Allmänt om riskhantering och anmälan av incidenter

I 2 kap. i cybersäkerhetslagen föreskrivs om riskhantering och anmälan av incidenter. Bestämmelser om aktörernas riskhanteringsskyldigheter finns i 7–10 § i cybersäkerhetslagen. I följande kapitel 4.3 behandlas skyldigheterna i varje paragraf och specificeras hur skyldigheten i fråga har förklarats i regeringens proposition om den. I anvisningen behandlas inte innehållet i förpliktelserna på ett uttömmande sätt och mer information kan till exempel sökas i detaljmotiveringarna till paragraferna i regeringens proposition. Närmare information om anmälan av incidenter finns i kapitel 4.4.

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom har utarbetat en rekommendation till NIS-tillsynsmyndigheterna om åtgärder för riskhantering inom cybersäkerhet. Rekommendationen finns på Traficoms webbplats. Aktörerna kan utnyttja rekommendationen som rättesnöre vid planeringen och genomförandet av åtgärder enligt cybersäkerhetslagen.

På Cybersäkerhetscentrets webbplats finns dessutom många anvisningar och guider för organisationer och företag: https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/anvisningar-och-guider-organisationer-och-foretag. Aktörerna kan också stöda bedömningen och utvecklingen av cybersäkerheten med Cybersäkerhetscentrets avgiftsfria cybermätare: https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren.

Såsom konstaterats ovan i kapitel 3 tolkas definitionen av aktör enligt rättssubjekt. I regeringens proposition konstateras för tydlighetens skull att när en juridisk person bedriver verksamhet som avses i bilagan till lagen, ska definitionen av aktör enligt lagen då omfatta den juridiska personen i fråga som helhet. Avsikten är således inte att tillämpningen av lagen och de skyldigheter som föreskrivs i den ska begränsas till en enhet eller funktion hos en juridisk person som bedriver sådan verksamhet som avses i bilagorna, utan skyldigheterna ska gälla den juridiska personen i fråga som sådan, dvs. aktören som helhet. Till exempel en juridisk person som verkar inom flera verksamhetsområden, av vilka endast en del nämns i bilagorna till lagen, omfattas således av regleringen även i fråga om sådana funktioner som inte nämns i bilagorna till lagen.[23]

Ovan i denna anvisning behandlas aktörer som hör till koncernstrukturen. I regeringens proposition om cybersäkerhetslagen konstateras att bolag som hör till samma koncern kan samarbeta med andra bolag inom samma koncern vid fullgörandet av riskhanterings- och rapporteringsskyldigheterna. Det är bra att beakta att om en del av bolagen i koncernstrukturen eller i något annat arrangemang som gäller bolagens inbördes ägande omfattas av tillämpningsområdet och andra bolag inte gör det, ska de beakta till exempel beroendet av tjänster som andra bolag tillhandahåller som en del av fullgörandet av riskhanterings- och rapporteringsskyldigheterna enligt 2 kap.[24]

[23] RP 57/2024 rd., s. 151.
[24] RP 57/2024 rd., s. 151.

I kapitel 3.3.3 ovan i denna anvisning behandlas kommuner som omfattas av tillämpningsområdet för cybersäkerhetslagen, eftersom de bedriver verksamhet som nämns i bilagan till lagen. Enligt 4 § 6 mom. i cybersäkerhetslagen tillämpas lagen på kommuner som avses i kommunallagen endast i fråga om verksamhet som avses i bilaga I eller II. På motsvarande sätt som vid bedömning av kommunens storlekskriterier ska riskhanterings-, rapporterings- och anmälningsskyldigheten inte tolkas så att den är förpliktande för kommunen i fråga om annan verksamhet än sådan som avses i bilagan till lagen.[25] Detta är ett undantag från det ovan nämnda, enligt vilket cybersäkerhetslagen tillämpas på en aktör som omfattas av tillämpningsområdet som helhet.

Dessutom tillämpas 2 kap. i cybersäkerhetslagen inte på verksamhet eller tjänster som tillhandahålls för tryggande av försvaret, den nationella säkerheten, allmän ordning och säkerhet eller förebyggande av brott, brottsutredning och väckande av åtal (4 § 1 mom. i cybersäkerhetslagen).

I denna anvisning behandlas riskhanteringsskyldigheterna enligt cybersäkerhetslagen. Med stöd av 9 § 5 mom. i cybersäkerhetslagen ska riskhanteringen, handlingsmodellen för riskhantering och hanteringsåtgärderna dessutom iaktta de genomförandeakter som kommissionen antar med stöd av artikel 21.5 i NIS 2-direktivet.

Utöver det ovan nämnda betonar Energimyndigheten att om det i någon annan lag eller i bestämmelser eller föreskrifter som utfärdats med stöd av den finns krav som avviker från cybersäkerhetslagen på hantering av cybersäkerhetsrisker eller anmälan om betydande incidenter och kraven till sina verkningar motsvarar minst skyldigheterna enligt cybersäkerhetslagen, tillämpas de i stället för motsvarande bestämmelser i denna lag. Likaså, om det i Europeiska unionens förordning eller i en förordning av kommissionen som utfärdats med stöd av NIS2-direktivet förutsätts att en aktör inför åtgärder för hantering av risker som gäller cybersäkerhet eller anmäler betydande incidenter och kraven till sina verkningar motsvarar minst skyldigheterna enligt cybersäkerhetslagen, tillämpas bestämmelserna i stället för 2, 4 och 5 kap. samt 41 § i denna lag (cybersäkerhetslagen 5 § mom. 1–2). Ovan nämnda undantag kommer att bedömas bland annat i och med verkställandet av nätföreskriften för cybersäkerhet (NCCS).[26]

Aktören bör också beakta att datasäkerheten vid behandling av personuppgifter fortfarande regleras i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och i dataskyddslagen (1050/2018).

---

[25] RP 57/2024 rd., s. 159.

[26] Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (NCCS).

4.3 Riskhantering

4.3.1 Allmän riskhanteringsskyldighet

I 7 § i cybersäkerhetslagen föreskrivs om allmän riskhanteringsskyldighet. Enligt 1 mom. ska en aktör identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sin verksamhet eller för att tillhandahålla sina tjänster. Hanteringen av cybersäkerhetsrisker ska förhindra eller minimera incidenternas inverkan på verksamheten, driftskontinuiteten, tjänstemottagarna och andra tjänster. Med stöd av lagens 7 § 2 mom. ska aktören vidta och riskhanteringsåtgärder som är aktuella, proportionella och tillräckliga i förhållande till riskerna för de kommunikationsnät och informationssystem som används i verksamheten samt kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet och tillhandahållande av tjänster.

Enligt detaljmotiveringen till ovan nämnda paragraf avses med riskhantering identifiering av risker som hänför sig till kommunikationsnät och informationssystem som är av betydelse med tanke på verksamheten eller tillhandahållandet av tjänster, bedömning av hur allvarliga riskerna är samt vidtagande av tillräckliga åtgärder för att hantera riskerna. Syftet med riskhanteringen är att förhindra eller minimera att störningar i kommunikationsnäten och informationssystemen påverkar verksamheten, tjänstemottagarna eller andra tjänster vid störningssituationer oberoende av orsaken till störningen. Riskhanteringen ska alltså syfta till att trygga kontinuiteten i verksamheten i situationer där kommunikationsnätens och informationssystemens funktion störs på grund av illvillig verksamhet eller av någon annan orsak. Hanteringen av cybersäkerhetsrisker är en del av organisationens riskhantering. Utgångspunkten för riskhanteringen är dels identifieringen av risker, dels de resultat med hjälp av vilka organisationen vill minska riskerna.[27]

Fastställandet av den identifierade riskens betydelse är både subjektivt på basis av aktörens egna affärs- eller serviceintressen och objektivt på basis av den allmänna och samhälleliga betydelsen och betydelsen av en tjänst som är beroende av tillförlitligheten hos aktörens kommunikationsnät och informationssystem. De objektiva kriterierna beskrivs närmare i 9 § och dess motivering.[28]

Riskhanteringsskyldigheten ska gälla aktörens verksamhet, kontinuiteten i verksamheten och tillhandahållandet av tjänster. Riskhanteringsskyldigheten är inte avsedd att gälla egenskaperna hos en produkt som aktören har tillverkat eller släppt ut på marknaden.[29]

Skyldigheten att ordna riskhantering inom cybersäkerheten är fortlöpande till sin karaktär, eftersom riskerna för säkerheten i kommunikationsnät och informationssystem förändras och säkerhetsåtgärderna utvecklas med tiden. Riskhanteringsåtgärderna ska framför allt vara aktuella, dvs. motsvara aktuell teknisk utveckling

[27] RP 57/2024 rd., s. 163–164.
[28] RP 57/2024 rd., s. 164.
[29] RP 57/2024 rd., s. 164.

och välkänd bästa praxis om hur cybersäkerhetsrisker kan skyddas eller deras effekter minimeras. Vid bedömningen av om riskhanteringen är tillräcklig och proportionell beaktas bland annat kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet eller tillhandahållande av tjänster, arten av de uppgifter som behandlas i kommunikationsnätet eller informationssystemet samt andra aktörers beroende av aktörens verksamhet, tillhandahållande av tjänster, kommunikationsnät eller informationssystem samt särskilt dess betydelse för samhällets kristålighet.

Syftet med bedömningen av cybersäkerhetsriskerna är att främja och utveckla en riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna. Ju större verkningarna blir om en risk realiseras och ju större sannolikheten är för att den realiseras, desto effektivare, högklassigare eller dyrare åtgärder krävs det för att riskhanteringen ska vara proportionerlig.[30]

4.3.2 Handlingsmodell för hantering av cybersäkerhetsrisker

Enligt 8 § i cybersäkerhetslagen ska aktören ha en uppdaterad handlingsmodell för hantering av cybersäkerhetsrisker för att skydda kommunikationsnät och informationssystem och deras fysiska miljö mot incidenter och deras verkningar. En verksamhetsmodell för riskhantering ska upprättas inom tre månader från det att cybersäkerhetslagen trätt i kraft eller från det att kriterierna för aktören uppfylls (47 § 3 mom. i cybersäkerhetslagen).

I handlingsmodellen för hantering av cybersäkerhetsrisker ska de risker som hänför sig till kommunikationsnät och informationssystem och deras fysiska miljö identifieras med beaktande av ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen ska målen, förfarandena och ansvaren för hanteringen av cybersäkerhetsrisker samt de åtgärder enligt 9 § genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot cyberhot och incidenter (hanteringsåtgärder) fastställas och beskrivas.

Handlingsmodellen för riskhantering kan också vara en del av aktörens mer omfattande riskhanteringsplan, som också beaktar andra risker som hänför sig till verksamheten, eller en del av den övriga säkerhetsberedskapen.[31] Till exempel el- och naturgasnätsinnehavare som har andra skyldigheter i anslutning till beredskapen med stöd av speciallagstiftningen om dessa kan ta skyldigheterna enligt cybersäkerhetslagen som en del av en mer omfattande riskhantering (28 § i elmarknadslagen och 27 § i naturgasmarknadslagen).

Handlingsmodellen ska i enlighet med en allriskansats (all-hazard approach) skapas så att den omfattar både kommunikationsnät och informationssystem och deras fysiska miljö. Syftet är att skydda kommunikationsnät och informationssystem samt den verksamhet som bedrivs eller de tjänster som tillhandahålls med hjälp av dem mot kränkningar av informationssäkerheten, systemfel, mänskliga misstag, avsiktligt skadliga handlingar och naturfenomen. I en allriskansats ska man alltså

[30] RP 57/2024 rd., s. 164.
[31] RP 57/2024 rd., s. 165.

beakta alla rimligen förutsebara hot mot kommunikationsnät och informationssystem, oavsett om de beror på hot mot informationssäkerheten, orsakas av naturen eller människan eller om de följer olyckor eller är avsiktligt orsakade.

En allriskansats ska omfatta risker för informations- och cybersäkerheten i kommunikationsnät och informationssystem, såsom administrativa risker, risker i fråga om personal, hårdvara, programvara, informationsmaterial och användarsäkerhet samt i fråga om deras fysiska miljö, lokaler och nödvändiga resurser sådana händelser som stöld, brand, översvämning, störning av telekommunikationen eller elavbrott, obehörigt fysiskt tillträde till aktörens information eller informationshanteringsmiljö samt skada och störningar som kan äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i fråga om den information eller de tjänster som hanteras i kommunikationsnäten och informationssystemen eller via dessa. I riskhanteringen ska det beaktas i vilken utsträckning aktören är beroende av kommunikationsnäten och informationssystemen. Ju viktigare system det är fråga om med tanke på tjänsteproduktionen och ju större skadliga effekter en risk skulle få för systemet, desto högklassigare riskhantering ska det krävas till denna del.

Handlingsmodellen för hantering av cybersäkerhetsrisker och de riskhanteringsåtgärder som grundar sig på den ska som en del av den fortlöpande identifieringen och bedömningen av risker som avses i 7 § som nämns i kapitel 4.3.1 uppdateras och hållas aktuell.[32]

4.3.3 Åtgärder för hantering av cybersäkerhetsrisker

Med stöd av 9 § i 1 mom. i cybersäkerhetslagen ska aktörerna vidta proportionella tekniska, driftsrelaterade eller organisatoriska hanteringsåtgärder i enlighet med handlingsmodellen för hantering av cybersäkerhetsrisker för att hantera sådana risker som hänför sig till säkerheten i kommunikationsnät och informationssystem samt förhindra eller minimera skadliga verkningar.

Enligt detaljmotiveringen till paragrafen ska man vid bedömningen av dessa åtgärders proportionalitet ta vederbörlig hänsyn till aktörens grad av riskexponering, aktörens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. Riskhanteringen ska alltså beakta å ena sidan sannolikheten för att risken realiseras och de kostnader som uppstår om risken realiseras och å andra sidan kostnaderna för och effekterna av de tillgängliga riskhanteringsåtgärderna.[33]

I 9 § 2 mom. i cybersäkerhetslagen föreskrivs det om de delområden som ska beaktas vid utarbetandet av en handlingsmodell för hantering av cybersäkerhetsrisker och vid fastställandet av behövliga riskhanteringsåtgärder. Listan över delområden är en minimilista, vilket innebär att alla aktörer åtminstone ska beakta de omständigheter som räknas upp i momentet. Aktören kan också genomföra en mer omfattande riskhantering när det bedöms som nödvändigt.[34]

---

[32] RP 57/2024 rd., s. 165.
[33] RP 57/2024 rd., s. 165.
[34] Se RP 57/2024 rd., s. 165.

När det gäller riskhanteringsåtgärder bör det beaktas att de lever i tiden, utvecklas och dessutom är teknikrelaterade. Den cybersäkerhetspolitiska miljön förändras också ständigt i takt med att både teknik och bästa praxis i anslutning till cybersäkerheten utvecklas. Aktörerna bör ges handlingsutrymme när det gäller det praktiska genomförandet av riskhanteringen. I riskhanteringsåtgärderna bör man också beakta att metoderna och den teknik som används är inbördes sammanlänkade – t.ex. när det gäller äldre nättekniker kan riskhanteringsåtgärderna av tekniska skäl inte vara lika heltäckande eller sofistikerade som när det gäller nyare nätverksteknik.[35]

Aktörerna ska dock i riskhanteringen och riskhanteringsåtgärderna beakta åtminstone de delområden som avses i 2 mom. samt kunna dokumentera och visa hur riskhanteringen genomförs inom delområdena.[36]

Enligt paragrafens 2 mom. ska man handlingsmodellen och de hanteringsåtgärder som baserar sig på den åtminstone beakta och uppdatera följande:

1) riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om hanteringsåtgärderna,

2) de riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem,

3) säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter,

4) den övergripande kvaliteten och resiliensen i leveranskedjan i fråga om direkta leverantörers produkter och tjänsteleverantörers tjänster, de hanteringsåtgärder som är inbyggda i dem samt cybersäkerhetspraxis hos direkta leverantörer och tjänsteleverantörer,

5) tillgångsförvaltningen och identifieringen av funktioner som är viktiga med tanke på dess säkerhet,

6) personalsäkerheten och utbildningen i cybersäkerhet,

7) förfarandena för åtkomsthantering och autentisering,

8) riktlinjerna och förfarandena för användning av krypteringsmetoder samt vid behov åtgärderna för användning av säker elektronisk kommunikation,

9) upptäckandet och hanteringen av incidenter i syfte att återställa och upprätthålla säkerheten och driftssäkerheten,

[35] RP 57/2024 rd., s. 165–166.
[36] RP 57/2024 rd., s. 166.

10) säkerhetskopieringen, katastrofhanteringen, krishanteringen och den övriga driftskontinuiteten och vid behov användningen av säkrade reservkommunikationssystem,

11) grundläggande praxis för informationssäkerhet för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet, samt

12) åtgärderna för att säkerställa den fysiska miljön, lokalsäkerheten och nödvändiga resurser i fråga om kommunikationsnät och informationssystem.

Åtgärderna ska ställas i relation till verksamhetens art och omfattning, de direkta konsekvenser som incidenten rimligtvis kan förutses ha, riskexponeringen i fråga om aktörens kommunikationsnät och informationssystem, sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, kostnaderna för åtgärderna samt de tekniska medel för att avvärja hot som med beaktande av den aktuella utvecklingen är tillgängliga.

I detaljmotiveringen till paragrafen behandlas för varje punkt vad skyldigheten omfattar. Dessutom har Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom utarbetar en rekommendation till NIS-tillsynsmyndigheterna om åtgärder för riskhantering inom cybersäkerhet. Aktörerna kan utnyttja rekommendationen som rättesnöre vid planeringen och genomförandet av åtgärder enligt cybersäkerhetslagen.

Energimyndigheten kan inom sitt ansvarsområde meddela tekniska föreskrifter som preciserar riskhanteringsskyldigheterna. Energimyndigheten ger tills vidare närmare information om riskhanteringsskyldigheterna genom denna anvisning. Energimyndighetens föreskrifter publiceras på Energimyndighetens webbplats (https://energiavirasto.fi/sv/framsida) och i Finlex-myndigheternas författningssamling (www.finlex.fi/sv/myndigheter/).

4.3.4 Ledningens ansvar

Aktörens ledning har ålagts ansvar för att skyldigheterna enligt cybersäkerhetslagen iakttas. Enligt 10 § i cybersäkerhetslagen ansvarar aktörens ledning för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av cybersäkerhetsrisker och utövar tillsyn över genomförandet av den. Aktörens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

Med ledning avses aktörens styrelse, förvaltningsråd och verkställande direktör samt någon annan i därmed jämförbar ställning som de facto leder dess verksamhet.

Enligt detaljmotiveringen till paragrafen ansvarar aktörens högsta ledning för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker i aktörens kommunikationsnät och informationssystem. Ansvaret innebär ett ansvar i sista hand för att ordna riskhanteringen och avsätta lämpliga resurser för den samt att övervaka dess verksamhet. Aktörens ledning skulle godkänna handlingsmodellen

för hantering av cybersäkerhetrisker samt övervakar genomförandet av riskhanteringen, resursfördelningen, åtgärderna, riskbedömningarnas aktualitet och åtgärdernas genomslag. Aktörens ledning ska också ha tillräcklig och aktuell förtrogenhet med hantering av cybersäkerhetsrisker, vilket förutsätter förtrogenhet antingen genom utbildning eller på något annat motsvarande sätt med regelbundna intervaller. Som en del av de hanteringsåtgärder som avses i 9 § sörjer ledningen också för att personalen får cybersäkerhetsutbildning.[37]

4.4 Incidentanmälningar

4.4.1 Anmälningskanal och allmänt om anmälan

Aktören ska utan dröjsmål underrätta Energimyndigheten om en betydande incident (nedan NIS-anmälan, 11 § 1 mom. i cybersäkerhetslagen).

NIS-anmälningar görs till Energimyndigheten via Cybersäkerhetscentrets anmälningsblankett vid Transport- och kommunikationsverket Traficom. En uppdaterad anmälningslänk upprätthålls på Energimyndighetens webbplats (https://energiavirasto.fi/sv/cybersakerhet). Anmälningsapplikationen styr i ifyllandet av anmälan.

När uppgifterna anmäls via anmälningsblanketten förmedlas de till både Energimyndigheten och Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom. Aktören kan i samband med anmälan be Cybersäkerhetscentrets CSIRT-enhet om vägledning och operativa råd om begränsande åtgärder.

Energimyndigheten kan inom sitt ansvarsområde meddela närmare tekniska föreskrifter för att precisera typen av information i och det tekniska formatet och förfarandet för anmälningar, underrättelser, information eller rapporter. Energimyndigheten ger tills vidare närmare information om ovan nämnda omständigheter genom denna anvisning. Energimyndighetens föreskrifter publiceras på Energimyndighetens webbplats (https://energiavirasto.fi/sv/framsida) och i Finlex-myndigheternas författningssamling (www.finlex.fi/sv/myndigheter/).

4.4.2 NIS-anmälningströskel

Med betydande incident avses en incident som

1. har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna,
2. har orsakat eller kan orsaka betydande ekonomiska förluster för den berörda aktören, eller
3. som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada.

[37] RP 57/2024 rd., s. 173–174.

Med incident avses en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem (cybersäkerhetslagen 2 § 11 punkten).

Aktören ska efter att ha upptäckt incidenten göra en preliminär bedömning av hur allvarlig incidenten är. Aktören ska i sin inledande bedömning av hur betydande incidenten är ta hänsyn åtminstone till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av aktörens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt aktörens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om driftsstörningen är allvarlig.[38]

Om en aktör upptäcker en händelse som uppfyller tröskeln för en betydande incident i någon annans verksamhet än sin egen, t.ex. i en direkt underentreprenörs, systemleverantörs eller en använd molntjänsts verksamhet, ska aktören rapportera händelsen endast om den för aktörens egen del är en händelse som överskrider tröskeln för en betydande incident.[39]

Utöver det ovan nämnda avses med betydande incident en situation som preciseras i Europeiska kommissionens genomförandeakt som antagits med stöd av artikel 23.11 i NIS2-direktivet och där incidenten anses vara betydande. Kommissionen kan anta sådana genomförandeakter för energisektorns aktörer.

Energimyndigheten rekommenderar för aktörer inom energisektorn att de alltid gör en NIS-anmälan när en observerad incident kan orsaka en driftsstörning i tjänsterna. Det är fråga om en rekommendation och den lagstadgade anmälningsskyldigheten gäller alltid endast incidenter som är betydande.[40] Läs mer om frivillig underrättelse i kapitel 4.4.6.

4.4.3 Innehållet i NIS-anmälningar och rapporter till myndigheter samt krav på tidtabell

Bestämmelser om innehållet i NIS-anmälningar och rapporter samt om tidtabellskraven finns i 11–13 § i cybersäkerhetslagen. Den första anmälan ska göras inom 24 timmar från det att den betydande incidenten upptäcktes och den uppföljande anmälan inom 72 timmar från det att den betydande incidenten upptäcktes. Aktören kan göra den första anmälan och den uppföljande anmälan på en och samma gång, om aktören inom tidsfristen för den första anmälan, dvs. utan dröjsmål och senast inom 24 timmar från det att incidenten upptäckte, har de uppgifter som förutsätts i båda anmälningarna.[41]

---

[38] Se RP 57/2024 rd, s. 174, artikel 23.3 och det inledande stycket 101 i NIS2-direktivet.

[39] RP 57/2024 rd., s. 174.

[40] Se även kapitel 4.4.6 och cybersäkerhetslagen 15 § 1 mom.: Aktörerna kan frivilligt göra anmälningar till tillsynsmyndigheten om andra incidenter, cyberhot och tillbud än de som avses i 11 §.

[41] RP 57/2024 rd., s. 175.

Aktören ska på begäran av Energimyndigheten lämna ytterligare information eller en delrapport om statusuppdateringar som gäller den betydande incidenten och om hur hanteringen framskrider. Om den betydande incidenten är långvarig, ska aktören lämna in en delrapport på eget initiativ senast en månad efter lämnandet av den uppföljande anmälan (cybersäkerhetslagen 12 §).

Aktören ska lämna Energimyndigheten en slutrapport om en betydande incident inom en månad från det att den uppföljande anmälan lämnades in eller, om det är fråga om en långvarig incident, inom en månad från det att hanteringen av den avslutades (cybersäkerhetslagen 13.1 §).[42]

NIS-anmälningar och -rapporter görs till Energimyndigheten via Cybersäkerhetscentrets anmälningsblankett vid Transport- och kommunikationsverket Traficom. Anmälningsapplikationen styr i ifyllandet av anmälan. Aktören kan i samband med anmälan be Cybersäkerhetscentrets CSIRT-enhet om vägledning och operativa råd om begränsande åtgärder.

En uppdaterad anmälningslänk upprätthålls på Energimyndighetens webbplats (https://energiavirasto.fi/sv/cybersakerhet). Anmälningsapplikationen styr i ifyllandet av anmälan.

I den första anmälan ska uppges

1) att en betydande incident har upptäckts,

2) om den betydande incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar,

3) möjligheten och sannolikheten för gränsöverskridande verkningar och uppgifter om förväntad utveckling vad gäller gränsöverskridande verkningar.

I den uppföljande anmälan ska uppges

1) en bedömning av den betydande incidentens art, allvarlighetsgrad och konsekvenser,

2) i förekommande fall, tekniska angreppsindikatorer,

3) eventuella uppdateringar av uppgifterna i den första anmälan.

Slutrapporten ska innehålla

1) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser,

2) en redogörelse för den typ av hot eller grundorsak som sannolikt har utlöst incidenten,

[42] Se 11–13 § i cybersäkerhetslagen.

3) en redogörelse för tillämpade och pågående åtgärder för att begränsa konsekvenserna av incidenten, och

4) en redogörelse för eventuella gränsöverskridande konsekvenser.

4.4.4 Mottagande och behandling av incidentanmälningar hos Energimyndigheten

Energimyndigheten svarar utan dröjsmål till den part som gjort en incidentanmälan. Svaret ska innehålla initial återkoppling om den betydande incidenten samt vägledning om hur den ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet (cybersäkerhetslagen 16.1 §). Svaret ges med ett krypterat meddelande inom kontorstid. Om aktören inte får Energimyndighetens svar inom två dagar bör aktören kontakta Energimyndighetens registratorskontor kirjaamo(at)energiavirasto.fi. Energimyndigheten kan i sitt svarsmeddelande begära mer information av aktören.[43]

NIS-anmälningar och -rapporter görs till Energimyndigheten via Cybersäkerhetscentrets anmälningsblankett vid Transport- och kommunikationsverket Traficom. Om anmälan eller rapporten dock lämnas in på något annat sätt direkt till Energimyndigheten, skickar Energimyndigheten anmälningarna och rapporterna omedelbart till Cybersäkerhetscentrets CSIRT-enhet. För att säkerställa ett obrutet och snabbt informationsutbyte bör aktören dock alltid göra anmälningarna via anmälningsapplikationen. Anmälningsapplikationen styr upprättandet av anmälan, varvid aktören säkerställs av att alla nödvändiga uppgifter har lämnats. En uppdaterad anmälningslänk upprätthålls på Energimyndighetens webbplats (https://energiavirasto.fi/sv/cybersakerhet).

Om en betydande incident har lett till en sådan i artikel 33 i den allmänna dataskyddsförordningen avsedd personuppgiftsincident som ska anmälas, ska Energimyndigheten anmäla upptäckten av incidenten till dataombudsmannen (cybersäkerhetslagen 17.2 §). Energimyndighetens skyldighet att informera dataombudsmannen om saken påverkar dock inte aktörernas skyldigheter, och Energimyndighetens anmälan uppfyller således inte exempelvis den personuppgiftsansvariges skyldighet att anmäla en personuppgiftsincident.[44]

Om det i samband med en betydande incident på grundval av aktörens anmälan kan antas att det har begåtts ett brott för vilket det föreskrivna maximistraffet är fängelse i minst tre år, ska tillsynsmyndigheten underrätta polisen om upptäckten av den betydande incidenten (cybersäkerhetslagen 17.3 §).[45]

Om en betydande incident påverkar andra medlemsstater i Europeiska unionen eller andra sektorer, ska Energimyndigheten informera den gemensamma kontaktpunkten, dvs. Transport- och kommunikationsverkets Cybersäkerhetscenter, om incidenten och sända anmälningar, rapporter och annat om den till den gemensamma

[43] Se 12 § i cybersäkerhetslagen.

[44] RP 57/2024 rd., s. 179.

[45] RP 57/2024 rd., s. 179. ”Brott som avses i paragrafen är till exempel grov dataskadegörelse enligt 35 kap. 3 b §, grov kränkning av kommunikationshemlighet enligt 38 kap. 4 §, grovt störande av post- och teletrafik enligt 38 kap. 6 §, grov systemstörning enligt 38 kap. 7 b § och grovt dataintrång enligt 38 kap. 8 a § i strafflagen. Till de brott som avses i paragrafen hör också till exempel landsförräderibrott enligt 12 kap. 1–7 § och 9 § i strafflagen.”

kontaktpunkten. Om en incident påverkar en annan medlemsstat i Europeiska unionen ska den gemensamma kontaktpunkten utan onödigt dröjsmål underrätta Europeiska unionens cybersäkerhetsbyrå och de medlemsstater som berörs av incidenten. Den gemensamma kontaktpunkten ska på begäran också sända de anmälningar och rapporter som avses i 11–13 § till den gemensamma kontaktpunkten i den medlemsstat som berörs av incidenten. Den gemensamma kontaktpunkten får i detta syfte lämna ut information om betydande incidenter till Europeiska unionens cybersäkerhetsbyrå och till de gemensamma kontaktpunkterna i andra medlemsstater i Europeiska unionen (cybersäkerhetslagen 17.4–5 §).[46]

4.4.5 Aktörens skyldighet att anmäla incidenter och cyberhot till andra än myndigheter

En aktör ska utan dröjsmål underrätta mottagarna av sina tjänster om en betydande incident, om den betydande incidenten sannolikt inverkar negativt på tillhandahållandet av aktörens tjänster (cybersäkerhetslagen 14.1 §).

En aktör ska utan dröjsmål underrätta de mottagare av sina tjänster som kan påverkas av ett betydande cyberhot om ett betydande cyberhot och om de åtgärder som står till buds för att hantera cyberhotet (cybersäkerhetslagen 14.2 §).

Om det ligger i allmänt intresse att det informeras om en betydande incident, kan tillsynsmyndigheten ålägga aktören att informera om saken eller själv informera om saken (cybersäkerhetslagen 14.3 §).

4.4.6 Frivillig underrättelse

Aktörer kan på frivillig basis underrätta tillsynsmyndigheten om andra än i 11 § avsedda incidenter, cyberhot och tillbud.[47] När det inte är fråga om en sådan anmälan om betydande incident som avses i 11 § i cybersäkerhetslagen och det är frivilligt att göra anmälan, behöver anmälaren inte iaktta kraven på innehållet i och tidtabellen för anmälningar och rapporter om betydande incidenter.

Energimyndigheten rekommenderar för aktörer inom energisektorn att de alltid gör en NIS-anmälan när en observerad incident kan orsaka en driftsstörning i tjänsterna. Det är fråga om en rekommendation och den lagstadgade anmälningsskyldigheten gäller alltid endast betydande incidenter.[48]

Energimyndigheten tar inom sitt verksamhetsområde emot frivilliga incidentanmälningar om betydande incidenter, incidenter, cyberhot och tillbud även från andra aktörer än de som avses i cybersäkerhetslagen. Med sektor avses el-, fjärrvärme och kyla-, naturgas- och vätgasbranscherna. Den frivilliga anmälaren bör dock beakta att Energimyndigheten har delad behörighet med Tukes inom naturgas- och vätebranscherna.

---

[46] Se närmare 17 § i cybersäkerhetslagen.

[47] Bestämmelser om frivillig underrättelse finns i 15 § i cybersäkerhetslagen.

[48] Se kapitel 4.4.2.

Frivilliga anmälningar görs till Energimyndigheten via Cybersäkerhetscentrets anmälningsblankett vid Transport- och kommunikationsverket Traficom. Anmälningsapplikationen styr i ifyllandet av anmälan. Om en frivillig anmälan lämnas till Energimyndigheten på annat sätt, ska Energimyndigheten underrätta den gemensamma kontaktpunkten, dvs. Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom, om anmälan.

Energimyndigheten får prioritera besvarandet av anmälningar som avses i 11 § och hanteringen av dem i förhållande till frivilliga underrättelser (cybersäkerhetslagen 16.2 §).

5 Tillsyn

Bestämmelser om tillsynen finns i 4 kap. i cybersäkerhetslagen. Energimyndigheten har till uppgift att övervaka efterlevnaden av cybersäkerhetslagen, de föreskrifter som utfärdats med stöd av den och de bestämmelser som utfärdats med stöd av NIS2-direktivet i fråga om de aktörer som hör till Energimyndighetens behörighet (se kapitel 3.2). NIS-tillsynsmyndigheterna samarbetar sinsemellan vid genomförandet av tillsynen (26 § i cybersäkerhetslagen).

Tillsynen inriktas på de väsentliga aktörerna. Energimyndigheten kan dock inrikta tillsynen också gentemot andra än väsentliga aktörer om det finns grundad anledning att misstänka att aktören inte har iakttagit denna lag, föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet (27.1 § i cybersäkerhetslagen och se 3.6 kap.).

Energimyndigheten kan ställa de uppgifter som föreskrivs för den i denna lag i prioritetsordning enligt en riskbaserad bedömning. Energimyndigheten ska vid inriktning av tillsynen och vid beslut om användning av åtgärder enligt 29–34 § beakta arten och omfattningen av den verksamhet som avses i bilagan till lagen, informationssystemets eller kommunikationsnätets betydelse för den verksamhet som avses och de omständigheter som avses i 37 § (se cybersäkerhetslagen 27 §).

I cybersäkerhetslagen föreskrivs om Energimyndighetens tillsynsbefogenheter. Energimyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få bland annat information om hanteringen av cybersäkerhetsrisker, handlingsmodellen för riskhantering, hanteringsåtgärderna och betydande incidenter samt annan information som direkt anknyter till ovannämnda information och som är nödvändig för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker och över anmälan och rapporteringen av betydande incidenter. Informationen ska lämnas ut utan dröjsmål, i den form som Energimyndigheten begärt och avgiftsfritt (se 28 § i cybersäkerhetslagen).[49]

[49] Rätten till information enligt 28 § i cybersäkerhetslagen gäller inte sekretessbelagd information om sådan tjänsteproduktion eller användning av tjänster i säkerhetsnätet som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) eller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

Om begäran om information gäller en sådan del av riskhanteringen som aktören har lagt ut på entreprenad, är aktören skyldig att lämna informationen oberoende av om den innehas av aktören eller av en underleverantör. Aktören är alltså vid behov skyldig att skaffa den begärda informationen av sin leverantör och lämna den till Energimyndigheten.[50]

Utövande av rätten att få information är en primär och huvudsaklig åtgärd som tillsynsmyndigheten vidtar gentemot aktörerna och som syftar till att möjliggöra tillsynen över att riskhanterings- och rapporteringsskyldigheterna fullgörs.[51]

Utöver rätten att få information har Energimyndigheten rätt att förrätta inspektioner av aktörer. Inspektionen förrättas för tillsynen över att skyldigheterna enligt cybersäkerhetslagen eller föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs, i den omfattning det behövs (se 29 § i cybersäkerhetslagen). Inspektioner kan vara slumpmässiga, göras till följd av en betydande incident eller vara regelbundna och bygga på en riskbedömning för de aktörer som är mest kritiska med tanke på samhällets funktion.[52]

Energimyndigheten har dessutom rätt att i vissa situationer ålägga en aktör att låta utföra en säkerhetsrevision som gäller hanteringen av cybersäkerhetsrisker (se 30 § i cybersäkerhetslagen).

Om Energimyndigheten upptäcker att aktören inte har iakttagit ovan nämnda bestämmelser eller att det finns brister i iakttagandet av de föreskrivna skyldigheterna, föreskrivs i cybersäkerhetslagen om de tillsynsåtgärder som Energimyndigheten kan vidta för att säkerställa att skyldigheterna iakttas. I 31 § i cybersäkerhetslagen föreskrivs om tillsynsbeslut och varning. I 32 § i cybersäkerhetslagen föreskrivs om begränsning av ledningens verksamhet. I 34 § föreskrivs om möjligheten att förena ett beslut med vite, hot om tvångsutförande eller hot om avbrytande.

Påföljdsavgiftsnämnden i anslutning till Transport- och kommunikationsverket påför en administrativ påföljdsavgift på framställning av tillsynsmyndigheten, till exempel Energimyndigheten. Enligt 35 § 1 mom. i cybersäkerhetslagen kan en aktör påföras en administrativ påföljdsavgift om denne uppsåtligen eller av grov oaktsamhet försummar

1) att fullgöra riskhanteringsskyldigheten enligt 7 §, att utarbeta en handlingsmodell för hantering av cybersäkerhetsrisker enligt 8 § eller att beakta de delområden som avses i 9 § 1 mom. som en del av handlingsmodellen för hantering av cybersäkerhetsrisker,

2) att vidta de åtgärder som avses i 9 § 2 mom.,

[50] Se RP 57/2024 rd., s. 198.
[51] RP 57/2024 rd., s. 197.
[52] RP 57/2024 rd., s. 200.

3) att lämna en incidentanmälan enligt 11 §, delrapport enligt 12 § eller slutrapport enligt 13 § till tillsynsmyndigheten,

4) att lämna tillsynsmyndigheten de uppgifter som avses i 41 §.

Närmare bestämmelser om påförande, maximibelopp och avstående från påföljdsavgift finns i 5 kap. i cybersäkerhetslagen.

Energimyndigheten kan återkalla ett elnätstillstånd, naturgasnätstillstånd eller en befrielse eller ett undantagslov som avses i 12 § i elmarknadslagen eller 11 § i naturgasmarknadslagen om tillståndshavaren upprepade gånger och i väsentlig grad bryter mot cybersäkerhetslagen och den varning som i förväg getts tillståndshavaren om att tillståndet kommer att återkallas inte har lett till att bristerna i verksamheten har rättats till (23 § 6 punkten i lagen om tillsyn över el- och naturgasmarknaden 590/2013.

6 Anmälan till aktörsförteckningen (VERTTI-tillsynsuppgiftssystemet)

6.1 NIS2-aktörsförteckning i VERTTI-tillsynsuppgiftssystemet

Energimyndighetens aktörsförteckning enligt 41 § i cybersäkerhetslagen, dvs. NIS2-aktörsförteckningen, finns i VERTTI-tillsynsuppgiftssystemet. Länk till datasystemet VERTTI: https://vertti.energiavirasto.fi/.

Observera: Bekanta dig noggrant med kapitel 3 i denna anvisning om cybersäkerhetslagens tillämpningsområde innan du påbörjar anmälan.

För anmälan till aktörsförteckningen behöver användaren fullmakten ”Anmälan av aktörsuppgifter i anslutning till cybersäkerhet”. Mer information om fullmakter och befullmäktigande finns på webbplatsen suomi.fi: https://www.suomi.fi/fullmakter/fullmaktsarenden/anmalan-av-aktorsuppgifter-i-anslutning-till-cybersakerhet/ebecc9b754228fda35055eebd09b89dc.

När användaren har Suomi.fi-fullmakt visas i menyn i övre kanten rubriken ”NIS2-aktörsförteckning” och en knapp, genom vilken användaren kan redigera användarinformation.

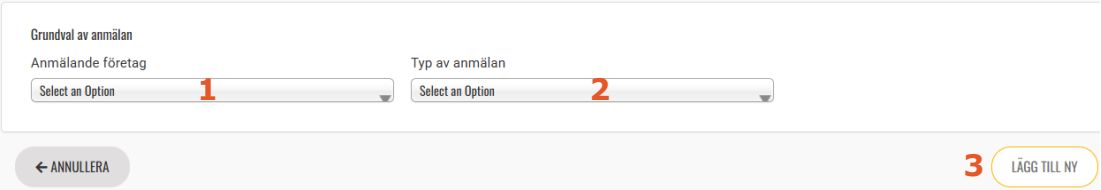
6.2 Att skapa ny anmälan

Börja skapa en ny anmälan på fliken NIS2-aktörsförteckning genom att klicka på knappen ”Ny”, som öppnar anmälans val av basuppgifter.

På sidan ”Lägg till ny” ska anmälaren välja det företag som lämnar in anmälan (1) och som typ av anmälan väljs ”Ny anmälan till NIS2-aktörsförteckningen” i rullgardinsmenyn. En ny anmälan skapas genom att klicka på ”Lägg till ny” (3).

Användaren kan välja flera företag om användaren har fullmakt att uträtta ärenden för flera företag. Anmälan görs företagsspecifikt, dvs. anmälan ska skapas separat för varje företag som ska anmälas.

Ett företag kan ha endast en aktiv anmälningsblankett. Om du anmäler ändringar i redan anmälda uppgifter eller om du anmäler utträde ur aktörsförteckningen, öppna anmälan på föregående sida.



På huvudsidan för NIS2-aktörsförteckningen skapas därefter en ny anmälan som du kan fylla i genom att välja ”Fyll i anmälan” (1) i kolumnen ”Öppna anmälan”.

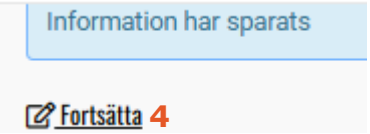
6.3 Ifyllande av ny anmälan

6.3.1 Anmälningsblankettens struktur och knappar

De punkter som ska fyllas i på anmälan öppnas när du väljer ”NIS2-aktörsförteckning – bakgrundsuppgifter” (1) och ”NIS2-aktörsförteckning – tilläggsuppgifter” (2). Båda flikarna ska fyllas i och sparas med knappen ”Spara” (3) innan anmälan skickas.

Med knappen ”Granska” (A) kan användaren kontrollera om alla obligatoriska punkter har besvarats. Med knappen ”Ta bort anmälan” (B) kan användaren radera en påbörjad anmälan. När anmälan har tagits bort skapas en ny anmälan enligt kapitel 6.2.

Efter att du sparat kan du gå tillbaka till anmälan genom att klicka på ”Fortsätt” (4).



6.3.2 Uppgifter som ska anmälas: fliken Bakgrundsuppgifter

Punkt 1: Företagets namn

Företagets namn fylls i automatiskt på basis av valet av basuppgifter i anmälan.

Punkt 2: FO-nummer

Företagets FO-nummer fylls i automatiskt på basis av valet av basuppgifter i anmälan.

Företagets kontaktuppgifter

Punkt 3: Gatuadress

Lägg till information om företagets kontaktuppgifter.

Punkt 4: Postnummer

Lägg till information om företagets kontaktuppgifter.

Punkt 5: Ort

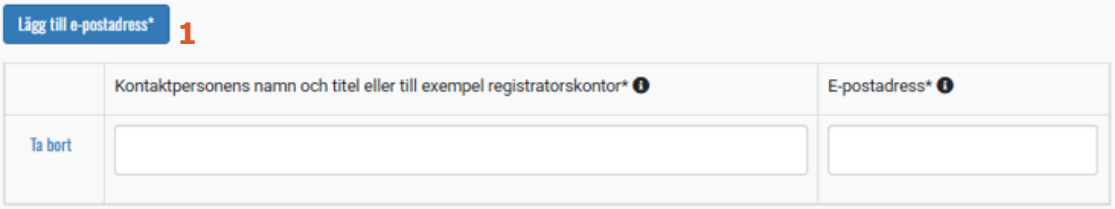
Lägg till information om företagets kontaktuppgifter.

Punkt 6: Telefonnummer

Lägg till information om företagets kontaktuppgifter. Användaren kan ange flera än ett telefonnummer. Börja lägga till ett telefonnummer genom att välja ”Lägg till telefonnummer” (1). Ange vid varje telefonnummer kontaktpersonens namn och titel eller om det till exempel är fråga om ett journummer.

Punkt 7: E-postadress

Lägg till information om företagets kontaktuppgifter. Användaren kan ange flera än en e-postadress. Börja lägga till e-postadressen genom att välja ”Lägg till e-postadress” (1). Ange vid varje e-postadress kontaktpersonens namn och titel eller om det till exempel är fråga om t.ex. registratorskontoret.



Punkt 8: Deltagande i det frivilliga arrangemanget för informationsutbyte om cybersäkerhet

Företaget ska meddela om det deltar i det frivilliga arrangemang för informationsutbyte om cybersäkerhet vid Traficoms Cybersäkerhetscenter. Observera: Ange nuläget.

Frivilliga arrangemang för informationsutbyte i enlighet med cybersäkerhetslagens 23 § anses bland annat innefatta samarbete i informationsutbytesgrupper med Traficoms Cybersäkerhetscenters CSIRT-enhet, vilket inkluderar frivillig informationsdelning. Som frivilligt informationsdelningsarrangemang beaktas också att aktören tillhör en branschspecifik e-postlista som upprätthålls av Traficoms Cybersäkerhetscenters CSIRT-enhet. Alla aktörer som omfattas av cybersäkerhetslagen har möjlighet att ansluta sig till e-postlistan. Via listorna skickas informationssäkerhetsmeddelanden om ämnen som är aktuella för sektorn.

Mer information om e-postlistor och om hur du ansluter dig till dem: https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/lagesbild?toggle=Sektorspecifik%20l%C3%A4gesbild%20och%20meddelanden

6.3.3 Uppgifter som ska anmälas: fliken Tilläggsuppgifter

Ange den verksamhet eller aktörstyp som avses i bilaga I till cybersäkerhetslagen

Punkt 8: Välj inom vilken bransch företaget är verksam

Välj i rullgardinsmenyn de delsektorer som Energimyndigheten övervakar och som nämns i bilagan till cybersäkerhetslagen. Valbara delsektorer är el, fjärrvärme eller fjärrkyla, gas och väte. Ange alla delsektorer där aktören är verksam och som omfattas av cybersäkerhetslagen.

Om aktören utöver den verksamhet som övervakas av Energimyndigheten bedriver annan verksamhet som omfattas av cybersäkerhetslagen och som övervakas av en annan NIS2-tillsynsmyndighet, ska den anmäla sig separat till aktörsförteckningarna hos alla dessa myndigheter.

Observera: Endast de delsektorer som övervakas av Energimyndigheten kan väljas. Inom energisektorn är till exempel Säkerhets- och kemikalieverket (Tukes) den tillsynsmyndighet som övervakar oljesektorn.

Punkt 8.1: Välj vilken verksamhet inom den valda branschen företaget bedriver

När användaren har valt inom vilken sektor företaget är verksamt, ska användaren precisera vilken verksamhet inom branschen som företaget bedriver. Välj i rullgardinsmenyn de aktörstyper enligt cybersäkerhetslagen som beskriver företaget och som gör att företaget omfattas av cybersäkerhetslagens tillämpningsområde.

Observera: Endast de aktörstyper som övervakas av Energimyndigheten kan väljas. När det gäller gas och väte har Energimyndigheten och Säkerhets- och kemikalieverket (Tukes) delad tillsynsbehörighet som är beroende av den verksamhet som företaget bedriver inom delsektorn (se kapitel 3).

Om aktören bedriver flera verksamheter enligt cybersäkerhetslagen, varav en del omfattas av Energimyndighetens tillsyn och en del av till exempel Säkerhets- och kemikalieverkets (Tukes) tillsyn, ska aktören anmäla sig separat till den aktörsförteckning som upprätthålls av respektive myndighet.

Närmare uppgifter om aktörens verksamhet är nödvändiga för skötseln av tillsynsuppgifterna enligt cybersäkerhetslagen.

Viktig eller väsentlig aktör

Punkt 9: Välj om aktören är en viktig eller väsentlig aktör

Välj i rullgardinsmenyn om aktören är en viktig eller väsentlig aktör (se kapitel 3.6).

Punkt 9.1: Varför är företaget en väsentlig aktör?

Om användaren har valt att aktören är väsentlig, ska användaren precisera varför aktören är en väsentlig aktör. Välj i rullgardinsmenyn varför företaget är en väsentlig aktör.

Observera: Energimyndigheten har gett anvisningar i kapitel 3.4 i denna anvisning om att aktörer som oberoende av storlek hör till tillämpningsområdet för att säkerställa en enhetlig tolkning av undantagskriterierna ska vänta på att en förordning av statsrådet utfärdas. Om aktören på det sätt som presenteras i kapitel 3.3 på grund av sin storlek omfattas av tillämpningsområdet för cybersäkerhetslagen, ska aktören anmäla sig till Energimyndigheten som en aktör som ska övervakas. När kriterierna för aktörer oberoende av storlek har preciserats genom förordning av statsrådet, ska en aktör som uppfyller kriterierna anmäla sig till eller uppdatera sin anmälan i NIS-aktörsförteckningen.

Aktörer enligt CER-direktivet definieras för första gången 2026 (se kapitel 3.5).

Punkt 9.1.1: Välj varför företaget är väsentlig oberoende av sin storlek

Om användaren har valt att aktören är väsentlig oberoende av sin storlek, ska användaren precisera vilken eller vilka av de fyra undantagsgrunderna aktören uppfyller.

Observera: Energimyndigheten har gett anvisningar i kapitel 3.4 i denna anvisning om att aktörer som oberoende av storlek hör till tillämpningsområdet för att säkerställa en enhetlig tolkning av undantagskriterierna ska vänta på att en förordning

av statsrådet utfärdas. Om aktören på det sätt som presenteras i kapitel 3.3 på grund av sin storlek omfattas av tillämpningsområdet för cybersäkerhetslagen, ska aktören anmäla sig till Energimyndigheten som en aktör som ska övervakas. När kriterierna för aktörer oberoende av storlek har preciserats genom förordning av statsrådet, ska en aktör som uppfyller kriterierna anmäla sig till eller uppdatera sin anmälan i NIS-aktörsförteckningen.

Punkt 9.1.2: Motivera varför företaget är en väsentlig aktör oberoende av sin storlek

Om användaren har valt att aktören är väsentlig oberoende av sin storlek, ska användaren motivera varför företaget är en väsentlig aktör. Välj flera grunder vid behov. Detta är fallet till exempel om aktören överskrider kriterierna för medelstora företag och aktören också har identifierats som en kritisk aktör enligt CER-direktivet.

Observera: Energimyndigheten har gett anvisningar i kapitel 3.4 i denna anvisning om att aktörer som oberoende av storlek hör till tillämpningsområdet för att säkerställa en enhetlig tolkning av undantagskriterierna ska vänta på att en förordning av statsrådet utfärdas. Om aktören på det sätt som presenteras i kapitel 3.3 på grund av sin storlek omfattas av tillämpningsområdet för cybersäkerhetslagen, ska aktören anmäla sig till Energimyndigheten som en aktör som ska övervakas. När kriterierna för aktörer oberoende av storlek har preciserats genom förordning av statsrådet, ska en aktör som uppfyller kriterierna anmäla sig till eller uppdatera sin anmälan i NIS-aktörsförteckningen.

Punkt 10: Fritt formulerad beskrivning av aktörs verksamhet

Punkten är inte obligatorisk. Under punkten kan användaren lägga till en fritt formulerad beskrivning av företagets verksamhet. En aktör som hör till en koncern kan lyfta fram till vilken koncern företaget hör. Användaren kan också ange om företaget utöver Energimyndigheten övervakas av någon annan NIS2-tillsynsmyndighet.

Verksamhetens geografiska omfattning

Punkt 11: EU-medlemsstater, där företaget tillhandahåller tjänster som omfattas av NIS2-direktivets tillämpningsområde

Aktören ska förse tillsynsmyndigheten med en förteckning över de medlemsstater i Europeiska unionen där den tillhandahåller tjänster som omfattas av NIS2-direktivets tillämpningsområde. Användaren väljer alla lämpliga länder i rullgardinsmenyn.

IP-adressintervall

Punkt 12: IP-adressintervall

Aktören ska meddela alla sina offentliga IP-adressintervall.

Anmälan av IP-adresser möjliggör en förebyggande upptäckt av sårbarheter, cyberhot och osäkert konfigurerade inställningar i kommunikationsnät och informationssystem gällande aktörer som omfattas av cybersäkerhetslagen. Aktören informeras om dessa observationer, vilket förbättrar aktörernas möjligheter att skydda sig mot utnyttjande av sårbarheter och cyberhot. I Finland ansvarar Cybersäkerhetscentrets CSIRT-enhet för dessa åtgärder och har rätt att få uppgifter ur förteckningen över aktörer av Energimyndigheten.

Om aktörens IP-adresser administreras av någon annan part, till exempel en teleoperatör eller tjänsteleverantör, ska aktören som omfattas av regleringen skaffa dessa IP-adressuppgifter och vidarebefordra uppgifterna till tillsynsmyndigheten.

IP-adress: Numerisk kod som identifierar en databehandlings- eller dataöverföringsenhet eller nätanslutning som är kopplad till internet, till exempel 198.51.100.34

IP-adressintervall: IP-adressintervall som bildas av flera offentliga webbadresser (IP-adresser).

IP-adressintervallet ska anges i NIS2-aktörsförteckningen i följande format:

- Till exempel 198.51.100.0-198.51.100.255 eller 93.190.96.0-93.190.103.255 (IP-range) eller
- Till exempel 198.51.100.0/24 eller 93.190.96.0/21 (CIDR-format)

Uppgifterna kan vid behov också meddelas som enskilda IP-adresser, om det större adressintervallet inte är känt: till exempel 198.51.100.34

Uppgifterna kan också anges i IPv6-format: till exempel 2001:db8:3333:4444:5555:6666:7777:8888

Observera: Följande nät är så kallade privatnät, dvs. interna adressintervall, och ska inte anmälas till aktörsförteckningen:

- IPv4:

  10.0.0.0-10.255.255.255 eller 10.0.0.0/8

  172.16.0.0-172.31.255.254 eller 172.16.0.0/12

  192.168.0.0-192.168.255.255 eller 192.168.0.0/24

- IPv6:

  fc00::/7

  fec0::/10

Om en aktör har både statiska och dynamiska IP-adresser, ska aktören lämna Energimyndigheten åtminstone uppgifter om statiska IP-adresser samt försöka lämna relevanta uppgifter om dynamiska IP-adresser, till exempel en förteckning över de

nätblock som aktörens IP-adress är reserverad för, samt antalet sådana adresser eller annan motsvarande ändamålsenlig information.

För att utreda vilka uppgifter som behövs rekommenderar vi att du kontaktar din IT-administratör eller tjänsteleverantör.

Aktörerna ska utan dröjsmål och i varje fall inom två veckor från ändringsdagen underrätta tillsynsmyndigheten om alla ändringar i de IP-adressuppgifter som lämnats in.

Mer information

Punkt 13: Jag har kontrollerat att uppgifterna på blanketten är korrekta

Användaren väljer att de ifyllda uppgifterna har kontrollerats.

Punkt 14: Samtycke till elektronisk delgivning

Användaren väljer om hen samtycker till att Energimyndigheten skickar alla handlingar och meddelanden som gäller NIS2-aktörsförteckningen till kontaktpersonens e-postadress. Samtycket omfattar beslut, begäran om tilläggsutredningar, andra dokument och meddelanden.

Bekräftelsemeddelanden om anmälan till aktörsförteckningen, anmälan av ändrade uppgifter och utträde ur aktörsförteckningen samt meddelande om begäran om rättelse skickas alltid automatiskt per e-post till kontaktpersonens e-postadress.

Punkt 15: Namn

Uppgiften fylls i automatiskt i samband med att anmälningsblanketten skickas. Om uppgifterna är bristfälliga ska uppgifterna korrigeras i användarens egna uppgifter, som finns uppe till höger på sidan.

Punkt 16: Telefonnummer

Uppgiften fylls i automatiskt i samband med att anmälningsblanketten skickas. Om uppgifterna är bristfälliga ska uppgifterna korrigeras i användarens egna uppgifter, som finns uppe till höger på sidan.

Punkt 17: E-postadress

Uppgiften fylls i automatiskt i samband med att anmälningsblanketten skickas. Om uppgifterna är bristfälliga ska uppgifterna korrigeras i användarens egna uppgifter, som finns uppe till höger på sidan.

Punkt 18: Skickad

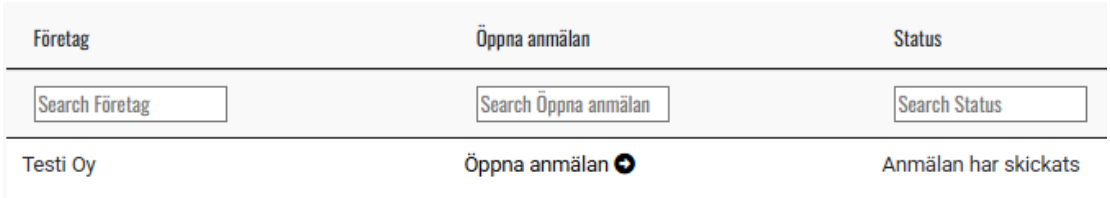
Uppgiften fylls i automatiskt i samband med att anmälningsblanketten skickas.

6.4 Att skicka ny anmälan

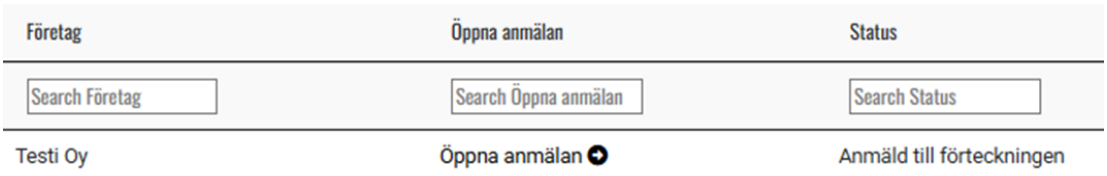
När användaren har fyllt i anmälan kan användaren med knappen ”Granska” (1) kontrollera att alla obligatoriska punkter har fyllts i. Om obligatoriska punkter inte har fyllts i påpekar systemet detta och användaren ska fylla i de uppgifter som saknas. Användaren kan ändra uppgifterna tills anmälan har skickats.

Anmälan skickas med knappen ”Skicka” (2).

När anmälan har skickats ändras dess status till ”Anmälan har skickats”.



Användaren får en bekräftelse per e-post när aktören är anmäld i aktörsförteckningen. Anmälans status ändras därefter till ”Anmäld till förteckningen”.



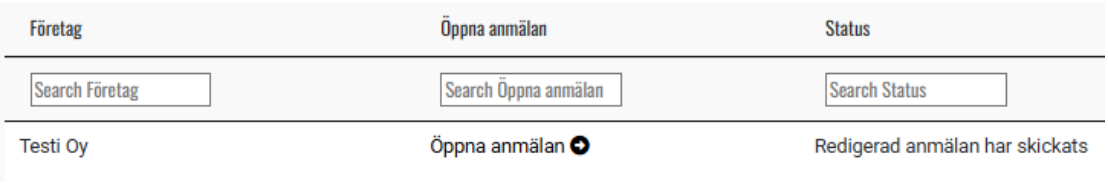
6.5 Anmäl ändrade uppgifter till aktörsförteckningen

Om det sker ändringar i aktörens uppgifter börjar användaren anmäla de ändrade uppgifterna genom att öppna aktörens anmälan med knappen ”Öppna anmälan”.

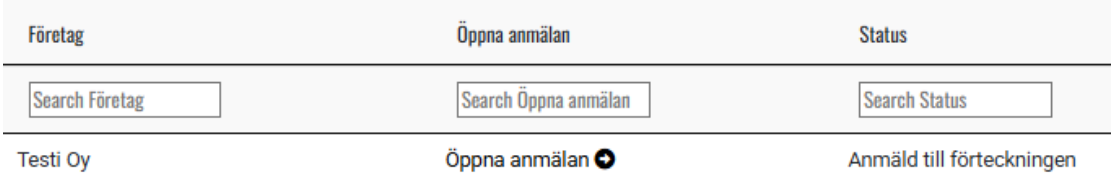
Genom att välja ”Redigera uppgifter” (2) kan användaren redigera uppgifterna under flikarna bakgrundsuppgifter och tilläggsuppgifter.

Användaren sparar uppgifterna med knappen ”Spara” (3) innan anmälan skickas. När användaren har redigerat, lagt till eller tagit bort de nödvändiga uppgifterna skickar användaren den redigerade anmälan till Energimyndigheten med knappen ”Skicka” (4).

När de redigerade uppgifterna har skickats ändras anmälans status till ”Redigerad anmälan har skickats”.



Användaren får en bekräftelse per e-post när de ändrade uppgifterna om aktören har anmälts till Energimyndighetens NIS2-aktörsförteckning. Anmälans status ändras därefter till ”Anmäld till förteckningen”.

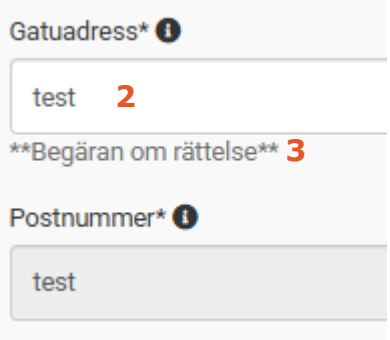


6.6 Energimyndigheten begär rättelse av anmälan

Om Energimyndigheten anser att den skickade anmälan kräver rättelse av företaget, returnerar Energimyndigheten anmälan till företaget och öppnar de punkter i anmälan som ska ändras. Ett e-postmeddelande om begäran om rättelse skickas alltid automatiskt till e-postadressen av den användare som gjort anmälan.

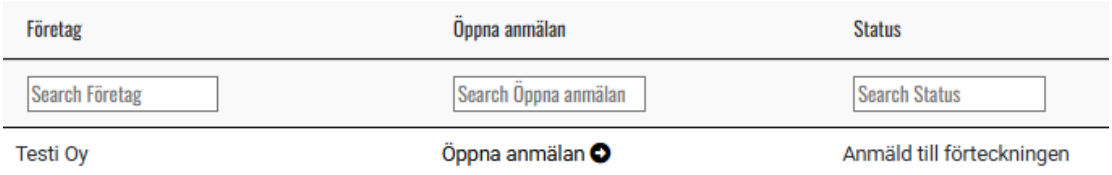
Börja komplettera de punkter som kräver rättelse genom att öppna aktörens anmälan med knappen ”Öppna anmälan” (1)

De punkter som kräver korrigering hittas genom att öppna flikarna i anmälan. Den punkt som kräver korrigering identifieras av att de har öppnats för redigering (2) och under dem finns en kommentar med **-tecken (3) om varför punkten kräver korrigering. Postnumret har inte öppnats på bilden nedan.



Användaren sparar uppgifterna med knappen ”Spara” (4) innan anmälan skickas. När användaren har gjort de nödvändiga ändringarna skickas den korrigerade anmälan med knappen ”Skicka” (5).

Användaren får en bekräftelse per e-post när uppgifterna om aktören är anmälda till Energimyndighetens NIS2-aktörsförteckning. Anmälans status ändras därefter till ”Anmäld till förteckningen”.



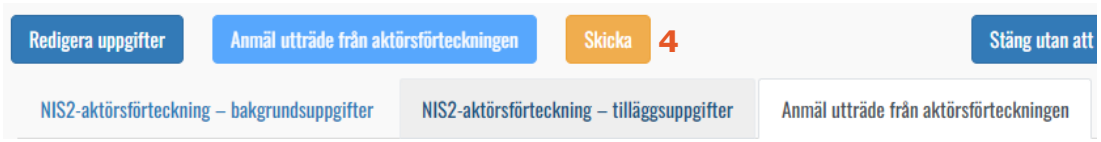
6.7 Anmäl utträde från aktörsförteckningen

Om aktören inte längre uppfyller förutsättningarna i cybersäkerhetslagen och inte längre omfattas av cybersäkerhetslagen, ska användaren anmäla utträdet ut aktörsförteckningen i VERTTI-tillsynsuppgiftssystemet.

Anmälan inleds genom att öppna aktörens anmälan med knappen ”Öppna anmälan” (1).

När användaren har öppnat anmälningsblanketten gör användaren anmälan genom att välja ”Anmäl utträde från aktörsförteckningen” (2). En ny flik ”Anmäl utträde från aktörsförteckningen” (3) öppnas för anmälan.

Användaren ska motivera varför aktören inte längre omfattas av cybersäkerhetslagen. När motiveringen har lagts till kan användaren skicka anmälan med knappen "Skicka” (4).



När anmälan om utträde från aktörsförteckningen har skickats ändras anmälans status till ”Utträde har begärts”

Användaren får en bekräftelse per e-post när aktören har utträtt från aktörsförteckningen. Anmälningsblanketten finns inte längre till företagets påseende i VERTTI-tillsynsuppgiftssystemet. Om företaget senare ska anmäla sig till aktörsförteckningen på nytt, ska en ny anmälan göras.

7 Mer information och länkar

Energimyndighetens webbplats om cybersäkerhet: https://energiavirasto.fi/sv/cybersakerhet

Transport- och kommunikationsverkets Cybersäkerhetscenter har sammanställt ett allmänt informationspaket om NIS2-direktivet: https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/nis2-europeiska-unionens-cybersakerhetsdirektiv

Cybersäkerhetscentrets anvisningar och guider för organisationer och företag: https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/anvisningar-och-guider-organisationer-och-foretag

Cybersäkerhetscentrets cybermätare: www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren

Cybersäkerhetslagen (124/2025): https://finlex.fi/sv/lagstiftning/forfattningssamling/2025/124

Kommissionens rekommendation 2003/361/EY om definitionen av mikroföretag samt små och medelstora företag: https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=celex%3A32003H0361

Användarhandledning om definitionen av SMF-företag: https://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0018.03/DOC_1

NIS2-direktivet: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=sv

CER-direktivet: https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=sv