Datum
2024-07-01

Energisystem
Emma Johansson, 08-677 25 05
emma.johansson@energiforetagen.se

Säkerhet för energisektorn – en översikt över nuvarande och kommande regleringar

Energiföretagens medlemsföretag berörs av många lagstiftningar inom säkerhetsområdet. Detta dokument sammanfattar de viktigaste lagstiftningarna som berör energisektorn. Fokus är främst på cybersäkerhet men även andra säkerhetsområden berörs. Utöver de lagstiftningar som sammanfattas här finns det flera andra relevanta lagstiftningar som inte riktar sig specifikt mot energisektorn, exempelvis dataskyddsförordningen (GDPR).

Innehåll

Säkerhetsarbete bidrar till en resilient energiförsörjning

Energiförsörjningen är helt avgörande för samhällets försörjningstrygghet. Ett omfattande, långvarigt avbrott får konsekvenser för många samhällsviktiga verksamheter och för totalförsvaret. Därför ska de mest nödvändiga funktionerna inom energiförsörjningen kunna upprätthållas vid kriser i fredstid, men även vid höjd beredskap och krig.

Säkerhets- och beredskapsfrågor är en viktig del i att skydda vårt energisystem och vårt samhälle i stort. I takt med omvärldsutvecklingen av ökade hot, risker och ett ökat militärt krigshot med väpnad konflikt blir ett kontinuerligt och långsiktigt säkerhetsarbete allt väsentligare. Detta i kombination med energisektorns roll som kritisk för samhällets försörjningstrygghet förstärker ytterligare behoven genom den ökande elektrifieringen och klimatomställningen.

I takt med att hoten förändrats så växer nu även kraven på effektiv cybersäkerhet, resiliens och beredskap från lagstiftare och tillsynsmyndigheter. Resiliens handlar om att vid en händelse så snabbt som möjligt återkomma till normaldrift, och att dra lärdomar av händelsen. Riskanalyserna har förändrats från att analysera kriser till att omfatta hela hotskalan under gråzon med cyberattacker, sabotage och spionage samt desinformationsspridning till att även ta höjd för ett totalförsvarsperspektiv i verksamhetsplanering och beslut.

Exempel på nuvarande och kommande regleringar för energisektorn redovisas nedan. Genom att införa nya krav och kontinuerligt följa upp åtgärder och regelefterlevnad kan energibranschen tillsammans bättre ta sig an dagens och framtidens hot och risker när det gäller att säkerställa resilient energiförsörjning och minimera avbrott.

Checklista för företag inom energisektorn

Denna checklista är inte avsedd att vara komplett utan syftar till att ge en översiktlig bild av aktiviteter som företag inom energisektorn behöver beakta inom säkerhetsarbetet för regelefterlevnad. Tillsammans ingår att kontinuerligt följa upp den digitala och fysiska miljön, personal och leverantörer samt konsulter som har tillgång till uppgifter i system och anläggningar. En övergripande planering för införande av åtgärder, uppföljning och översyn rekommenderas.

1. Utvärdera aktuellt tillstånd i verksamheten. Gör en grundlig bedömning av ditt företags befintliga policys, processer, rutiner och förmågor. Identifiera styrkor, svagheter och luckor enligt en SWOT- eller GAP-analys.
2. Utvärdera säkerheten för kritisk infrastruktur. Särskilt nätverk och system samt produkter för att i första hand minimera störningar och avbrott i produktion, distribution och handel med energi.
3. Förstå regelkrav. Bekanta dig med regleringar och bestämmelser. Förstå vad som förväntas och vilka krav som ställs när det gäller säkerhetsåtgärder. Beakta särskilt de sektorspecifika reglerna för energisektorn som är skall krav om verksamheten omfattas.
4. Identifiera och hantera risker. Utveckla en riskhanteringsstrategi där påverkan och konsekvenser på företaget ekonomi och varumärke, cybersäkerheten, den fysiska miljön och personalen omhändertas. Identifiera potentiella hot, risker och sårbarheter som är generella och specifika för din verksamhet. Prioritera risker baserat på konsekvens och sannolikhet.
5. Implementera säkerhetsåtgärder. Exempelvis förbättra nätverkssäkerheten, implementera kontrollpunkter regelbundet, utveckla intrångsdetekteringssystem och åtkomstkontroller. Härda utrustning. Uppdatera programvara regelbundet och korrigera kända sårbarheter så snart som möjligt.
6. Använd den informationssäkerhet som krävs och säkra kommunikationskanaler vid behov. Kryptera skyddsvärda data under överföring och använd säkra protokoll.
7. Utbilda personal. Utbilda anställda i policys och rutiner för säkerhet. Se till att de förstår verksamhetens ansvar kopplat till sin roll när det gäller att upprätthålla säkerheten.
8. Öva personalen. Främja en säkerhetsmedveten kultur inom organisationen för att förebygga incidenter och öka medvetenheten om hot och risker genom övningar.
9. Upprätta plan för hantering av incidenter. Definiera och dokumentera procedurer för hantering specifikt för cybersäkerhetsincidenter.
10. Upprätta andra planer. Planer för kontinuitetshantering, beredskapsplan, planer för manuell hantering samt återställningsplaner efter eventuella incidenter för att minimera störningar och avbrott.
11. Upprätta kommunikationskanaler och förbered kommunikation och budskap internt och externt. För att lättare sortera och rapportera lägesbilder och reagera på eventuella tillbud, olyckor och kriser eller inkommande information som behöver omhändertas.
12. Samarbeta och dela information. Samarbeta med andra företag, organisationer och tillsynsorgan. Dela hotinformation och lär dig av andras erfarenheter.
13. Dokumentera regelefterlevnad. Upprätthåll register över efterlevnadsarbete. Dokumentera principer, procedurer och säkerhetskontroller. Här är standarder ett bra verktyg att ta hjälp av.
14. Medverka vid interna och externa granskningar. Var beredd på och medverka aktivt vid myndighetstillsyn, revisioner och bedömningar.

Gällande och kommande regleringar

1. Direktivet om nät- och informationssäkerhet (NIS)

Kort om direktivet

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, eller NIS-direktivet som trädde i kraft 2016 och var den första EU-omfattande cybersäkerhetslagstiftningen. NIS-direktivet är uppbyggt kring fyra huvuddelar:

1 Stärkande av den nationella cybersäkerhetskapaciteten, särskilt genom antagande av en nationell strategi för cybersäkerhet, inrättande av en eller flera nationella behöriga myndigheter för cybersäkerhet och inrättande av minst en enhet för hantering av cybersäkerhetsincidenter (CSIRT-enhet).
2 Inrättande av en ram för samarbete mellan medlemsstaterna, och i synnerhet inrättandet av samarbetsnätverket som består av företrädare för medlemsstaterna, kommissionen och Enisa och CSIRT-nätverket (som består av företrädare för nationella CSIRT-enheter och CERT-EU) i syfte att underlätta informationsutbyte om potentiella risker och sårbarheter.
3 Förstärkning av säkerheten för leverantörer av samhällsviktiga tjänster genom minimikrav på säkerhet och rapportering av incidenter som kan ha en betydande inverkan på relevanta nationella myndigheter:
4 Införande av gemensamma europeiska cybersäkerhetsregler för leverantörer av digitala tjänster på områdena molntjänster, sökmotorer och internetbaserade marknadsplatser.

Syftet med NIS-lagstiftningen är att uppnå en hög nivå av säkerhet i nätverk och informationssystem för samhällsviktiga tjänster. Detta ska uppnås genom krav på införande av systematiskt och riskbaserat informationssäkerhetsarbete och incidentrapportering. Organisationen ska också vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuitet. Nuvarande NIS-direktivet genomfördes i svensk rätt 2018 genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NISL) och Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NISF). NIS-lagen gäller inte om säkerhetsskyddslagen är tillämplig enligt 8 § NISL. Myndigheten för samhällsskydd och beredskap (MSB) har föreskriftsrätt.

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt NIS-direktiv och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Betydelse/konsekvenser för energisektorn

Energisektorn omfattades redan av NIS-direktivet, med el, gas och olja som delsektorer. Anmälningsplikt råder för de som identifierat sig som NIS-leverantör enligt MSBFS 2024:4 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Energimyndigheten har tagit fram sektorsspecifik föreskrift Statens Energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (STEMFS 2021:3). Samt vägledning på föreskriften: Vägledning till Statens Energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (ER 2022:17).

Efterlevnad av regelverket följs upp genom tillsyn. För energiförsörjningen är det Energimyndigheten som är tillsynsmyndighet för hela NIS-lagstiftningen.

2. Direktivet om nät- och informationssäkerhet (NIS2)

Kort om det direktivet och lagstiftningen

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, eller NIS2-direktivet som tillhandahåller en rättslig ram för att hålla jämna steg med den ökade digitaliseringen och en föränderlig hotbild mot cybersäkerheten.

I kommissionens översyn av NIS-direktivet drogs slutsatsen att genomförandet av direktivet visade sig vara en utmaning på grund av dess begränsade tillämpningsområde, dess brist på tydlighet när det gäller tillämpningsområde och befogenheter, men också på grund av den ineffektiva kontrollen av efterlevnaden på medlemsstatsnivå och alltför stora skillnader mellan de nationella strategierna. NIS2-direktivet antogs i syfte att bredda dess tillämpningsområde. Kommissionen kan lämna delegerade akter kopplat till genomförandet av kraven i NIS2-direktivet för att anpassa och harmonisera reglerna på EU-nivå.

I Sverige kommer NIS2-direktivet att implementeras genom en ny lag, cybersäkerhetslagen och en ny förordning, cybersäkerhetsförordningen (ej fastställda ännu). Den nu gällande NIS-lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster ska då upphävas.

Enligt NIS2-direktivet är medlemsstaterna skyldiga att ytterligare stärka sin cybersäkerhetskapacitet genom att utvidga tillämpningsområdet för sina nationella cybersäkerhetsstrategier och genom att öka sitt samarbete. Dessutom måste de inrätta ramar för hantering av cybersäkerhetskriser och en samordnad sårbarhetsrapportering. Det europeiska samarbetet utvidgas också, både på strategisk och teknisk nivå, men också på krishanteringsnivå genom inrättandet av ett nytt nätverk, Cyber Crisis Liaison Organisation Network (CyCLONe).

En av de största förändringarna är den enorma utvidgningen av tillämpningsområdet för NIS2 jämfört med NIS-direktivet. NIS2 omfattar 18 sektorer, däribland energisektorn. Förutom nya sektorer har också nya typer av enheter inom befintliga sektorer lagts till i direktivets tillämpningsområde. Distinktionen mellan "väsentliga" och "viktiga" enheter görs nu på grundval av enhetens storlek, dess omsättning och vilken typ av enhet det rör sig om. "Väsentliga" och "viktiga" entiteter som omfattas av direktivet måste vidta lämpliga åtgärder för att hantera riskerna för säkerheten i sina nätverks- och informationssystem och för att förebygga incidenter eller mildra effekterna av incidenter. I NIS2-direktivet fastställs också mer omfattande regler kring incidentrapportering till nationella behöriga myndigheter.

Överträdelser kan resultera i betydande ekonomiska sanktioner. Väsentliga entiteter som överträder artikel 21 eller 23, kan få sanktionsavgifter på högst 10 000 000 EUR eller högst 2 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst.

Betydelse/konsekvenser för energisektorn

Den nya cybersäkerhetslagen har föreslagits träda i kraft 1 januari 2025. Energisektorn är utpekad som väsentlig entitet och omfattades redan av NIS-direktivet, med el, gas och olja som delsektorer. I NIS2-direktivet tillkommer inom energisektorn fjärrvärme och fjärrkyla. Enligt NIS2 måste verksamheterna utföra självutvärdering och självregistrering genom anmälningsplikt för att informera myndigheterna om de kriterier som fastställs i lagstiftningen. Energimyndigheten föreslås bli tillsynsmyndighet för energisektorn.

3. Kritiska entiteters motståndskraft (CER)

Kort om direktivet

Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft, eller CER-direktivet, som syftar till att stärka kritiska entiteters motståndskraft mot en rad hot och risker. Direktivet trädde i kraft den 16 januari 2023. EU-länderna har nu fram till den 17 oktober 2024 på sig att anta nationell lagstiftning för att införliva direktivet. Preliminärt sker den svenska implementeringen genom den nya lag som träder i kraft först under 2025. De behöriga myndigheterna ska sedan använda förteckningen i Bilagan till CER-direktivet för att göra en riskbedömning senast den 17 januari 2026.

I CER-direktivet konstateras att kritiska verksamhetsutövare spelar en avgörande roll för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden. Det är därför enligt direktivet viktigt att det på unionsnivå skapas en reglering som syftar till att stärka kritiska verksamhetsutövares motståndskraft genom att fastställa harmoniserade minimiregler. Det är också viktigt att bistå verksamhetsutövarna genom enhetligt stöd och tillsynsåtgärder.

Genom CER-direktivet upphävdes rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (ECI-direktivet).

I rådets direktiv 2008/114/EG föreskrivs ett förfarande för att klassificera infrastruktur i energi- och transportsektorerna som europeisk infrastruktur, vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Vid utvärderingen av det direktivet konstaterades att säkerhetsåtgärderna i det direktivet inte är tillräckliga för att förhindra alla störningar från att uppstå. Det är därför nödvändigt att säkerställa att risker redovisas bättre, att skapa enhetlighet i rollen och uppgifterna för kritiska verksamhetsutövare och att anta unionsregler för att stärka kritiska verksamhetsutövares motståndskraft. Kritiska verksamhetsutövare bör kunna öka sin förmåga att förebygga, skydda sig mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från incidenter som kan störa tillhandahållandet av samhällsviktiga tjänster.

Vidare anges i direktivet att kritiska verksamhetsutövare behöver rustas bättre eftersom det finns en dynamisk hotbild och ett ökande ömsesidigt beroende mellan infrastruktur och de olika sektorerna. Direktivet syftar till att åstadkomma en solid harmoniseringsnivå när det gäller de sektorer och kategorier av verksamhetsutövare som omfattas av tillämpningsområdet. Direktivet inrättar en övergripande ram för att hantera kritiska verksamhetsutövares motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller orsakade av människan, olyckshändelser eller avsiktligt framkallade faror (skäl 1–4).

Riskbedömning av medlemsstaterna

Kommissionen ges i direktivet befogenhet att anta en delegerad akt för att komplettera direktivet med en icke uttömmande förteckning över samhällsviktiga tjänster inom de sektorer och undersektorer som omfattas av direktivet. De behöriga myndigheterna ska använda förteckningen för att göra en riskbedömning senast den 17 januari 2026 (medlemsstaternas riskbedömning). Medlemsstaternas riskbedömningar ska innehålla en redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot. Inom tre månader från att riskbedömningen har gjorts ska medlemsstaten förse kommissionen med relevant information om de typer av risker som har identifierats och resultatet av riskbedömningen per sektor och undersektor.

CER-direktivet handlar inte direkt om cybersäkerhet, men det definierar tydligt dess förhållande till NIS2-direktivet. Enligt skäl 9 och artikel 1.2 i CER-direktivet ska detta direktiv inte tillämpas på frågor som omfattas av NIS2-direktivet. Mot bakgrund av förhållandet mellan kritiska entiteters fysiska säkerhet och cybersäkerhet ska medlemsstaterna dock säkerställa att de två direktiven genomförs på ett samordnat sätt. Enligt artikel 9.6 i CER-direktivet måste det dessutom finnas en viss samordning mellan den nationella behöriga CER-myndigheten och den nationella behöriga myndigheten för NIS2-direktivet för att säkerställa att luckor inte finns.

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Betydelse/konsekvenser för energisektorn

Bilagan innehåller 11 sektorer däribland energi, med delsektorerna elektricitet, fjärrvärme eller fjärrkyla, olja, gas och vätgas. Undantagna är laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt inte omfattas av CER-direktivet.

En skillnad mellan CER och NIS-2 direktivet är att enligt CER-direktivet ska kritiska entiteter identifieras och pekas ut av medlemsstaterna. Energimyndigheten föreslås bli tillsynsmyndighet för CER-lagstiftningen för energisektorn.

4. Nätkod för cybersäkerhet vid gränsöverskridande elflöden (NC CS)

Kort om förordningen

Nätkod om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (NC CS) syftar till att fastställa en europeisk standard för cybersäkerhet för gränsöverskridande elflöden. Här inbegrips regler om gemensam riskbedömnings- och riskhanteringsprocess, säkerhetskrav, övervakning, rapportering och krishantering. Nätföreskrifter är rättsligt bindande i alla medlemsstater. Förordningen kompletterar EU:s förordning (EU) 2019/943 genom att fastställa nätföreskrifter för sektorsspecifika regler som rör cybersäkerhetsaspekter av gränsöverskridande elflöden. Trädde i kraft den 13 juni 2024.

Förordningen syftar till att harmonisera regler och förfaranden mellan medlemsländerna för att förbättra samarbetet och hantera cyberhot på ett effektivt sätt. Den omfattar också gränsöverskridande elflöden i sammankopplade digitaliserade kraftsystem. Förordningen betonar vikten av att hantera cybersäkerhetsrisker för att upprätthålla en säker elförsörjning och säkerställa höga cybersäkerhetsnivåer inom energisektorn.

Digitalisering och cybersäkerhet är avgörande för att tillhandahålla samhällsviktiga tjänster och är av strategisk betydelse för kritisk energiinfrastruktur.

Entiteter som identifieras ha stor påverkan och kritisk påverkan behöver inrätta ett riskhanteringssystem för cybersäkerhet, om det inte redan finns på plats. Nätföreskrifterna kräver att entiteter med stor påverkan och kritisk påverkan inrättar ett sådant ledningssystem för informationssäkerhet för att hantera cybersäkerhetsriskerna och genomförandet av cybersäkerhetskontroller, beroende på typen av enheter. De allmänna kraven på ett ledningssystem, är huvudsakligen härledda från ISO/IEC 27001-standarden, men det krävs inte att enheter följer specifikt denna standard eller certifieras mot standarden.

Den omfattar också flöden för informationsutbyte om cybersäkerhet för att säkerställa information i rätt tid, främja snabba och samordnade reaktioner från berörda parter och tillhandahålla regler för incidenthantering och krishantering. Dessutom omfattar nätföreskrifterna en ram för cybersäkerhetsövningar för att förbättra alla operatörers beredskap, regler för skydd av informationsutbyte och en ram för övervakning, rik märkning och rapportering.

Överträdelser kan i nuläget inte resultera i ekonomiska sanktioner.

Betydelse för elenergisektorn

NC CS har direkta konsekvenser för elsektorn, och i synnerhet för den typ av enheter som anges nedan:

- leverantörer
- systemansvariga för distributionssystem
- systemansvariga för överföringssystem
- producenter
- aggregatorer
- lagringsoperatörer
- efterfrågeflexibilitet aktörer
- elhandlare elhandelsföretag

Vilka entiteter som omfattas identifieras och pekas ut av medlemsstaterna. Energimyndigheten är av regering utsedd till Sveriges behöriga myndighet för NC CS.

5. AI-rättsakt

Kort om förordningen

Den 12 juli 2024 offentliggjordes Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (AI) och om ändring av vissa unionslagstiftningsakter. Förordningen ska tillämpas fullt ut två år efter att den trätt i kraft vilket troligtvis sker under våren 2026 i Sverige.

I förslaget till förordning fastställs följande:

- Bred tillämplighet: Påverkar leverantörer, spridare, importörer, distributörer och tillverkare av AI-system inom EU, inbegripet dem vars AI-utdata används i EU, oavsett var de befinner sig.
- Stränga efterlevnadskrav: Upprättar rigorösa efterlevnadskrav, med undantag för militär-, försvars- och forskningsändamål.

- Krav på verkställighet: Förtydligar tillämpningsområdet, kraven och konsekvenserna av AI.
- Praktiska strategier för efterlevnad: Betonar vikten av AI-styrningsprogram och proaktivt engagemang för att uppnå efterlevnad.

Vidare innehåller den särskilda regler för AI-system som skapar en hög risk för fysiska personers hälsa och säkerhet eller grundläggande rättigheter. De omfattar regler om riskhanteringssystem, data och dataförvaltning, teknisk dokumentation, registerföring, transparens och tillhandahållande av information till användare, mänsklig tillsyn och noggrannhet, robusthet och cybersäkerhet. Utöver detta fastställs i förordningen regler om skyldigheter för leverantörer och användare av AI-system med hög risk och andra parter. Enheter inom energisektorn som använder eller överväger att använda AI-system som betraktas som AI-system med hög risk måste erkänna de regler som fastställs i rättsakten om artificiell intelligens.

Överträdelser av AI-förordningen kan resultera i betydande ekonomiska sanktioner. Sanktionsavgifterna kan uppgå till tre procent (3 %) av ett företags globala årsomsättning. För överträdelser av förbudet mot användning av AI-system inom riskgrupp 1 kan sanktionsavgifter uppgå till motsvarande sju procent (7 %).

Betydelse för energisektorn

AI-förordningen får ett brett tillämpningsområde. Producenter, importörer, återförsäljare och användare av AI-system omfattas alla, i varierande grad av AI-förordningens bestämmelser, inklusive dess ansvarsbestämmelser. AI-system med hög risk omfattas som AI-system som är avsedda att användas som säkerhetskomponenter vid försörjning av vatten, gas, värme och el.

Det finns ännu inget besked om vilken svensk myndighet som ska få det övergripande ansvaret. Dock finns förväntningar på att Integritetsmyndigheten (IMY) förväntas bli ansvarig myndighet för AI-förordningen.

6. Cybersäkerhetsakten

Kort om den kommande lagstiftningen

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) är till alla delar bindande och direkt tillämplig i alla medlemsstater. I cybersäkerhetsakten fastställs mål, uppgifter och organisatoriska frågor som rör Enisa och en ram för inrättandet av europeiska ordningar för cybersäkerhetscertifiering.

Utöver reglerna om Enisa inrättas genom cybersäkerhetsakten en europeisk ram för cybersäkerhetscertifiering som fastställer de viktigaste övergripande kraven för europeiska ordningar för cybersäkerhetscertifiering. Cybersäkerhetsakten gör det också möjligt att erkänna och använda europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse för IKT-produkter, IKT-tjänster eller IKT-processer i alla medlemsstater. IKT står för Informations- och kommunikationstjänster. Enligt skälet till förordningen är assuransnivån i ett europeiskt certifieringssystem en grund för förtroende för att en IKT-produkt, IKT-tjänst eller IKT-process uppfyller säkerhetskraven i en specifik europeisk ordning för cybersäkerhetscertifiering.

Förslaget går ut på att ändra tillämpningsområdet för den europeiska ramen för cybersäkerhetscertifiering i cybersäkerhetsakten så att den omfattar "förvaltade säkerhetstjänster". Den föreslagna ändringen ska göra det möjligt att i framtiden anta europeiska certifieringssystem för "hanterade säkerhetstjänster" som omfattar områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster. Certifiering är avgörande för att säkerställa en hög kvalitetsnivå och tillförlitlighet hos dessa mycket kritiska och känsliga cybersäkerhetstjänster som hjälper företag och organisationer att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Enligt förslaget ska leverantörer av hanterade säkerhetstjänster anses vara väsentliga eller viktiga entiteter som tillhör en sektor med enligt NIS2-direktivet.

Betydelse för energisektorn indirekt

Syftet med cybersäkerhetscertifieringen är att öka förtroendet för och säkerheten för IKT-produkter, IKT-tjänster och IKT-processer. Enligt förordningen är styrsystem för industriell automation och smarta nät bara några exempel där certifiering redan används i stor utsträckning eller sannolikt används inom en snar framtid.

Försvarets Materielverk (FMV) är nationell tillsynsmyndighet för cybersäkerhetscertifiering.

7. Rättsakt om cyberresiliens (CRA)

Kort om den kommande lagstiftningen

Förslag till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020. Förordningen är fortfarande ett utkast, och det har föreslagits att den ska tillämpas från och med 24 månader efter dagen för ikraftträdandet med några få undantag.

Enligt förordningens skäl föreslås rättsakten om cyberresiliens eftersom EU:s nuvarande rättsliga ram inte tar upp cybersäkerheten för icke-inbyggd programvara, även om cybersäkerhetsattacker i allt högre grad riktar sig mot sårbarheter i dessa produkter, vilket orsakar betydande samhälleliga och ekonomiska kostnader.

Med hänvisning till den europeiska ordningen för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 förutsätts produkter med digitala delar som har certifierats överensstämma med de väsentliga kraven i rättsakten om cyberresiliens. Det har dock sagts att den befintliga unionslagstiftningen om cybersäkerhet, inbegripet [direktiv (NIS2)] och Europaparlamentets och rådets förordning (EU) 2019/881 15, inte direkt omfattar obligatoriska krav på säkerhet för produkter med digitala delar.

I förslaget till förordning fastställs skyldigheter för tillverkare, importörer och distributörer. Enligt förslaget till förordning ska tillverkarna, när de släpper ut en produkt med digitala delar på marknaden, säkerställa att den har utformats, utvecklats och tillverkats i enlighet med de väsentliga kraven i avsnitt 1 i bilaga I. Tillverkaren är också skyldig att underrätta Enisa om alla aktivt utnyttjade sårbarheter i produkten med digitala element. Enligt den föreslagna förordningen måste tillverkaren utföra en bedömning av produktens överensstämmelse med digitala element.

Betydelse/konsekvenser för energisektorn

Syftet är att säkerställa utvecklingen av säkra produkter med digitala element genom att säkerställa att hård- och mjukvaruprodukter släpps ut på marknaden med färre sårbarheter och att tillverkarna tar säkerheten på allvar under en produkts hela livscykel.

Den föreslagna förordningen syftar också till att skapa förutsättningar som gör det möjligt för användare att ta hänsyn till cybersäkerhet när de väljer och använder produkter med digitala element.

8. Förslag till förordning om EU:s rättsakt om cybersolidaritet (CSA)

Kort om den kommande lagstiftningen

Förslag till Europaparlamentets och Rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter. Förordningen är fortfarande ett utkast och blir i alla delar bindande och direkt tillämplig i alla medlemsstater efter dagen för ikraftträdandet. Förordningen syftar till att stärka solidariteten på unionsnivå för att bättre upptäcka, förbereda sig för och reagera på hot och incidenter mot cybersäkerheten. Detta mål uppnås genom:

- En europeisk cybersköld, utplacering av en alleuropeisk infrastruktur för att bygga upp och förbättra gemensam kapacitet för upptäckt av och medvetenhet om cyberhot.
- En mekanism för cyberkriser för att stärka beredskapen genom att testa entiteter inom mycket kritiska sektorer, som energi, för potentiella sårbarheter och hjälpa medlemsstaterna att förbereda sig för, reagera på och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter. Stöd till incidenthantering ska också göras tillgängligt för unionens institutioner, organ och byråer.
- En europeisk mekanism för granskning av cyberincidenter. För att granska och bedöma specifika betydande eller storskaliga incidenter.

Enisa är ett expertcentrum för cybersäkerhet på EU-nivå. Enisa bistår idag som EU unionens organ och medlemsstaterna vid utarbetandet och genomförandet av unionens politik på cybersäkerhetsområdet, stöder kapacitetsuppbyggnad och beredskap i hela unionen, främjar samarbete, bidrar till att öka cybersäkerhetskapaciteten på unionsnivå, främjar användningen av europeisk cybersäkerhetscertifiering och en hög nivå av medvetenhet om cybersäkerhet. Enisa tillhandahåller sekretariatet för CSIRT-nätverket och stöder medlemsstaterna när det gäller operativt samarbete inom CSIRT-nätverket.

Betydelse för energisektorn

Cyberkrismekanismen ska stödja beredskapsåtgärder, inbegripet samordnade beredskapstester eller så kallade stresstester av entiteter som är verksamma inom mycket kritiska sektorer i hela unionen. Kommissionen ska identifiera de berörda sektorerna, eller delsektorerna, bland de sektorer som är mycket kritiska och som förtecknas i bilagan i NIS2-direktivet, från vilket enheter kan bli föremål för samordnade beredskapstester. Energisektorn är en av dessa sektorer.

Enisa anordnar även regelbundet cybersäkerhetsövningar på unionsnivå som företag kan delta i och utarbeta tekniska lägesrapporter om cybersäkerhet.

9. Säkerhetskyddslagstiftning

Kort om lagstiftningen

För att stärka säkerhetsskyddet infördes den 1 april 2019 den nya säkerhetsskyddslagen (2018:585). I säkerhetsskyddslagen finns bland annat bestämmelser om verksamhetsutövarens ansvar, säkerhetsskyddsanalys och säkerhetsskyddsåtgärder, samt

om tillsynsmyndigheternas ansvar. Varje verksamhet ska själva utreda och bedöma om och i vilken omfattning verksamheten omfattas av säkerhetsskyddslagen och kraven på säkerhetsskyddsåtgärder. Bedömningen görs i en säkerhetsskyddsanalys. Exempel på främmande makts metoder för underrättelseinhämtning är öppna källor, signalspaning, cyberspionage mot skyddsvärda verksamheter i syfte att stjäla information eller att förbereda sabotage, flyg- och satellitspaning, traditionell personbaserad inhämtning.

För att stärka skyddet för Sveriges säkerhet ytterligare finns sedan 1 januari 2021 flera ändringar i säkerhetsskyddslagen. Den 1 december 2021 kom även en ny säkerhetsskyddsförordning (2021:955) för att ytterligare stärka verksamheter. Förordningen innehåller kompletterande bestämmelser till säkerhetsskyddslagen. I förordningen behandlas bland annat säkerhetsskyddschefens roll, informationssäkerhet och säkerhetsprövning.

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) innehåller kompletterande bestämmelser till säkerhetsskyddslagen och säkerhetsskyddsförordningen, och gäller från 1 mars 2022. Till kraven på säkerhetsskyddsåtgärder finns flertalet vägledningar från Säkerhetspolisen som bland annat omfattar säkerhetsskyddanalys, informationssäkerhet, fysisk skydd och personalsäkerhet med flera.

Sektorspecifika tillsynsmyndigheter för energisektorn

Svenska kraftnät och Energimyndigheten får utfärda föreskrifter om säkerhetsskydd för enskilda verksamhetsutövare inom el- och energiförsörjning. För elförsörjningen är Svenska kraftnät (Svk) tillsynsmyndighet. För övriga energislag är Energimyndigheten tillsynsmyndighet för säkerhetsskyddet från den 1 december 2021. Respektive tillsynsmyndighet tar fram föreskrifter och särskilda blanketter för anmälningar som kompletterar Säkerhetspolisens vägledningar. Se respektive tillsynsmyndighets hemsida.

Försvarsmaktens föreskrifter om signalskyddstjänsten gäller alla verksamhetsutövare som ska använda kryptografiska funktioner för att kommunicera säkerhetsskyddsklassificerade uppgifter till ett informationssystem utanför verksamhetsutövarens kontroll.

Offentlighets- och sekretesslagens (OSL) regler om sekretess måste vara tillämpbara för att uppgifter ska vara säkerhetsskyddsklassificerade. Företagen ska därför göra en prövning om en uppgift skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig även för dem. Enskilda verksamhetsutövare behöver hänvisa till den bestämmelse i OSL som sekretessen avseende en viss handling eller uppgift hänförs till, för att underlätta en korrekt hantering och transparens när det gäller säkerhetsklassificerade uppgifter och handlingar.

En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst 50 000 000 kronor enligt lag (2021:952). När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till de omständigheter som anges.

Betydelse för energisektorn

Säkerhetsläget är allvarligt i Sverige. Omvärldsförändringar och globalisering har flyttat gränserna för den nationella säkerheten. Det har lett till ett behov av att säkerhetsskyddslagstiftningen nu omfattar fler samhällssektorer, som vissa delar av energisektorn som bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Innehavare av verksamheter har ett stort ansvar att svara mot samhällets krav på säkerhetsskydd som bland annat innebär att skyddsvärda uppgifter inte kommer i orätta händer, vilket om så sker, kan leda till skada för Sverige. Det är därför viktigt att alla ägare av verksamhet inom energisektorn arbetar systematiskt med att klassificera sina informationstillgångar och därefter vidtar nödvändiga åtgärder för att skydda dessa tillgångar så att endast de som har behov och är behöriga har tillgång till dem.

Om ni har signalskyddsutrustning eller säkerhetsskyddsklassificerade uppgifter som inte omfattas av säkerhetsskyddsavtal så är det ändock att betrakta inom ramen för er säkerhetskänsliga verksamhet. För handledning, se ”Att säkerhetsskyddsklassificera skyddsvärda uppgifter” från Energiföretagen Sverige.

10. Riskberedskap inom elsektorn

Kort om den gällande lagstiftningen

I Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG, fastställs regler för samarbete mellan medlemsstaterna i syfte att förebygga, förbereda sig inför och hantera el kriser i en anda av solidaritet och öppenhet och med fullt beaktande av kraven på en konkurrensutsatt inre marknad för el.

I förordningen fastställs regler för riskbedömning med avseende på en trygg elförsörjning, inbegripen identifiering av de mest relevanta regionala och nationella elkrisscenarierna och upprättande av riskberedskapsplaner och åtgärder på grundval av dessa planer. I förordningen fastställs också regler för hantering av elkriser, inklusive regler för tidig varning, tillkännagivande av en elkris, samarbete och bistånd mellan medlemsstaterna samt efterhandsutvärdering.

Enligt skäl 7 i förordningen kompletterar det NIS-direktivet (EU) 2016/1148 genom att säkerställa att cyberincidenter identifieras korrekt som en risk och att de åtgärder som vidtas för att hantera dem återspeglas korrekt i riskberedskapsplanerna. Enligt skäl 2 sträcker sig konsekvenserna av elkriser ofta över nationsgränserna. Även om sådana kriser börjar lokalt kan deras effekter snabbt sprida sig över gränserna. Vissa extrema omständigheter, som köldknäppar, värmeböljor eller cyberattacker, kan påverka hela regioner samtidigt.

Betydelse/konsekvenser för energisektorn

Förordningen säkerställer att medlemsstaterna och andra aktörer som operatörer, systemansvariga för överföringssystem (TSO:er) och systemansvariga för distributionssystem (DSO:er) kan samarbeta effektivt över gränserna. I direktivet fastställs också en gemensam ram med regler för hur elkriser ska förebyggas, förberedas och hanteras, vilket ger större insyn i förberedelsefasen och under en elkris och säkerställer att åtgärder vidtas på ett samordnat och effektivt sätt. Som redan har nämnts ser förordningen också till att cybersäkerhetsrisker (nät- och informationssäkerhet) ingår i riskberedskapsplanerna. I Sverige är Energimyndigheten utpekad krisberedskapsmyndighet för energisektorn.

11. Elberedskapslagstiftning

Kort om lagstiftningen

Elberedskapen omfattas bland annat av elberedskapslag (1997:288), förordning (1997:294) om elberedskap samt affärsverket svenska kraftnäts föreskrifter om elberedskap (SvKFS 2023:1).

Syftet med beredskap är att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället, under fredstida kriser och i höjd beredskap. Att upprätta beredskapsplaner är en beredskapsåtgärd. Andra åtgärder är robusthöjande åtgärder som sambandskommunikation via Rakel, reparationsberedskap och ö-driftförmågor.

Betydelse för energisektorn

Elberedskapslagen gäller för de aktörer som bedriver produktion av el, handel med el eller sådan överföring av el som sker med stöd av nätkoncession enligt 2 kap. 1 § ellagen (1997:857). Elberedskapslagen innehåller även en skyldighet för elföretag att anmäla vissa förändringar i anläggningar eller i verksamheten som kan påverka elförsörjningens förmågor. Svenska kraftnät är av regeringen utsedd till Sveriges elberedskapsmyndighet.

Energimyndigheten är sektorsansvarig myndighet för hela energiförsörjningen enligt Förordning (2022:524) om statliga myndigheters beredskap.

Fjärrvärme och fjärrkyla saknar i dagsläget legala krav på energiberedskap.

12. Externa dokument

Nedan ges en sammanställning över länkar till relevanta externa dokument, såväl lagstiftningar som vägledningar.

- EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/ 1148 - av den 6 juli 2016 - om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela union (NIS-direktivet)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2024:4)
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)
- Energimyndigheten föreskrift STEMFS 2021: 3.pdf
- Vägledning inom informationssäkerhet för dig som arbetar utifrån NIS-direktivet inom energisektorn (energimyndigheten.se)
- EUROPAPARALMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 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 upphävning av direktiv (EU) 2016/1148 (NIS 2-direktivet)
- EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet)
- KOMISSIONENS 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 (NC CS)
- Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (AI-akten)
- EUROPAPARALAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/ av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten CRA)
- EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU 2019/1020 COM (2022) 454
- Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om åtgärder för att stärka solidaritet och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter COM (2023) 209 final (CSA)

- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordning (SFS 2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)
- Affärsverket svenska kraftnäts föreskrift om säkerhetsskydd (SvKFS 2022:1
- Statens energimyndighets föreskrifter om säkerhetsskydd (STEMFS 2023:2)
- Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2021:1)
- Att säkerhetsskyddsklassificera skyddsvärda uppgifter, en handledning från Energiföretagen Sverige
- Offentlighets- och sekretesslag (2009:400)
- EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG
- Nationell riskberedskapsplan för Sveriges elförsörjning i enlighet med Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG
- Elberedskapslag (1997:288)
- Förordning (1997:294) om elberedskap
- Affärsverket svenska kraftnäts föreskrifter om elberedskap (SvKFS 2023:1).
- Förordning (2022:524) om statliga myndigheters beredskap