Europeiska unionens
officiella tidning

SV
L-serien

2024/1366

24.5.2024

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

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el ([1]), särskilt artikel 59.2 e, och

av följande skäl:

(1) Hanteringen av cybersäkerhetsrisker är mycket viktig för att upprätthålla en trygg elförsörjning. och för att säkerställa en hög nivå av cybersäkerhet i elsektorn.

(2) Digitalisering och cybersäkerhet är avgörande för tillhandahållandet av samhällsviktiga tjänster och därmed av strategisk betydelse för kritisk energiinfrastruktur.

(3) Europaparlamentets och rådets direktiv (EU) 2022/2555 ([2]) omfattar åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen. Europaparlamentets och rådets förordning (EU) 2019/941 ([3]) kompletterar direktiv (EU) 2022/2555 genom att säkerställa att cybersäkerhetsincidenter i elsektorn på rätt sätt identifieras som en risk och de åtgärder som vidtas för att hantera dem återspeglas korrekt i riskberedskapsplanerna. Förordning (EU) 2019/943 kompletterar direktiv (EU) 2022/2555 och förordning (EU) 2019/941 genom att fastställa särskilda regler för elsektorn på unionsnivå. Den här delegerade förordningen kompletterar också bestämmelserna om elsektorn i direktiv (EU) 2022/2555 i de fall då gränsöverskridande elflöden berörs.

(4) I ett sammanhang med sammanlänkade digitaliserade elsystem kan förebyggandet och hanteringen av elkriser i samband med cyberangrepp inte anses som enbart en nationell uppgift. Alla möjligheter till effektivare och billigare åtgärder genom regionalt samarbete och unionssamarbete bör utvecklas så långt det går. Därför behövs en gemensam ram av regler och mer samordnade förfaranden för att säkerställa att medlemsstaterna och andra aktörer klarar att samarbeta effektivt över gränserna, i en anda av mer öppenhet, förtroende och solidaritet mellan medlemsstaterna och behöriga myndigheter med ansvar för el och cybersäkerhet.

(5) Den hantering av cybersäkerhetsrisker som omfattas av denna förordning kräver en strukturerad process som bland annat omfattar identifiering av risker för gränsöverskridande elflöden till följd av cyberangrepp, berörda operativa processer och områden samt motsvarande cybersäkerhetskontroller och verifieringsmekanismer. Tidsramen för hela processen sträcker sig över flera år, men varje enskilt steg bör bidra till en hög gemensam nivå av cybersäkerhet i sektorn och en reducering av cybersäkerhetsriskerna. Alla deltagare i processen bör göra sitt yttersta för att utveckla och enas om metoderna snarast möjligt och utan onödigt dröjsmål och under alla omständigheter inom de tidsfrister som anges i förordningen.

([1]) EGT L 158, 14.6.2019, s. 54.

([2]) Europaparlamentets 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 upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

([3]) Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG (EUT L 158, 14.6.2019, s. 1).

(6) Bedömningarna av cybersäkerhetsrisker på unions-, medlemsstats- och entitetsnivå enligt denna förordning får begränsas till sådana som följer på cyberangrepp enligt definitionen i Europaparlamentets och rådets förordning (EU) 2022/2554 ([4]), vilket innebär att exempelvis fysiska angrepp, naturkatastrofer och avbrott på grund av förlust av anläggningar eller mänskliga resurser inte omfattas. Unionstäckande och regionala risker i samband med fysiska angrepp eller naturkatastrofer på elområdet omfattas redan av annan befintlig unionslagstiftning, såsom förordning (EU) 2019/941 (artikel 5) eller kommissionens förordning (EU) 2017/1485 ([5]) om fastställande av riktlinjer för driften av elöverföringssystem. På samma sätt syftar Europaparlamentets och rådets direktiv (EU) 2022/2557 ([6]) om kritiska entiteters motståndskraft till att stärka den fysiska resiliensen hos kritiska entiteter, och det täcker alla relevanta naturrisker och risker orsakade av människan vilka kan påverka tillhandahållandet av samhällsviktiga tjänster, t.ex. olyckor, naturkatastrofer, hot mot folkhälsan såsom pandemier samt hybridhot eller andra antagonistiska hot, inbegripet terroristbrott, kriminell infiltration och sabotage.

(7) Begreppet ”entiteter med kritisk eller stor påverkan” i denna förordning är grundläggande för att fastställa vilka entiteter som bör vara föremål för de skyldigheter som beskrivs i denna förordning. Det riskbaserade tillvägagångssätt som beskrivs i de olika bestämmelserna syftar till att identifiera de processer, tillgångar och entiteter som påverkar de gränsöverskridande elflödena. Beroende på omfattningen av den påverkan på gränsöverskridande elflöden som eventuella cyberangrepp har kan de anses ha ”stor påverkan” eller ”kritisk påverkan”. I artikel 3 i direktiv (EU) 2022/2555 fastställs begreppen ”väsentliga” och ”viktiga” entiteter och kriterierna för identifiering av entiteter i dessa kategorier. Många av dem kommer att anses och identifieras som ”väsentliga” i den mening som avses i artikel 3 i direktiv (EU) 2022/2555 och samtidigt som entiteter med kritisk eller stor påverkan i enlighet med artikel 24 i denna förordning, men de kriterier som fastställs i denna förordning avser endast deras roll och påverkan när det gäller elprocesser som påverkar gränsöverskridande flöden, utan hänsyn till de kriterier som fastställs i artikel 3 i direktiv (EU) 2022/2555.

(8) De entiteter som omfattas av denna förordnings tillämpningsområde och som anses ha stor eller kritisk påverkan enligt artikel 24 i förordningen och omfattas av dess skyldigheter, är i första hand sådana entiteter som har en direkt påverkan på de gränsöverskridande elflödena i EU.

(9) Denna förordning utnyttjar befintliga mekanismer, som redan inrättats genom annan lagstiftning, för att säkerställa effektivitet och motverka dubbelarbete när det gäller att uppnå målen.

(10) Vid tillämpningen av denna förordning bör medlemsstaterna, berörda myndigheter och systemansvariga beakta de europeiska standarder och tekniska specifikationer som antagits av de europeiska standardiseringsorganisationerna och agera i enlighet med den unionslagstiftning som rör utsläppandet på marknaden eller ibruktagandet av produkter som omfattas av den unionslagstiftningen.

([4]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

([5]) Kommissionens förordning (EU) 2017/1485 av den 2 augusti 2017 om fastställande av riktlinjer för driften av elöverföringssystem (EUT L 220, 25.8.2017, s. 1).

([6]) 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 (EUT L 333, 27.12.2022, s. 164).

(11) För att reducera cybersäkerhetsriskerna är det nödvändigt att fastställa ett detaljerat regelverk för åtgärder som vidtas av och samordnas mellan berörda intressenter vars verksamhet avser cybersäkerhetsaspekter av gränsöverskridande elflöden, med sikte på att säkerställa systemsäkerhet. Dessa organisatoriska och tekniska regler bör säkerställa att de flesta elincidenter där cybersäkerhet är grundorsaken hanteras effektivt på operativ nivå. Det är nödvändigt att fastställa vad dessa berörda intressenter bör göra för att förhindra sådana kriser och vilka åtgärder de kan vidta om det inte längre räcker med enbart systemdriftsreglerna. Därför är det nödvändigt att fastställa en gemensam ram med regler för hur man kan förebygga, förbereda sig för och hantera samtidiga elkriser där cybersäkerhet är en grundorsak. Detta ökar transparensen i den förberedande fasen och under en samtidig elkris och säkerställer att åtgärder vidtas på ett samordnat och effektivt sätt tillsammans med de behöriga cybersäkerhetsmyndigheterna i medlemsstaterna. Medlemsstaterna och berörda entiteter bör vara skyldiga att samarbeta på regional nivå och i tillämpliga fall på bilateral nivå, i en anda av solidaritet. Dessa samarbeten och regler är avsedda att förbättra beredskapen för cybersäkerhetsrisker till en lägre kostnad, vilket också är i linje med målen i direktiv (EU) 2022/2555. Det förefaller också nödvändigt att stärka den inre elmarknaden genom att öka tilliten och förtroendet mellan medlemsstaterna, och i synnerhet att reducera risken för onödiga inskränkningar i gränsöverskridande elflöden, vilket reducerar risken för negativa spridningseffekter i angränsande medlemsstater.

(12) För en trygg elförsörjning krävs ett effektivt samarbete mellan medlemsstater, unionens institutioner, organ, kontor och byråer samt berörda intressenter. Systemansvariga för distributionssystem och systemansvariga för överföringssystem har en viktig roll för att säkerställa ett säkert, tillförlitligt och effektivt elsystem i enlighet med artiklarna 31 och 40 i Europaparlamentets och rådets direktiv (EU) 2019/944 ([7]). De olika tillsynsmyndigheterna och andra berörda behöriga nationella myndigheter har också en viktig roll för att säkerställa och övervaka cybersäkerheten i elförsörjningen, som ett led i sina arbetsuppgifter enligt direktiven (EU) 2019/944 och (EU) 2022/2555. Medlemsstaterna bör utse en befintlig eller ny entitet till sin behöriga nationella myndighet för genomförandet av denna förordning, med målet att säkerställa ett transparent och inkluderande deltagande av alla berörda aktörer, effektiva förberedelser för ett korrekt genomförande av förordningen, samarbete mellan de olika berörda intressenterna och behöriga myndigheterna på el- och cybersäkerhetsområdet, samt att främja förebyggande åtgärder, informationsutbyte och efterhandsutvärdering avseende elkriser där cybersäkerhet är en grundorsak.

(13) I de fall då en entitet med stor eller kritisk påverkan tillhandahåller tjänster i mer än en medlemsstat, eller har sitt säte eller annat verksamhetsställe eller en företrädare i en medlemsstat men sina nätverks- och informationssystem i en eller flera andra medlemsstater, bör dessa medlemsstater uppmuntra sina respektive behöriga myndigheter att göra sitt yttersta för att bistå och samarbeta med varandra vid behov.

(14) Medlemsstaterna bör säkerställa att de behöriga myndigheterna har de befogenheter som är nödvändiga i förhållande till entiteter med stor eller kritisk påverkan, för att främja efterlevnaden av denna förordning. Dessa befogenheter bör göra det möjligt för de behöriga myndigheterna att utföra inspektioner på plats och tillsyn på distans. Detta kan innefatta slumpmässiga kontroller, regelbundna revisioner, riktade säkerhetsrevisioner baserade på riskbedömningar eller riskrelaterad tillgänglig information och säkerhetsskanningar baserade på objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vilket innefattar att begära information som är nödvändig för att bedöma de cybersäkerhetsåtgärder som vidtagits av entiteten. Denna information bör omfatta dokumenterade cybersäkerhetsstrategier, åtkomstdata, dokument eller annan information som de behöver för att utföra sina tillsynsuppgifter, samt bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevisning.

([7]) Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).

(15) För att motverka luckor eller överlappningar mellan riskhanteringsskyldigheter som införs för entiteter med stor påverkan eller kritisk påverkan bör de nationella myndigheterna enligt direktiv (EU) 2022/2555 och de behöriga myndigheterna enligt denna förordning samarbeta när det gäller genomförandet av riskhanteringsåtgärder på cybersäkerhetsområdet och tillsynen över efterlevnaden av dessa åtgärder på nationell nivå. En entitets uppfyllande av de riskhanteringskrav på cybersäkerhetsområdet som fastställs i denna förordning kan av de behöriga myndigheterna enligt direktiv (EU) 2022/2555 anses säkerställa uppfyllandet av motsvarande krav i det direktivet och vice versa.

(16) För ett gemensamt tillvägagångssätt för att förebygga och hantera samtidiga elkriser krävs att medlemsstaterna har en gemensam förståelse av vad som utgör en samtidig elkris och när ett cyberangrepp är en viktig faktor i en sådan. I synnerhet bör samordning mellan medlemsstater och berörda entiteter främjas i syfte att hantera situationer där en potentiell risk för stor elbrist eller för att el inte ska kunna levereras till kunderna föreligger eller är överhängande och detta beror på ett cyberangrepp.

(17) I skäl 1 i Europaparlamentets och rådets förordning (EU) 2019/881 ([8]) erkänns att nätverks- och informationssystem samt elektroniska kommunikationsnät och kommunikationstjänster har en avgörande betydelse för samhället och för att hålla igång ekonomin inom nyckelsektorer som energi, medan skäl 44 förklarar att Europeiska unionens cybersäkerhetsbyrå (Enisa) bör samarbeta med Europeiska unionens byrå för samarbete mellan energitillsynsmyndigheter (Acer).

(18) Genom förordning (EU) 2019/943 tilldelas systemansvariga för överföringssystem och systemansvariga för distributionssystem särskilda ansvarsområden med avseende på cybersäkerhet. Deras europeiska sammanslutningar, Europeiska nätverket av systemansvariga för överföringssystemet för el (Entso för el) och den europeiska enheten för unionens systemansvariga för distributionssystem (EU DSO-enheten) ska, i enlighet med artiklarna 30 respektive 55 i den förordningen, främja cybersäkerhet i samarbete med relevanta myndigheter och reglerade enheter.

(19) En gemensam strategi för att förebygga och hantera samtidiga elkriser där cybersäkerhet är en grundorsak förutsätter också att alla berörda intressenter använder harmoniserade metoder och definitioner för att identifiera risker som rör cybersäkerheten i elförsörjningen. Det måste också vara möjligt att effektivt jämföra hur väl de och deras grannar presterar på detta område. Därför är det nödvändigt att fastställa processerna, rollerna och ansvarsområdena för utveckling och uppdatering av riskhanteringsmetoder, kriterier för klassificering av nätincidenter och cybersäkerhetsåtgärder som är anpassade till de cybersäkerhetsrisker som påverkar gränsöverskridande elflöden.

(20) Medlemsstaterna är, genom den behöriga myndighet som utsetts för denna förordning, ansvariga för att identifiera de entiteter som uppfyller kriterierna för att anses som entiteter med stor eller kritisk påverkan. För att undanröja skillnaderna mellan medlemsstaterna i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringsåtgärderna avseende cybersäkerhet och rapporteringsskyldigheterna för alla relevanta entiteter, bör det fastställas ett antal kriterier som avgör vilka entiteter som omfattas av denna förordnings tillämpningsområde. Denna uppsättning kriterier bör fastställas och regelbundet uppdateras genom den process för utarbetande och antagande av villkor och metoder som fastställs i denna förordning.

(21) Bestämmelserna i denna förordning bör inte påverka tillämpningen av unionslagstiftning om särskilda regler för certifiering av informations- och kommunikationsteknikprodukter (*IKT-produkter*), IKT-tjänster och IKT-processer, och i synnerhet inte tillämpningen av förordning (EU) 2019/881 med avseende på ramverket för inrättandet av europeiska ordningar för cybersäkerhetscertifiering. Inom ramen för denna förordning bör IKT-produkter även omfatta teknisk utrustning och programvara som möjliggör direkt interaktion med det elektrotekniska nätet, i synnerhet industriella kontrollsystem som kan användas för överföring, distribution och produktion av energi och för insamling och överföring av tillhörande information. Bestämmelserna bör säkerställa att de relevanta säkerhetsmålen i artikel 51 i förordning (EU) 2019/881 uppfylls av de IKT-produkter, IKT-tjänster och IKT-processer som ska upphandlas.

([8]) 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) (EUT L 151, 7.6.2019, s. 15).

(22) Senare tids cyberangrepp visar att entiteter allt oftare är måltavlor för angrepp mot leveranskedjor. Sådana angrepp mot leveranskedjor påverkar inte bara de enskilda entiteter som är föremål för dem utan kan även ha kaskadeffekter på större angrepp på entiteter som de är sammankopplade med i elnätet. Därför har bestämmelser lagts till som bör bidra till att reducera de cybersäkerhetsrisker som är förbundna med processer som rör leveranskedjan, i synnerhet upphandling, och som påverkar gränsöverskridande elflöden.

(23) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande avbrott i energiförsörjningen och skada för ekonomin och konsumenterna bör dessa sårbarheter snabbt identifieras och åtgärdas för att reducera riskerna. För att främja ett effektivt genomförande av denna förordning bör berörda entiteter och behöriga myndigheter samarbeta för att öva och testa verksamhet som anses ändamålsenlig för detta syfte, inbegripet utbyte av information om cyberhot, cyberangrepp, sårbarheter, verktyg och metoder, typer av taktik, teknik och förfaranden, beredskap för hantering av cybersäkerhetsrisker och andra övningar. I och med att tekniken ständigt utvecklas och elsektorn genomgår en snabb digitalisering bör genomförandet av de bestämmelser som antas inte hämma innovation eller utgöra ett hinder för att få tillträde till elmarknaden och därefter använda innovativa lösningar som bidrar till att göra elsystemet effektivare och mer hållbart..

(24) Den information som samlas in i syfte att övervaka genomförandet av denna förordning bör begränsas på ett rimligt sätt utifrån principen om behovsenlig behörighet. Intressenterna bör ges uppnåeliga och ändamålsenliga tidsfrister för att lämna in sådan information. Dubbel anmälan bör undvikas.

(25) Cybersäkerhetsskyddet stannar inte vid unionens gränser. För ett säkert system krävs att angränsande tredjeländer deltar. Unionen och dess medlemsstater bör sträva efter att stödja angränsande tredjeländer vars elinfrastruktur är sammankopplad med det europeiska elnätet att tillämpa liknande cybersäkerhetsregler som de som fastställs i denna förordning.

(26) För att snabbt förbättra säkerhetssamordningen och testa framtida bindande villkor och metoder bör Entso för el, EU DSO-enheten och de behöriga myndigheterna börja utarbeta en icke-bindande vägledning så fort denna förordning har trätt i kraft. Vägledningen kommer att fungera som utgångspunkt för utarbetandet av framtida villkor och metoder. Samtidigt bör de behöriga myndigheterna identifiera entiteter som kandidater till entiteter med stor eller kritisk påverkan som på frivillig grund kan börja uppfylla skyldigheterna.

(27) Denna förordning har utarbetats i nära samarbete med Acer, Enisa, Entso för el, EU DSO-enheten och andra intressenter för att verkningsfulla, balanserade och proportionella regler ska kunna antas, baserat på öppenhet och delaktighet.

(28) Förordningen kompletterar och förbättrar de krishanteringsåtgärder som fastställs i EU-ramen för hantering av cyberkriser, enligt kommissionens rekommendation (EU) 2017/1584 ([9]). Ett cyberangrepp kan också orsaka, bidra till eller sammanfalla med en elkris enligt definitionen i artikel 2.9 i förordning (EU) 2019/941 som påverkar de gränsöverskridande elflödena. En sådan elkris skulle kunna leda till en samtidig elkris enligt definitionen i artikel 2.10 i förordning (EU) 2019/941. En sådan incident kan också påverka andra sektorer som är beroende av en trygg elförsörjning. Om incidenten sedan eskalerar till en storskalig cybersäkerhetsincident i den mening som avses i artikel 16 i direktiv (EU) 2022/2555 bör den artikelns bestämmelser om inrättande av det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) tillämpas. För krishantering på unionsnivå bör berörda intressenter stödja sig på EU-arrangemangen för integrerad politisk krishantering (IPCR-arrangemang) enligt rådets genomförandebeslut (EU) 2018/1993 ([10]).

(29) Denna förordning bör inte påverka medlemsstaternas befogenhet att vidta de åtgärder som är nödvändiga för att skydda sin väsentliga säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra utredning, upptäckt och lagföring av brott, i överensstämmelse med unionsrätten. Enligt artikel 346 i EUF-fördraget bör ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.

([9]) Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

([10]) Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering (EUT L 320, 17.12.2018, s. 28).

(30) Även om denna förordning i princip tillämpas på entiteter som bedriver verksamhet inom produktion av el från kärnkraftverk kan en del sådan verksamhet vara kopplad till nationell säkerhet.

(31) Unionens dataskyddslagstiftning och integritetslagstiftning bör tillämpas på all behandling av personuppgifter inom ramen för denna förordning. I synnerhet bör denna förordning inte påverka tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 ([11]), Europaparlamentets och rådets direktiv 2002/58/EG ([12]) eller Europaparlamentets och rådets förordning (EU) 2018/1725 ([13]). Därmed bör den inte påverka exempelvis uppgifterna och befogenheterna för de myndigheter som är behöriga att övervaka efterlevnaden av unionens tillämpliga dataskyddslagstiftning och integritetslagstiftning.

(32) Mot bakgrund av hur viktigt det är med internationellt samarbete om cybersäkerhet bör de behöriga myndigheter som ansvarar för att utföra arbetsuppgifter de tilldelats enligt denna förordning och som utses av medlemsstaterna kunna delta i internationella samarbetsnätverk. Därför bör de behöriga myndigheterna för utförandet av sina arbetsuppgifter kunna utbyta information, inbegripet personuppgifter, med behöriga myndigheter i tredjeländer, under förutsättning att villkoren i unionens dataskyddslagstiftning om överföring av personuppgifter till tredjeländer, bland annat villkoren i artikel 49 i förordning (EU) 2016/679, uppfylls.

(33) Behandling av personuppgifter i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i tillgångar hos entiteter med stor eller kritisk påverkan kan anses vara laglig på grund av att sådan behandling är förenlig med en rättslig förpliktelse som åvilar den personuppgiftsansvarige i enlighet med kraven i artikel 6.1 c och artikel 6.3 i förordning (EU) 2016/679. Behandling av personuppgifter kan även vara nödvändig på grund av berättigade intressen hos entiteter med stor eller kritisk påverkan, samt tillhandahållare av säkerhetsteknik och säkerhetstjänster som agerar på dessa entiteters vägnar, i enlighet med artikel 6.1 f i förordning (EU) 2016/679, bland annat när sådan behandling är nödvändig för arrangemang för informationsutbyte om cybersäkerhet eller frivillig relevant information i enlighet med denna förordning. Åtgärder som rör förebyggande, upptäckt, identifiering, begränsning, analys och hantering av cyberangrepp, åtgärder för att öka medvetenheten om specifika cyberhot, informationsutbyte i samband med avhjälpande av sårbarheter och samordnat meddelande av sårbarhetsinformation, frivilligt informationsutbyte om sådana cyberangrepp samt cyberhot och sårbarheter, angreppsindikatorer, typer av taktik och teknik och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg kan kräva behandling av vissa kategorier av personuppgifter, såsom IP-adresser, webbadresser (URL), domännamn, e-postadresser och, i den mån de avslöjar personuppgifter, tidsstämplar. Personuppgiftsbehandling av behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter kan utgöra en rättslig förpliktelse eller anses vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning i enlighet med artikel 6.1 c eller e och artikel 6.3 i förordning (EU) 2016/679, eller på grund av ett berättigat intresse hos entiteterna med stor eller kritisk påverkan, enligt vad som avses i artikel 6.1 f i den förordningen. Vidare kan nationell rätt innehålla bestämmelser som tillåter att behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter, i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem hos entiteter med stor eller kritisk påverkan, behandlar särskilda kategorier av personuppgifter i enlighet med artikel 9 i förordning (EU) 2016/679, särskilt genom att föreskriva lämpliga och särskilda åtgärder för att skydda fysiska personers grundläggande rättigheter och intressen, däribland tekniska begränsningar för vidareutnyttjande av sådana uppgifter samt användning av moderna säkerhetsåtgärder och integritetsbevarande åtgärder, såsom pseudonymisering, eller kryptering i de fall då anonymisering avsevärt kan påverka det eftersträvade ändamålet.

([11]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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) (EUT L 119, 4.5.2016, s. 1).

([12]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([13]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

(34) Säkerheten för personuppgifter undergrävs ofta till följd av cyberangrepp. I detta sammanhang bör de behöriga myndigheterna samarbeta och utbyta information om alla relevanta frågor med de myndigheter som avses i förordning (EU) 2016/679 och direktiv 2002/58/EG.

(35) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 17 november 2023.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

I den här förordningen fastställs en nätföreskrift med sektorspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden, bland annat regler om gemensamma minimikrav, planering, övervakning, rapportering och krishantering.

Artikel 2

Tillämpningsområde

1. Denna förordning gäller cybersäkerhetsaspekter av gränsöverskridande elflöden i följande entiteters verksamhet, om de identifieras som entiteter med stor eller kritisk påverkan i enlighet med artikel 24:

a) Elföretag enligt definitionen i artikel 2.57 i direktiv (EU) 2019/944.

b) Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i förordning (EU) 2019/943.

c) Organiserade marknadsplatser eller organiserade marknader enligt definitionen i artikel 2.4 i kommissionens genomförandeförordning (EU) nr 1348/2014 ([14]), vilka genomför transaktioner med produkter av relevans för de gränsöverskridande elflödena.

d) Leverantörer av kritiska IKT-tjänster enligt artikel 3.9 i denna förordning.

e) Entso för el inrättat i enlighet med artikel 28 i förordning (EU) 2019/943.

f) EU DSO-enheten inrättad i enlighet med artikel 52 i förordning (EU) 2019/943.

g) Balansansvariga parter enligt definitionen i artikel 2.14 i förordning (EU) 2019/943.

h) Laddningsoperatörer med ansvar för laddningspunkter enligt definitionen i bilaga I till direktiv (EU) 2022/2555.

i) Regionala samordningscentrum inrättade i enlighet med artikel 35 i förordning (EU) 2019/943.

j) Leverantörer av utlokaliserade säkerhetstjänster (MSSP, *Managed Security Service Provider*) enligt definitionen i artikel 6.40 i direktiv (EU) 2022/2555.

k) Varje annan entitet eller tredje part till vilken ansvar har delegerats eller tilldelats i enlighet med denna förordning.

2. Följande myndigheter är ansvariga för att, som en del av sina nuvarande mandat, utföra de uppgifter som de tilldelas i denna förordning:

a) Europeiska unionens byrå för samarbete mellan energitillsynsmyndigheter (Acer), inrättad genom Europaparlamentets och rådets förordning (EU) 2019/942 ([15]).

b) Nationella behöriga myndigheter som ansvarar för att utföra de uppgifter som de tilldelas i enlighet med denna förordning och som utses av medlemsstaterna i enlighet med artikel 4, eller *behörig myndighet*.

c) Nationella tillsynsmyndigheter utsedda av varje medlemsstat i enlighet med artikel 57.1 i direktiv (EU) 2019/944.

([14]) Kommissionens genomförandeförordning (EU) nr 1348/2014 av den 17 december 2014 om rapportering av uppgifter för att genomföra artikel 8.2 och 8.6 i Europaparlamentets och rådets förordning (EU) nr 1227/2011 om integritet och öppenhet på grossistmarknaderna för energi (EUT L 363, 18.12.2014, s. 121).

([15]) Europaparlamentets och rådets förordning (EU) 2019/942 av den 5 juni 2019 om inrättande av Europeiska unionens byrå för samarbete mellan energitillsynsmyndigheter (EUT L 158, 14.6.2019, s. 22).

d) Behöriga myndigheter med ansvar för riskberedskap (RP-NCA, *Risk Preparedness – National Competent Authority*) inrättade i enlighet med artikel 3 i förordning (EU) 2019/941.

e) Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) som utses eller inrättas i enlighet med artikel 10 i direktiv (EU) 2022/2555.

f) Behöriga myndigheter med ansvar för cybersäkerhet (CS-NCA, *Cybersecurity – National Competent Authority*) som utses eller inrättas i enlighet med artikel 8 i direktiv (EU) 2022/2555.

g) Europeiska unionens cybersäkerhetsbyrå (Enisa), inrättad i enlighet med förordning (EU) 2019/881.

h) Varje annan myndighet eller tredje part till vilken ansvar har delegerats eller tilldelats i enlighet med artikel 4.3.

3. Denna förordning ska också tillämpas på alla entiteter som inte är etablerade i unionen men som tillhandahåller tjänster till entiteter i unionen, förutsatt att de har identifierats som entiteter med stor eller kritisk påverkan av de behöriga myndigheterna i enlighet med artikel 24.2.

4. Denna förordning påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, däribland säkerställandet av statens territoriella integritet och upprätthållandet av lag och ordning.

5. Denna förordning påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet i samband med verksamhet som rör produktion av el från kärnkraftverk, inbegripet verksamhet inom kärnenergins värdekedja, i enlighet med fördragen.

6. Entiteter, behöriga myndigheter, gemensamma kontaktpunkter på entitetsnivå och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av denna förordning och i enlighet med förordning (EU) 2016/679, i synnerhet ska sådan behandling baseras på artikel 6 i den förordningen.

Artikel 3

Definitioner

Följande definitioner gäller:

(1) *tillgång*: all information, programvara eller maskinvara i nätverks- och informationssystemen, antingen materiell eller immateriell, som har värde för en enskild person, en organisation eller en regering.

(2) *behörig myndighet för riskberedskap*: den behöriga myndighet som utsetts i enlighet med artikel 3 i förordning (EU) 2019/941.

(3) *enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet)*: en enhet som ansvarar för risk- och incidenthantering i enlighet med artikel 10 i direktiv (EU) 2022/2555.

(4) *tillgång med kritisk påverkan*: en tillgång som är nödvändig för att utföra en process med kritisk påverkan.

(5) *entitet med kritisk påverkan*: en entitet som utför en process med kritisk påverkan och som identifieras av de behöriga myndigheterna i enlighet med artikel 24.

(6) *område med kritisk påverkan*: ett område som definieras av en i artikel 2.1 avsedd entitet, som rymmer alla tillgångar med kritisk påverkan och inom vilket åtkomsten till dessa tillgångar kan kontrolleras, och som definierar tillämpningsområdet för cybersäkerhetskontrollerna på avancerad nivå.

(7) *process med kritisk påverkan*: verksamhetsprocess som utförs av en entitet för vilken indexen för påverkan på cybersäkerheten för el ligger över tröskelvärdet för kritisk påverkan.

(8) *tröskelvärde för kritisk påverkan*: de i artikel 19.3 b avsedda indexvärdena för påverkan på cybersäkerheten för el (ECII), över vilka ett cyberangrepp på en verksamhetsprocess kommer att orsaka allvarliga avbrott i de gränsöverskridande elflödena.

(9) *leverantör av kritiska IKT-tjänster*: en entitet som tillhandahåller en IKT-tjänst eller en IKT-process som är nödvändig för en process med kritisk eller stor påverkan som inverkar på cybersäkerhetsaspekter av gränsöverskridande elflöden och som, om den äventyras, kan orsaka ett cyberangrepp vars påverkan överskrider tröskelvärdet för kritisk eller stor påverkan.

(10) *gränsöverskridande elflöde*: gränsöverskridande flöde enligt definitionen i artikel 2.3 i förordning (EU) 2019/943.

(11) *cyberangrepp*: en incident enligt definitionen i artikel 3.14 i förordning (EU) 2022/2554.

(12) *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

(13) *cybersäkerhetskontroll*: åtgärder eller förfaranden som vidtas i syfte att undvika, upptäcka, motverka eller minimera cybersäkerhetsrisker.

(14) *cybersäkerhetsincident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.

(15) *ledningssystem för cybersäkerhet*: policyer, förfaranden, riktlinjer och tillhörande resurser och verksamheter, som gemensamt förvaltas av en entitet, med målet att skydda dess informationstillgångar från cyberhot genom systematiskt upprättande, implementering, drift, övervakning, översyn, underhåll och förbättring av säkerheten hos en organisations nätverks- och informationssystem.

(16) *driftscentrum för cybersäkerhet*: särskilt centrum där en teknisk grupp bestående av en eller flera experter, med stöd av it-system för cybersäkerhet, utför säkerhetsrelaterade uppgifter (*tjänster utförda av driftscentrumet för cybersäkerhet, CSOC-tjänster*), till exempel hantering av cyberangrepp och fel i säkerhetskonfigurationer, säkerhetsövervakning, logganalys och upptäckt av cyberangrepp.

(17) *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

(18) *hantering av cybersäkerhetsmässig sårbarhet*: identifiering och åtgärdande av sårbarheter.

(19) *entitet*: entitet enligt definitionen i artikel 6.38 i direktiv (EU) 2022/2555.

(20) *förvarning*: den information som krävs för att indikera om en betydande incident misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.

(21) *index för påverkan på cybersäkerheten för el* (*ECII*): index eller klassificeringsskala som rangordnar de möjliga konsekvenserna av cyberangrepp på verksamhetsprocesser som ingår i gränsöverskridande elflöden.

(22) *europeisk ordning för cybersäkerhetscertifiering*: ordning enligt definitionen i artikel 2.9 i förordning (EU) 2019/881.

(23) *entitet med stor påverkan*: en entitet som utför en process med stor påverkan och som identifieras av de behöriga myndigheterna i enlighet med artikel 24.

(24) *process med stor påverkan*: verksamhetsprocess som utförs av en entitet för vilken indexvärdena för påverkan på cybersäkerheten för el ligger över tröskelvärdet för stor påverkan.

(25) *tillgång med stor påverkan*: en tillgång som är nödvändig för att utföra en process med stor påverkan.

(26) *tröskelvärde för stor påverkan*: de i artikel 19.3 b avsedda värdena på indexen för påverkan på cybersäkerheten för el, över vilka ett framgångsrikt cyberangrepp på en process kommer att orsaka allvarliga avbrott i de gränsöverskridande elflödena.

(27) *område med stor påverkan*: ett område som definieras av en i artikel 2.1 förtecknad entitet, som rymmer alla tillgångar med stor påverkan och inom vilket åtkomsten till dessa tillgångar kan kontrolleras, och som definierar tillämpningsområdet för cybersäkerhetskontrollerna på lägsta nivå.

(28) *IKT-produkt*: en IKT-produkt enligt definitionen i artikel 2.12 i förordning (EU) 2019/881.

(29) *IKT-tjänst*: en IKT-tjänst enligt definitionen i artikel 2.13 i förordning (EU) 2019/881.

(30) *IKT-process*: en IKT-process enligt definitionen i artikel 2.14 i förordning (EU) 2019/881.

(31) *äldre system*: ett äldre IKT-system enligt definitionen i artikel 3.3 i förordning (EU) 2022/2554.

(32) *nationell gemensam kontaktpunkt*: den gemensamma kontaktpunkt som utses eller inrättas av varje medlemsstat i enlighet med artikel 8.3 i direktiv (EU) 2022/2555.

(33) *NIS-cyberkrishanteringsmyndigheter*: de myndigheter som utses eller inrättas i enlighet med artikel 9.1 i direktiv (EU) 2022/2555.

(34) *initiativtagare*: entitet som tar initiativ till utbyte, delning eller lagring av information.

(35) *upphandlingsspecifikationer*: de specifikationer som entiteter fastställer för upphandling av nya eller uppdaterade IKT-produkter, IKT-processer eller IKT-tjänster.

(36) *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att företräda en entitet med stor eller kritisk påverkan som inte är etablerad i unionen men som levererar tjänster till entiteter i unionen, och till vilken en behörig myndighet eller en CSIRT-enhet kan vända sig i stället för till entiteten med stor eller kritisk påverkan, i frågor som gäller de skyldigheter som den entiteten har enligt denna förordning.

(37) *risk*: risk enligt definitionen i artikel 6.9 i direktiv (EU) 2022/2555.

(38) *riskpåverkansmatris*: matris som används under riskbedömningen för att fastställa den resulterande påverkansnivån för varje bedömd risk.

(39) *samtidig elkris*: samtidig elkris enligt definitionen i artikel 2.10 i förordning (EU) 2019/941.

(40) *gemensam kontaktpunkt på entitetsnivå*: gemensam kontaktpunkt på entitetsnivå som utses enligt artikel 38.1 c.

(41) *intressent*: varje part som har ett intresse av en organisations eller process fungerande verksamhet och fortlöpande drift, såsom anställda, direktörer, aktieägare, tillsynsmyndigheter, sammanslutningar, leverantörer och kunder.

(42) *standard:* standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 1025/2012 ([16]).

(43) *systemdriftsregion*: systemdriftsregion enligt definitionen i bilaga I till Acers beslut 05–2022 om definition av systemdriftsregioner, vilka fastställts i enlighet med artikel 36 i förordning (EU) 2019/943.

(44) *systemansvariga*: systemansvarig för distributionssystem och systemansvarig för överföringssystem enligt definitionerna i artikel 2.29 och 2.35 i direktiv (EU) 2019/944.

(45) *unionsomfattande process med kritisk påverkan*: varje process inom elsektorn, eventuellt involverande flera entiteter, för vilken den möjliga påverkan från ett cyberangrepp anses kunna vara stor i den unionsomfattande bedömningen av cybersäkerhetsrisker.

(46) *unionsomfattande process med stor påverkan*: varje process inom elsektorn, eventuellt involverande flera entiteter, för vilken den möjliga påverkan från ett cyberangrepp anses kunna vara stor i en unionsomfattande bedömningen av cybersäkerhetsrisker.

(47) *ej avhjälpt, aktivt utnyttjad sårbarhet*: sårbarhet som ännu inte har offentliggjorts och avhjälpts och för vilken det finns tillförlitliga bevis på att en aktör använt skadlig kod mot ett system utan tillstånd från systemets ägare.

(48) *sårbarhet*: sårbarhet enligt definitionen i artikel 6.15 i direktiv (EU) 2022/2555.

Artikel 4

Behörig myndighet

1. Så snart som möjligt och under alla omständigheter senast den 13 december 2024 ska varje medlemsstat utse en nationell statlig myndighet eller tillsynsmyndighet som ska ansvara för att utföra de uppgifter som den tilldelas genom denna förordning (behörig myndighet). Fram till dess att den behöriga myndigheten har fått i uppdrag att utföra uppgifterna enligt denna förordning ska den tillsynsmyndighet som utsetts av varje medlemsstat i enlighet med artikel 57.1 i direktiv (EU) 2019/944 utföra den behöriga myndighetens uppgifter i enlighet med denna förordning.

2. Medlemsstaterna ska utan dröjsmål underrätta kommissionen, Acer, Enisa, samarbetsgruppen för nät- och informationssäkerhet, som inrättats i enlighet med artikel 14 i direktiv (EU) 2022/2555, och gruppen för samordning på elområdet, som inrättats genom artikel 1 i kommissionens beslut av den 15 november 2012 ([17]), och meddela dem namnet på och kontaktuppgifterna för den behöriga myndighet som utsetts i enlighet med punkt 1 i denna artikel och eventuella senare ändringar därav.

([16]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

([17]) Kommissionens beslut av den 15 november 2012 om inrättande av gruppen för samordning på elområdet (2012/C 353/02) (EUT C 353, 17.11.2012, s. 2).

3. Medlemsstaterna får tillåta att deras behöriga myndighet delegerar uppgifter som den tilldelats genom denna förordning till andra nationella myndigheter, med undantag för de uppgifter som anges i artikel 5. Varje behörig myndighet ska övervaka att de myndigheter till vilka den har delegerat uppgifter tillämpar denna förordning. Den behöriga myndigheten ska för de myndigheter till vilka en uppgift har delegerats meddela namn, kontaktuppgifter, tilldelade uppgifter och eventuella senare ändringar därav till kommissionen, Acer, gruppen för samordning på elområdet, Enisa och samarbetsgruppen för nät- och informationssäkerhet.

Artikel 5

Samarbete mellan relevanta myndigheter och organ på nationell nivå

De behöriga myndigheterna ska samordna och säkerställa lämpligt samarbete mellan de behöriga myndigheterna med ansvar för cybersäkerhet, cyberkrishanteringsmyndigheterna, de nationella tillsynsmyndigheterna, de behöriga myndigheterna med ansvar för riskberedskap och CSIRT-enheterna i syfte att fullgöra de relevanta skyldigheter som fastställs i denna förordning. De behöriga myndigheterna ska också samordna med andra organ eller myndigheter enligt vad som fastställs av varje medlemsstat, för att säkerställa effektiva förfaranden och undvika överlappande uppgifter och skyldigheter. De behöriga myndigheterna ska kunna ge respektive nationella tillsynsmyndigheter i uppdrag att begära ett yttrande från Acer i enlighet med artikel 8.3.

Artikel 6

Villkor, metoder eller planer

1. Systemansvariga för överföringssystem ska, i samarbete med EU DSO-enheten, utarbeta förslag till villkor eller metoder i enlighet med punkt 2, eller till planer i enlighet med punkt 3.

2. Följande villkor eller metoder, och eventuella ändringar av dessa, ska vara föremål för alla behöriga myndigheters godkännande:

a) Metoderna för bedömning av cybersäkerhetsrisker i enlighet med artikel 18.1.

b) Den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden i enlighet med artikel 23.

c) Cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i enlighet med artikel 29, jämförelsen av cybersäkerhetskontroller för el med standarder i enlighet med artikel 34, inbegripet cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i leveranskedjan i enlighet med artikel 33.

d) En rekommendation om upphandling på cybersäkerhetsområdet i enlighet med artikel 35.

e) Metoden med en klassificeringsskala för cyberangrepp i enlighet med artikel 37.8.

3. Förslagen till regionala planer för reducering av cybersäkerhetsrisker i enlighet med artikel 22 ska godkännas av alla behöriga myndigheter i den berörda systemdriftsregionen.

4. De förslag till villkor eller metoder som förtecknas i punkt 2 eller till planer som förtecknas i punkt 3 ska innehålla ett förslag till tidsplan för genomförande och en beskrivning av förväntad effekt på målen för denna förordning.

5. EU DSO-enheten får lämna ett motiverat yttrande till de berörda systemansvariga för överföringssystem fram till tre veckor före tidsfristen för att lämna in förslaget till villkor, metoder eller planer till de behöriga myndigheterna. De systemansvariga för överföringssystem som ansvarar för förslaget till villkor, metoder eller planer ska beakta det motiverade yttrandet från EU DSO-enheten innan de lämnar in förslaget för de behöriga myndigheternas godkännande. Om EU DSO-enhetens yttrande inte beaktas, ska de systemansvariga för överföringssystem motivera det.

6. Vid gemensam utveckling av villkor, metoder och planer ska deltagande systemansvariga för överföringssystem ha ett nära samarbete. Systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, regelbundet informera behöriga myndigheter och Acer om framstegen med att utveckla villkoren, metoderna eller planerna.

Artikel 7

Omröstningsregler för systemansvariga för överföringssystem

1. Systemansvariga för överföringssystem som beslutar om förslag till villkor eller metoder ska, om de inte kan nå en överenskommelse, fatta beslut med kvalificerad majoritet. En kvalificerad majoritet för sådana förslag ska beräknas enligt följande:

a) Systemansvariga för överföringssystem som representerar minst 55 % av medlemsstaterna, och

b) systemansvariga för överföringssystem som representerar medlemsstater som omfattar minst 65 % av unionens befolkning.

2. En blockerande minoritet i fråga om beslut om förslag till villkor eller metoder som förtecknas i artikel 6.2 ska omfatta systemansvariga för överföringssystem som representerar minst fyra medlemsstater; i annat fall ska den kvalificerade majoriteten anses vara uppnådd.

3. En systemdriftsregions systemansvariga för överföringssystem som beslutar om förslag till planer som förtecknas i artikel 6.2 ska, om de inte kan nå en överenskommelse och den berörda systemdriftsregionen består av fler än fem medlemsstater, fatta beslut med kvalificerad majoritet. För en kvalificerad majoritet för förslag som förtecknas i artikel 6.2 krävs

a) systemansvariga för överföringssystem som representerar minst 72 % av de berörda medlemsstaterna, och

b) systemansvariga för överföringssystem som representerar medlemsstater som omfattar minst 65 % av det berörda områdets befolkning.

4. En blockerande minoritet i fråga om beslut om förslagen till planerna ska inkludera åtminstone ett minimiantal systemansvariga för överföringssystem som representerar mer än 35 % av befolkningen i de deltagande medlemsstaterna, samt systemansvariga för överföringssystem som representerar ytterligare minst en berörd medlemsstat; i annat fall ska den kvalificerade majoriteten anses vara uppnådd.

5. Då systemansvariga för överföringssystem beslutar om förslag till villkor eller metoder enligt artikel 6.2 ska en röst tillskrivas varje medlemsstat. Om det finns flera systemansvariga för överföringssystem på en medlemsstats territorium, ska medlemsstaten fördela röstvärdet mellan de systemansvariga för överföringssystem.

6. Om de systemansvariga för överföringssystem, i samarbete med EU DSO-enheten, inte kan lämna in ett ursprungligt eller ändrat förslag till villkor, metoder eller planer till de relevanta behöriga myndigheterna inom de tidsfrister som anges i denna förordning, ska de lämna in de relevanta utkasten till villkor, metoder eller planer till de berörda behöriga myndigheterna och Acer. De ska förklara vad som har förhindrat en överenskommelse. De behöriga myndigheterna ska gemensamt vidta lämpliga åtgärder för att anta de nödvändiga villkoren, metoderna eller planerna. Detta kan till exempel göras genom att begära ändringar av utkasten i enlighet med denna punkt, genom att revidera och komplettera de utkasten eller, i de fall då inga utkast har lämnats in, genom att fastställa och godkänna de nödvändiga villkoren, metoderna eller planerna.

Artikel 8

Inlämnande av förslag till de behöriga myndigheterna

1. De systemansvariga för överföringssystem ska lämna in förslagen till villkor, metoder eller planer för godkännande till de relevanta behöriga myndigheterna inom de respektive tidsfrister som anges i artiklarna 18, 23, 29, 33, 34, 35 och 37. De behöriga myndigheterna får gemensamt förlänga dessa tidsfrister under exceptionella omständigheter, särskilt i fall där en tidsfrist inte kan hållas på grund av omständigheter som de systemansvariga för överföringssystem eller EU DSO-enheten inte kan kontrollera.

2. Förslag till villkor, metoder eller planer enligt punkt 1 ska lämnas in för kännedom till Acer samtidigt som de lämnas in till de behöriga myndigheterna.

3. På gemensam begäran av de nationella tillsynsmyndigheterna ska Acer avge ett yttrande om förslaget till villkor, metoder eller planer inom sex månader från mottagandet av förslagen till villkor, metoder eller planer och underrätta de nationella tillsynsmyndigheterna och de behöriga myndigheterna om yttrandet. Nationella tillsynsmyndigheter, behöriga myndigheter med ansvar för cybersäkerhet och alla andra myndigheter som har utsetts till behöriga myndigheter ska samordna med varandra innan de nationella tillsynsmyndigheterna begär ett yttrande från Acer. Acer får inkludera rekommendationer i ett sådant yttrande. Acer ska samråda med Enisa innan Acer avger ett yttrande om de förslag som förtecknas i artikel 6.2.

4. De behöriga myndigheterna ska samråda, samordna och driva ett nära samarbete med varandra för att nå en överenskommelse om de föreslagna villkoren, metoderna eller planerna. Innan de godkänner villkoren, metoderna eller planerna ska de vid behov se över och komplettera förslagen, efter samråd med Entso för el och EU DSO-enheten, för att säkerställa att förslagen är förenliga med denna förordning och bidrar till en hög gemensam cybersäkerhetsnivå i hela unionen.

5. De behöriga myndigheterna ska besluta om villkoren, metoderna eller planerna inom sex månader från det att den relevanta behöriga myndigheten eller, i tillämpliga fall, från det att den sista relevanta behöriga myndigheten tagit emot villkoren, metoderna eller planerna.

6. Om Acer avger ett yttrande ska de relevanta behöriga myndigheterna beakta detta yttrande och fatta sina beslut inom sex månader från mottagandet av Acers yttrande.

7. Om de behöriga myndigheterna gemensamt kräver en ändring av de föreslagna villkoren, metoderna eller planerna för att godkänna dem, ska de systemansvariga för överföringssystem, i samarbete med EU DSO-enheten, utarbeta ett förslag till en sådan ändring av villkoren, metoderna eller planerna. De systemansvariga för överföringssystem ska inom två månader från de behöriga myndigheternas begäran lämna in det ändrade förslaget för godkännande. De behöriga myndigheterna ska besluta om de ändrade villkoren, metoderna eller planerna inom två månader från det att de lämnats in.

8. Om de behöriga myndigheterna inte har kunnat nå någon överenskommelse inom den tid som anges i punkt 5 eller 7, ska de underrätta kommissionen om detta. Kommissionen får vidta lämpliga åtgärder för att göra det möjligt att anta de villkor, metoder eller planer som krävs.

9. De systemansvariga för överföringssystem, med bistånd från Entso för el, och av EU DSO-enheten, ska offentliggöra villkoren, metoderna eller planerna på sina webbplatser efter godkännande av de relevanta behöriga myndigheterna, såvida inte denna information anses vara konfidentiell i enlighet med artikel 47.

10. De behöriga myndigheterna får gemensamt begära förslag till ändringar av de godkända villkoren, metoderna eller planerna från de systemansvariga för överföringssystem och EU DSO-enheten och fastställa en tidsfrist för inlämning av dessa förslag. De systemansvariga för överföringssystem, i samarbete med EU DSO-enheten, får även på eget initiativ lämna förslag till ändringar till de behöriga myndigheterna. Förslagen till ändring av villkoren, metoderna eller planerna ska utarbetas och godkännas i enlighet med förfarandet i denna artikel.

11. Minst vart tredje år efter det första antagandet av respektive villkor, metoder eller planer, ska de systemansvariga för överföringssystem i samarbete med EU DSO-enheten se över de antagna villkorens, metodernas eller planernas effektivitet och utan onödigt dröjsmål rapportera resultaten av översynen till de behöriga myndigheterna och Acer.

Artikel 9

Samråd

1. De systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, samråda med intressenter, däribland Acer, Enisa och varje medlemsstats behöriga myndighet, om utkasten till förslag till de villkor eller metoder som förtecknas i artikel 6.2 och till de planer som avses i artikel 6.3. Samrådet ska vara i minst en månad.

2. Förslag till villkor eller metoder som förtecknas i artikel 6.2 och som lämnas in av de systemansvariga för överföringssystem, i samarbete med EU DSO-enheten, ska offentliggöras och lämnas in för samråd på unionsnivå. Förslag till planer som avses i artikel 6.3 och som lämnas in på regional nivå av de relevanta systemansvariga för överföringssystem, i samarbete med EU DSO-enheten, ska lämnas in för samråd på åtminstone regional nivå.

3. De systemansvariga för överföringssystem, med bistånd från Entso för el, och EU DSO-enheten som ansvarar för förslaget till villkor, metoder eller planer ska vederbörligen beakta de synpunkter från intressenter som framkommit vid de samråd som genomförts i enlighet med punkt 1, innan förslaget lämnas in för formellt godkännande. I samtliga fall ska en välgrundad motivering för eller emot införande av synpunkterna från samrådet tillhandahållas tillsammans med inlämnandet och offentliggöras i god tid före, eller samtidigt med, förslaget till villkor eller metoder.

Artikel 10

Deltagande av intressenter

Acer ska, i nära samarbete med Entso för el och EU DSO-enheten, organisera deltagande av intressenter, inbegripet regelbundna möten med intressenter för att kartlägga problem och föreslå förbättringar i fråga om genomförandet av denna förordning.

Artikel 11

Kostnadstäckning

1. De kostnader som bärs av de systemansvariga för överföringssystem och de systemansvariga för distributionssystem och som härrör från de skyldigheter som fastställs i denna förordning och är föremål för reglerade nättariffer, inbegripet de kostnader som bärs av Entso för el och EU DSO-enheten, ska bedömas av den relevanta nationella tillsynsmyndigheten i varje medlemsstat.

2. Kostnader som bedöms vara rimliga, effektiva och proportionella ska täckas genom nättariffer eller andra lämpliga mekanismer, som fastställs av den relevanta nationella tillsynsmyndigheten.

3. På begäran av de relevanta nationella tillsynsmyndigheterna ska de systemansvariga för överföringssystem och systemansvariga för distributionssystem som avses i punkt 1, inom en rimlig tidsperiod som fastställs av den nationella tillsynsmyndigheten, tillhandahålla den information som krävs för att underlätta bedömningen av de uppkomna kostnaderna.

Artikel 12

Övervakning

1. Acer ska övervaka genomförandet av denna förordning i enlighet med artikel 32.1 i förordning (EU) 2019/943 och artikel 4.2 i förordning (EU) 2019/942. Under övervakningen får Acer samarbeta med Enisa och begära stöd från Entso för el och EU DSO-enheten. Acer ska regelbundet informera gruppen för samordning på elområdet och samarbetsgruppen för nät- och informationssäkerhet om genomförandet av denna förordning.

2. Acer ska minst vart tredje år efter denna förordnings ikraftträdande offentliggöra en rapport för att

a) se över läget i genomförandet av de tillämpliga riskhanteringsåtgärderna avseende cybersäkerhet i fråga om entiteter med stor och kritisk påverkan,

b) fastställa om ytterligare regler om gemensamma krav, planering, övervakning, rapportering och krishantering kan bli nödvändiga för att förebygga risker för elsektorn, och

c) identifiera förbättringsområden för revideringen av denna förordning, eller fastställa områden som inte omfattas och nya prioriteringar som kan uppstå på grund av den tekniska utvecklingen.

3. Senast den 13 juni 2025 får Acer, i samarbete med Enisa och efter samråd med Entso för el och EU DSO-enheten, utfärda en vägledning om den relevanta information som ska meddelas Acer för övervakningsändamål samt om processen och frekvensen för insamlingen, på grundval av de resultatindikatorer som fastställs i enlighet med punkt 5.

4. De behöriga myndigheterna kan få åtkomst till relevant information som innehas av Acer och som samlats in i enlighet med denna artikel.

5. Acer ska i samarbete med Enisa och med stöd av Entso för el och EU DSO-enheten utfärda icke-bindande resultatindikatorer för bedömning av operativ tillförlitlighet avseende cybersäkerhetsaspekter av gränsöverskridande elflöden.

6. De entiteter som förtecknas i artikel 2.1 i denna förordning ska till Acer lämna den information som krävs för att Acer ska kunna utföra de uppgifter som förtecknas i punkt 2.

Artikel 13

Riktmärkning

1. Senast den 13 juni 2025 ska Acer, i samarbete med Enisa, upprätta en icke-bindande vägledning för riktmärkning av cybersäkerhet. Vägledningen ska ge de nationella tillsynsmyndigheterna en förklaring av principerna för de genomförda cybersäkerhetskontrollernas riktmärkning i enlighet med punkt 2 i denna artikel, med beaktande av kostnaderna för att genomföra kontrollerna och effektiviteten hos de processer, produkter, tjänster, system och lösningar som används för att genomföra sådana kontroller. Acer ska beakta befintliga riktmärkningsrapporter vid fastställandet av den icke-bindande vägledningen för riktmärkning av cybersäkerhet. Acer ska lämna den icke-bindande vägledningen för riktmärkning av cybersäkerhet till de nationella tillsynsmyndigheterna för kännedom.

2. Inom 12 månader från upprättandet av vägledningen för riktmärkning i enlighet med punkt 1 ska de nationella tillsynsmyndigheterna genomföra en riktmärkningsanalys för att bedöma om nuvarande investeringar i cybersäkerhet

a) reducerar risker som påverkar gränsöverskridande elflöden,

b) tillhandahåller önskade resultat och effektivitetsvinster när det gäller utvecklingen av elsystemen,

c) är effektiva och integrerade i den övergripande upphandlingen av tillgångar och tjänster.

3. För riktmärkningsanalysen får de nationella tillsynsmyndigheterna ta hänsyn till den icke-bindande vägledning för riktmärkning av cybersäkerhet som fastställts av Acer, och ska de särskilt bedöma

a) de genomsnittliga cybersäkerhetsrelaterade utgifterna för att reducera de risker som påverkar de gränsöverskridande elflödena, i synnerhet när det gäller entiteter med stor och kritisk påverkan,

b) i samarbete med Entso för el och EU DSO-enheten, genomsnittspriserna på de cybersäkerhetstjänster, cybersäkerhetssystem och cybersäkerhetsprodukter som i stor utsträckning bidrar till att förbättra och upprätthålla riskhanteringsåtgärderna avseende cybersäkerhet i de olika systemdriftsregionerna,

c) förekomsten av cybersäkerhetstjänster, cybersäkerhetssystem och cybersäkerhetsprodukter som lämpar sig för genomförandet av denna förordning, samt jämförbarheten hos de därmed förbundna kostnaderna och funktionerna, genom vilket eventuella nödvändiga åtgärder för att främja utgifternas ändamålsenlighet kan identifieras, särskilt i de fall då det kan komma att krävas investeringar i cybersäkerhetsteknik.

4. All information som rör riktmärkningsanalys ska hanteras och behandlas i enlighet med dataklassificeringskraven i denna förordning, cybersäkerhetskontrollerna på lägsta nivå och rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden. Den riktmärkningsanalys som avses i punkterna 2 och 3 får inte offentliggöras.

5. Utan att det påverkar konfidentialitetskraven i artikel 47 och behovet av att skydda säkerheten för entiteter som omfattas av bestämmelserna i denna förordning ska den riktmärkningsanalys som avses i punkterna 2 och 3 i denna artikel delas med alla nationella tillsynsmyndigheter, alla behöriga myndigheter, Acer, Enisa och kommissionen.

Artikel 14

Överenskommelse med systemansvariga för överföringssystem från länder utanför unionen

1. Inom 18 månader från denna förordnings ikraftträdande ska de systemansvariga för överföringssystem i en systemdriftsregion som gränsar till ett tredjeland sträva efter att med det angränsande tredjelandets systemansvariga för överföringssystem nå en överenskommelse som står i överensstämmelse med relevant unionsrätt och som utgör grunden för samarbetet kring cybersäkerhetsskydd och samarbetsarrangemangen avseende cybersäkerhet med dessa systemansvariga för överföringssystem.

2. De systemansvariga för överföringssystem ska informera den behöriga myndigheten om de överenskommelser som nåtts i enlighet med punkt 1.

Artikel 15

Rättsliga företrädare

1. Entiteter som inte är etablerade i unionen, men tillhandahåller tjänster till entiteter i unionen och har anmälts som entiteter med stor eller kritisk påverkan i enlighet med artikel 24.6, ska inom tre månader från anmälan skriftligen utse en företrädare i unionen och informera den anmälande behöriga myndigheten om detta.

2. Till denna företrädare kan varje behörig myndighet eller CSIRT-enhet i unionen vända sig utöver eller i stället för entiteten med stor eller kritisk påverkan i frågor som gäller de skyldigheter som den entiteten har enligt denna förordning Entiteten med stor eller kritisk påverkan ska ge sin rättsliga företrädare nödvändiga befogenheter och tillräckliga resurser för att garantera ett effektivt samarbete i rätt tid med de relevanta behöriga myndigheterna eller CSIRT-enheterna.

3. Företrädaren ska vara etablerad i en av de medlemsstater där entiteten erbjuder sina tjänster. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Entiteter med stor eller kritisk påverkan ska anmäla den rättsliga företrädarens namn, postadress, e-postadress och telefonnummer till den behöriga myndigheten i den medlemsstat där den rättsliga företrädaren har sin hemvist eller är etablerad.

4. Det ska vara möjligt att hålla den utsedda rättsliga företrädaren ansvarig för bristande efterlevnad av skyldigheterna enligt denna förordning, utan att det påverkar de skadeståndskrav och rättsliga åtgärder som kan riktas direkt mot entiteten med stor eller kritisk påverkan.

5. Om det inte finns någon företrädare i unionen som utsetts enligt denna artikel, får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för bristande efterlevnad av skyldigheterna enligt denna förordning.

6. Att en rättslig företrädare inom unionen utses enligt punkt 1 ska inte utgöra en etablering i unionen.

Artikel 16

Samarbete mellan Entso för el och EU-DSO-enheten

1. Entso för el och EU DSO-enheten ska samarbeta vid utförandet av bedömningar av cybersäkerhetsrisker i enlighet med artiklarna 19 och 21, och i synnerhet vid följande uppgifter:

a) Utarbetande av metoderna för bedömning av cybersäkerhetsrisker i enlighet med artikel 18.1.

b) Utarbetande av den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden i enlighet med artikel 23.

c) Utveckling av den gemensamma ramen för cybersäkerhet i elsektorn i enlighet med kapitel III.

d) Utarbetande av en rekommendation om upphandling på cybersäkerhetsområdet i enlighet med artikel 35.

e) Utarbetande av metoden med en klassificeringsskala för cyberangrepp i enlighet med artikel 37.8.

f) Utveckling av det preliminära indexet för påverkan på cybersäkerheten för el (ECII) i enlighet med artikel 48.1 a.

g) Utarbetande av den konsoliderade preliminära förteckningen över entiteter med stor och kritisk påverkan i enlighet med artikel 48.3.

h) Utarbetande av den preliminära förteckningen över unionsomfattande processer med stor och kritisk påverkan i enlighet med artikel 48.4.

i) Utarbetande av den preliminära förteckningen över europeiska och internationella standarder och kontroller i enlighet med artikel 48.6.

j) Utförande av den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.

k) Utförande av regionala bedömningar av cybersäkerhetsrisker i enlighet med artikel 21.

l) Utformning av de regionala planerna för reducering av cybersäkerhetsrisker i enlighet med artikel 22.

m) Utarbetande av en vägledning om europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer i enlighet med artikel 36.

n) Utarbetande av riktlinjer för genomförandet av denna förordning i samråd med Acer och Enisa.

2. Samarbetet mellan Entso för el och EU DSO-enheten kan ske i form av en arbetsgrupp för cybersäkerhetsrisker.

3. Entso för el och EU-DSO-enheten ska regelbundet informera Acer, Enisa, samarbetsgruppen för nät- och informationssäkerhet och gruppen för samordning på elområdet om framstegen med genomförandet av de unionsomfattande och regionala bedömningarna av cybersäkerhetsrisker i enlighet med artiklarna 19 och 21.

Artikel 17

Samarbete mellan Acer och de behöriga myndigheterna

Acer ska i samarbete med varje behörig myndighet

1. övervaka genomförandet av riskhanteringsåtgärderna avseende cybersäkerhet i enlighet med artikel 12.2 a och rapporteringsskyldigheterna enligt artiklarna 27 och 39, och

2. övervaka antagningsprocessen och genomförandet av villkoren, metoderna eller planerna i enlighet med artikel 6.2 och 6.3. Samarbetet mellan Acer, Enisa och varje behörig myndighet kan ske i form av ett §organ för övervakning av cybersäkerhetsrisker.

KAPITEL II

RISKBEDÖMNING OCH IDENTIFIERING AV RELEVANTA CYBERSÄKERHETSRISKER

Artikel 18

Metoder för bedömning av cybersäkerhetsrisker

1. Senast den 13 mars 2025 ska de systemansvariga för överföringssystem, med bistånd från Entso för el, i samarbete med EU DSO-enheten och efter samråd med samarbetsgruppen för nät- och informationssäkerhet, lämna in ett förslag till metoder för bedömning på unionsnivå, regional nivå och medlemsstatsnivå av cybersäkerhetsrisker.

2. Metoderna för bedömning på unionsnivå, regional nivå och medlemsstatsnivå av cybersäkerhetsrisker ska innehålla följande:

a) En förteckning över cyberhot som ska beaktas, inbegripet åtminstone följande hot mot leveranskedjan:

   i) Ett allvarligt och oväntat fall av funktionsfel i leveranskedjan.

   ii) Otillgänglighet för IKT-produkter, IKT-tjänster eller IKT-processer i leveranskedjan.

iii) Cyberangrepp som initieras av aktörer i leveranskedjan.

iv) Läckage av känslig information genom leveranskedjan, inbegripet spårning i leveranskedjan.

v) Införande av svagheter eller bakdörrar i IKT-produkter, IKT-tjänster eller IKT-processer genom aktörer i leveranskedjan.

b) Kriterierna för att utvärdera påverkan av cybersäkerhetsrisker som stor eller kritisk med hjälp av fastställda tröskelvärden för konsekvenser och sannolikhet.

c) En strategi för att analysera de cybersäkerhetsrisker som härrör från äldre system, cyberangreppens kaskadeffekter och realtidskaraktären hos nätdriftssystemen.

d) En strategi för att analysera de cybersäkerhetsrisker som härrör från beroendet av en enda leverantör av IKT-produkter, IKT-tjänster eller IKT-processer.

3. Metoderna för bedömning på unionsnivå, regional nivå och medlemsstatsnivå av cybersäkerhetsrisker ska vid bedömningen av cybersäkerhetsrisker använda samma riskpåverkansmatris. Riskpåverkansmatrisen ska

a) ge ett mått på konsekvenserna av cyberangrepp utifrån kriterierna

i) belastningsförlust,

ii minskad elproduktion,

iii) kapacitetsförlust i den primära frekvensreserven,

iv) kapacitetsförlust för att återuppbygga ett elnät till driftstatus utan att förlita sig på det externa överföringsnätet efter en fullständig eller partiell avstängning (även kallat *dödnätsstart*),

v) förväntad varaktighet hos ett elavbrott som påverkar kunderna, i kombination med avbrottets omfattning räknat i antal kunder, och

vi) andra kvantitativa eller kvalitativa kriterier som rimligen skulle kunna fungera som en indikator på effekterna av ett cyberangrepp på gränsöverskridande elflöden,

b) ge ett mått på sannolikheten för en incident, uttryckt som antalet cyberangrepp per år.

4. I metoderna för bedömning på unionsnivå av cybersäkerhetsrisker ska det beskrivas hur tröskelvärden, i form av ECII-värden, för stor och kritisk påverkan kommer att fastställas. ECII-värdet ska göra det möjligt för entiteterna att, med hjälp av de kriterier som avses i punkt 2 b, uppskatta påverkan av riskerna på deras verksamhetsprocess under de konsekvensbedömningar för verksamheten som de utför i enlighet med artikel 26.4 c i.

5. Entso för el, i samordning med EU DSO-enheten, ska informera gruppen för samordning på elområdet om de förslag till metoder för bedömning av cybersäkerhetsrisker som utarbetas i enlighet med punkt 1.

Artikel 19

Unionsomfattande bedömning av cybersäkerhetsrisker

1. Inom nio månader från godkännandet av metoderna för bedömning av cybersäkerhetsrisker i enlighet med artikel 8 och därefter vart tredje år ska Entso för el, i samarbete med EU DSO-enheten och i samråd med samarbetsgruppen för nät- och informationssäkerhet, utan att det påverkar tillämpningen av artikel 22 i direktiv (EU) 2022/2555, göra en unionsomfattande bedömning av cybersäkerhetsrisker och utarbeta ett utkast till rapport om den unionsomfattande bedömningen av cybersäkerhetsrisker. För detta ändamål ska de att använda de metoder som utvecklats i enlighet med artikel 18 och godkänts i enlighet med artikel 8, för att identifiera, analysera och utvärdera de möjliga konsekvenserna av cyberangrepp som påverkar elsystemets driftsäkerhet och stör de gränsöverskridande elflödena. I den unionsomfattande bedömningen av cybersäkerhetsrisker ska inte cyberangreppens rättsliga, ekonomiska eller anseendemässiga skada beaktas.

2. Den rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker ska innehålla följande:

a) De unionsomfattande processerna med stor påverkan och de unionsomfattande processerna med kritisk påverkan.

b) En riskpåverkansmatris som entiteterna och de behöriga myndigheterna ska använda för att bedöma den cybersäkerhetsrisk som identifieras i bedömningen på medlemsstatsnivå av cybersäkerhetsrisker i enlighet med artikel 20 och i bedömningen på entitetsnivå av cybersäkerhetsrisker i enlighet med artikel 26.2 b.

3. När det gäller de unionsomfattande processerna med stor påverkan och de unionsomfattande processerna med kritisk påverkan ska rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker innehålla följande:

a) En bedömning av de möjliga konsekvenserna av ett cyberangrepp med hjälp av måtten som fastställs i den metod för bedömning av cybersäkerhetsrisker som utvecklats i enlighet med artikel 18 punkterna 2, 3 och 4 och godkänts i enlighet med artikel 8.

b) Det ECII-värde och de tröskelvärden för stor och kritisk påverkan som de behöriga myndigheterna ska använda i enlighet med artikel 24.1 och 24.2 för att identifiera entiteter med stor och kritisk påverkan som deltar i de unionsomfattande processerna med stor påverkan och i de unionsomfattande processerna med kritisk påverkan.

4. Entso för el ska, i samarbete med EU DSO-enheten, lämna in utkastet till rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker med resultaten av den unionsomfattande bedömningen av cybersäkerhetsrisker till Acer för yttrande. Acer ska avge ett yttrande om utkastet till rapport inom tre månader från mottagandet. Entso för el och EU DSO-enheten ska ta största möjliga hänsyn till Acers yttrande när rapporten slutförs.

5. Inom tre månader från mottagandet av Acers yttrande ska Entso för el, i samarbete med EU DSO-enheten, anmäla den slutliga rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker till Acer, kommissionen, Enisa och de behöriga myndigheterna.

Artikel 20

Bedömning på medlemsstatsnivå av cybersäkerhetsrisker

1. Varje behörig myndighet ska utföra en bedömning på medlemsstatsnivå av cybersäkerhetsrisker för alla entiteter med stor och kritisk påverkan i sin medlemsstat med hjälp av de metoder som utvecklats i enlighet med artikel 18 och godkänts i enlighet med artikel 8. I bedömningen på medlemsstatsnivå av cybersäkerhetsrisker ska riskerna för cyberangrepp som påverkar elsystemets driftsäkerhet och stör de gränsöverskridande elflödena identifieras och analyseras. Bedömningen på medlemsstatsnivå av cybersäkerhetsrisker ska inte beakta cyberangreppens rättsliga, ekonomiska eller anseendemässiga skada.

2. Inom 21 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6 och vart tredje år efter det datumet, och efter samråd med den behöriga myndigheten med ansvar för cybersäkerhet, ska varje behörig myndighet, med stöd av CSIRT-enheten, tillhandahålla en bedömning på medlemsstatsnivå av cybersäkerhetsrisker till Entso för el och EU DSO-enheten, med följande information för varje verksamhetsprocess med stor och kritisk påverkan:

a) Läget i genomförandet av cybersäkerhetskontroller på lägsta nivå och avancerad nivå i enlighet med artikel 29.

b) En förteckning över alla cyberangrepp som rapporterats under de föregående tre åren i enlighet med artikel 38.3.

c) En sammanfattning av den information om cyberhot som rapporterats under de föregående tre åren i enlighet med artikel 38.6.

d) För varje unionsomfattande process med stor eller kritisk påverkan, en uppskattning av riskerna för att konfidentialiteten, integriteten och tillgängligheten för information och relevanta tillgångar äventyras.

e) Vid behov, en förteckning över ytterligare entiteter som identifierats som entiteter med stor eller kritisk påverkan i enlighet med artikel 24 punkterna 1, 2, 3 och 5.

3. I rapporten om bedömning på medlemsstatsnivå av cybersäkerhetsrisker ska medlemsstatens riskberedskapsplan som upprättats i enlighet med artikel 10 i förordning (EU) 2019/941 beaktas.

4. Informationen i rapporten om bedömning på medlemsstatsnivå av cybersäkerhetsrisker enligt punkt 2 a–d får inte vara kopplad till specifika entiteter eller tillgångar. Rapporten om bedömning på medlemsstatsnivå av cybersäkerhetsrisker ska också innehålla en riskbedömning av de tillfälliga undantag som utfärdats av de behöriga myndigheterna i medlemsstaterna i enlighet med artikel 30.

5. Entso för el och EU DSO-enheten får begära ytterligare information från de behöriga myndigheterna i samband med de uppgifter som anges i punkt 2 a och 2 c.

6. De behöriga myndigheterna ska se till att den information de lämnar är exakt och korrekt.

Artikel 21

Bedömning på regional nivå av cybersäkerhetsrisker

1. Entso för el ska, i samarbete med EU DSO-enheten och i samråd med det berörda regionala samordningscentrumet, utföra en bedömning på regional nivå av cybersäkerhetsrisker för varje systemdriftsregion med hjälp av de metoder som utvecklats i enlighet med artikel 19 och godkänts i enlighet med artikel 8, för att identifiera, analysera och utvärdera riskerna för cyberangrepp som påverkar elsystemets driftsäkerhet och stör de gränsöverskridande elflödena. Bedömningarna på regional nivå av cybersäkerhetsrisker ska inte beakta cyberangreppens rättsliga, ekonomiska eller anseendemässiga skada.

2. Inom 30 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6, och vart tredje år därefter, ska Entso för el, i samarbete med EU DSO-enheten och i samråd med samarbetsgruppen för nät- och informationssäkerhet, utarbeta en rapport om bedömningen på regional nivå av cybersäkerhetsrisker för varje systemdriftsregion.

3. Rapporten om bedömningen på regional nivå av cybersäkerhetsrisker ska beakta den relevanta informationen i rapporterna om unionsomfattande bedömning av cybersäkerhetsrisker och i rapporterna om bedömning på medlemsstatsnivå av cybersäkerhetsrisker.

4. Bedömningen på regional nivå av cybersäkerhetsrisker ska beakta de regionala elkrisscenarier med anknytning till cybersäkerhet som identifierats i enlighet med artikel 6 i förordning (EU) 2019/941.

Artikel 22

Regionala planer för reducering av cybersäkerhetsrisker

1. Inom 36 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6, och senast den 13 juni 2031 och vart tredje år därefter, ska de systemansvariga för överföringssystem, med bistånd från Entso för el, i samarbete med EU DSO-enheten och i samråd med de regionala samordningscentrumen och samarbetsgruppen för nät- och informationssäkerhet, utarbeta en regional planer för reducering av cybersäkerhetsrisker för varje systemdriftsregion.

2. De regionala planerna för reducering av cybersäkerhetsrisker ska innehålla

a) de cybersäkerhetskontroller på lägsta nivå och avancerad nivå som entiteterna med stor eller kritisk påverkan ska tillämpa i systemdriftsregionen,

b) de kvarstående cybersäkerhetsriskerna i systemdriftsregionerna efter tillämpning av de kontroller som avses i led a.

3. Entso för el ska lämna in de regionala riskreduceringsplanerna till de berörda systemansvariga för överföringssystem, de behöriga myndigheterna och gruppen för samordning på elområdet. Gruppen för samordning på elområdet får rekommendera ändringar.

4. De systemansvariga för överföringssystem ska, med bistånd från Entso för el i samarbete med EU DSO-enheten och i samråd med samarbetsgruppen för nät- och informationssäkerhet, uppdatera de regionala riskreduceringsplanerna vart tredje år, såvida inte omständigheterna kräver uppdateringar oftare.

Artikel 23

Övergripande rapport om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden

1. Inom 40 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6 och vart tredje år därefter ska de systemansvariga för överföringssystem, med bistånd från Entso för el, i samarbete med EU DSO-enheten och i samråd med samarbetsgruppen för nät- och informationssäkerhet, tillhandahålla gruppen för samordning på elområdet en rapport om resultatet av bedömningen av cybersäkerhetsrisker i samband med gränsöverskridande elflöden (*den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden*).

2. Den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden ska baseras på rapporterna om bedömningen på nationell nivå, regional nivå och medlemsstatsnivå av cybersäkerheten och innehålla följande information:

a) Den förteckning över unionsomfattande processer med stor och kritisk påverkan som identifierats i rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.2 a, inbegripet uppskattningen av sannolikheten för och påverkan av de cybersäkerhetsrisker som utvärderats i rapporterna om bedömningen på regional nivå av cybersäkerhetsrisker enligt artikel 21.2 och artikel 19.3 a.

b) Aktuella cyberhot, med särskilt fokus på framväxande hot och risker för elsystemet.

c) Cyberangrepp under den föregående perioden på unionsnivå, med en kritisk översikt över hur sådana cyberangrepp kan ha påverkat de gränsöverskridande elflödena.

d) Det övergripande läget i genomförandet av cybersäkerhetsåtgärderna.

e) Läget i genomförandet av informationsflödena enligt artiklarna 37 och 38.

f) En förteckning över information eller särskilda kriterier för klassificering av information i enlighet med artikel 46.

g) Identifierade och belysta risker som kan uppstå till följd av osäker styrning i försörjningskedjan,

h) Resultat och samlade erfarenheter från regionala och regionövergripande cybersäkerhetsövningar som organiseras i enlighet med artikel 44.

i) En analys av utvecklingen av de övergripande gränsöverskridande cybersäkerhetsriskerna inom elsektorn sedan de senaste bedömningarna på regional nivå av cybersäkerhetsrisker.

j) All annan information som kan vara användbar för att identifiera möjliga förbättringar av denna förordning eller behov av en revidering av denna förordning eller något av dess verktyg.

k) Aggregerad och anonymiserad information om undantag som beviljats i enlighet med artikel 30.3.

3. De entiteter som förtecknas i artikel 2.1 får bidra till utarbetandet av den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden, med beaktande av informationens konfidentialitet i enlighet med artikel 47. De systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, samråda med dessa entiteter från ett tidigt skede.

4. Den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden ska omfattas av reglerna för skydd av informationsutbyte i enlighet med artikel 46. Utan att det påverkar tillämpningen av artiklarna 10.4 och 47.4 ska Entso för el och EU DSO-enheten publicera en offentlig version av rapporten som inte får innehålla information som kan orsaka skada för de entiteter som förtecknas i artikel 2.1. Den offentliga versionen av denna rapport ska endast publiceras med godkännande från samarbetsgruppen för nät- och informationssäkerhet och gruppen för samordning på elområdet. Entso för el ska i samordning med EU DSO-enheten ansvara för sammanställningen och publiceringen av den offentliga versionen av rapporten.

Artikel 24

Identifiering av entiteter med stor och kritisk påverkan

1. Varje behörig myndighet ska, genom att använda ECII och de tröskelvärden för stor och kritisk påverkan som ingår i rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.3 b, identifiera de entiteter med stor och kritisk påverkan i sin medlemsstat som deltar i de unionsomfattande processerna med stor och kritisk påverkan. De behöriga myndigheterna kan begära information från en entitet i sin medlemsstat för att fastställa ECII-värdena för den entiteten. Om det fastställda ECII-värdet för en entitet ligger över tröskelvärdet för stor eller kritisk påverkan, ska den identifierade entiteten förtecknas i den rapport om bedömningen på medlemsstatsnivå av cybersäkerhetsrisker som avses i artikel 20.2.

2. Varje behörig myndighet ska, genom att använda ECII och de tröskelvärden för stor och kritisk påverkan som ingår i rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.3 b, identifiera de entiteter med stor och kritisk påverkan som inte är etablerade i unionen i den mån de är verksamma inom unionen. Den behöriga myndigheten får begära information från en entitet som inte är etablerad i unionen för att fastställa ECII-värdena för den entiteten.

3. Varje behörig myndighet får identifiera ytterligare entiteter i sin medlemsstat som entiteter med stor eller kritisk påverkan, om följande kriterier är uppfyllda:

a) Entiteten ingår i en grupp av entiteter som löper betydande risk för att påverkas samtidigt av ett cyberangrepp.

b) Det aggregerade ECII-värdet för gruppen av entiteter ligger över tröskelvärdet för stor eller kritisk påverkan.

4. Om en behörig myndighet identifierar ytterligare entiteter i enlighet med punkt 3, ska alla processer vid dessa entiteter för vilka gruppens aggregerade ECII-värde ligger över tröskelvärdet för stor påverkan betraktas som processer med stor påverkan, och alla processer vid dessa entiteter för vilka gruppens aggregerade ECII-värde ligger över tröskelvärdet för kritisk påverkan betraktas som processer med kritisk påverkan.

5. Om en behörig myndighet identifierar sådana entiteter som avses i punkt 3 a i mer än en medlemsstat, ska den informera de andra behöriga myndigheterna, Entso för el och EU DSO-enheten. Entso för el ska i samarbete med EU DSO-enheten, på grundval av den information som tagits emot från alla behöriga myndigheter, tillhandahålla de behöriga myndigheterna en analys av aggregerade entiteter i mer än en medlemsstat som kan orsaka en utbredd störning (*distributed disturbance*) av de gränsöverskridande elflödena och resultera i ett cyberangrepp. Om en grupp entiteter i flera medlemsstater identifieras som en aggregering vars ECII-värde ligger över tröskelvärdet för stor eller kritisk påverkan, ska alla berörda behöriga myndigheter identifiera entiteterna i en sådan grupp som entiteter med stor eller kritisk påverkan för deras respektive medlemsstat, baserat på det aggregerade ECII-värdet för gruppen av entiteter, och de identifierade entiteterna ska förtecknas i rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker.

6. Varje behörig myndighet ska, inom nio månader från att ha underrättats av Entso för el och EU DSO-enheten om rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.5 och under alla omständigheter senast den 13 juni 2028 underrätta entiteterna i förteckningen om att de har identifierats som en entitet med stor eller kritisk påverkan i sin medlemsstat.

7. När det till en behörig myndighet rapporteras att en tjänsteleverantör är en leverantör av kritiska IKT-tjänster enligt artikel 27 c ska den behöriga myndigheten anmäla detta till de behöriga myndigheterna i de medlemsstater på vars territorium leverantören har sitt säte eller sin företrädare. Den sistnämnda behöriga myndigheten ska underrätta tjänsteleverantören om att den har identifierats som en leverantör av kritiska tjänster.

Artikel 25

Nationella verifieringssystem

1. De behöriga myndigheterna får inrätta ett nationellt verifieringssystem för att verifiera att entiteter med kritisk påverkan som identifierats i enlighet med artikel 24.1 har genomfört den nationella rättsliga ram som ingår i den jämförelsematris som avses i artikel 34. Det nationella verifieringssystemet får baseras på en inspektion som utförs av den behöriga myndigheten, på oberoende säkerhetsrevisioner eller på ömsesidiga sakkunnigbedömningar som utförs av entiteterna med kritisk påverkan i samma medlemsstat, under den behöriga myndighetens tillsyn.

2. Om en behörig myndighet beslutar att inrätta ett nationellt verifieringssystem, ska den säkerställa att verifieringen utförs i enlighet med följande krav:

a) Varje part som utför sakkunnigbedömningen, revisionen eller inspektionen ska vara oberoende i förhållande till den entitet med kritisk påverkan som verifieras och får inte ha några intressekonflikter.

b) Den personal som utför sakkunnigbedömningen, revisionen eller inspektionen ska ha påvisbar kunskap om

   i) cybersäkerhet inom elsektorn,

   ii) ledningssystem för cybersäkerhet,

   iii) revisionsprinciperna,

   iv) bedömning av cybersäkerhetsrisker,

   v) den gemensamma ramen för cybersäkerhet i elsektorn,

   vi) lagstiftning och regelverk på nationell nivå och europeiska och internationella standarder som är relevanta för verifieringen,

   vii) de processer med kritisk påverkan som omfattas av verifieringen.

c) Den part som utför sakkunnigbedömningen, revisionen eller inspektionen ska ges tillräckligt med tid för utförandet.

d) Den part som utför sakkunnigbedömningen, revisionen eller inspektionen ska vidta lämpliga åtgärder för att skydda den information som samlas in under verifieringen, i enlighet med konfidentialitetsnivån på denna.

e) Sakkunnigbedömningarna, revisionerna eller inspektionerna ska genomföras minst en gång om året och en fullständig verifiering ska göras minst vart tredje år.

3. Om en behörig myndighet beslutar att inrätta ett nationellt verifieringssystem, ska den årligen rapportera till Acer om hur ofta den har utfört inspektioner inom ramen för det systemet.

Artikel 26

Cybersäkerhetsriskhantering på entitetsnivå

1. Varje entitet med stor och kritisk påverkan som identifierats av de behöriga myndigheterna i enlighet med artikel 24.1 ska hantera cybersäkerhetsrisker för alla sina tillgångar i sina områden med stor och kritisk påverkan. Varje entitet med stor och kritisk påverkan ska vart tredje år hantera riskerna enligt faserna i punkt 2.

2. Varje entitet med stor och kritisk påverkan ska grunda sin hantering av cybersäkerhetsrisker på en metod som syftar till att skydda dess nätverks- och informationssystem och som omfattar följande faser:

a) Fastställande av kontext.

b) Bedömning på entitetsnivå av cybersäkerhetsrisker.

c) Behandling av cybersäkerhetsrisker.

d) Acceptans av cybersäkerhetsrisker.

3. Under fasen ”Fastställande av kontext” ska varje entitet med stor och kritisk påverkan

a) fastställa omfattningen av bedömningen av cybersäkerhetsrisker, inbegripet de processer med stor och kritisk påverkan som identifierats av Entso för el och EU DSO-enheten, och andra processer som kan utgöra mål för cyberangrepp med stor eller kritisk påverkan på de gränsöverskridande elflödena, och

b) fastställa kriterierna för riskutvärdering och för riskacceptans i enlighet med den riskpåverkansmatris som entiteterna och de behöriga myndigheterna ska använda för att bedöma cybersäkerhetsriskerna i de metoder för bedömning på unionsnivå, regional nivå och medlemsstatsnivå av cybersäkerhetsrisker som tagits fram av Entso för el och EU DSO-enheten i enlighet med artikel 19.2.

4. Under fasen ”Bedömning av cybersäkerhetsrisker” ska varje entitet med stor påverkan och kritisk påverkan göra följande:

a) Identifiera cybersäkerhetsrisker genom att beakta

i) alla tillgångar som stöder unionsomfattande processer med stor och kritisk påverkan, varvid en bedömning ska göras av huruvida de gränsöverskridande elflödena påverkas av om tillgången äventyras,

ii) möjliga cyberhot med beaktande av de cyberhot som identifierats i den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden som avses i artikel 23 och med beaktande av hoten mot leveranskedjan,

iii) sårbarheter, inbegripet sårbarheter i äldre system,

iv) möjliga cyberangreppsscenarier, inbegripet cyberangrepp som påverkar elsystemets driftsäkerhet och stör de gränsöverskridande elflödena,

v) relevanta riskutvärderingar och riskbedömningar som utförs på unionsnivå, inbegripet samordnade riskbedömningar av kritiska leveranskedjor i enlighet med artikel 22 i direktiv (EU) 2022/2555, och

vi) befintliga genomförda kontroller.

b) Analysera sannolikheten för och konsekvenserna av de cybersäkerhetsrisker som identifieras i led a och fastställa cybersäkerhetsrisknivån, med hjälp av den riskpåverkansmatris som används för att bedöma cybersäkerhetsrisker i de metoder på unionsnivå, regional nivå och medlemsstatsnivå för bedömning av cybersäkerhetsrisker som tagits fram av de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten i enlighet med artikel 19.2.

c) Klassificera tillgångar efter möjliga konsekvenser när cybersäkerheten äventyras och fastställa området med stor och kritisk påverkan med hjälp av följande steg:

i) Genomför, med hjälp av ECII och för alla processer som omfattas av bedömningen av cybersäkerhetsrisker, en konsekvensbedömning för verksamheten.

ii) Klassificera en process som en process med stor eller kritisk påverkan, om dess ECII-värde ligger över tröskelvärdet för stor respektive kritisk påverkan.

iii) Fastställa att alla tillgångar med stor och kritisk påverkan är de tillgångar som behövs för processerna med stor respektive kritisk påverkan.

iv) Definiera alla områden där det finns tillgångar med stor respektive kritiska påverkan som områden med stor eller kritisk påverkan, så att tillträde till områdena kan kontrolleras.

d) Utvärdera cybersäkerhetsrisker genom att prioritera dem med hjälp av de riskutvärderingskriterier och riskacceptanskriterier som avses i punkt 3 b.

5. Under fasen ”Behandling av cybersäkerhetsrisker” ska varje entitet med stor och kritisk påverkan upprätta en riskreduceringsplan på entitetsnivå genom att välja lämpliga riskbehandlingsalternativ för att hantera riskerna och identifiera de kvarstående riskerna.

6. Under fasen ”Acceptans av cybersäkerhetsrisker” ska varje entitet med stor och kritisk påverkan besluta, på grundval av de kriterier för riskacceptans som fastställs i punkt 3 b, huruvida den kvarstående risken ska accepteras.

7. Varje entitet med stor och kritisk påverkan ska registrera de tillgångar som identifieras i punkt 1 i ett tillgångsinventarium. Detta tillgångsinventarium ska inte ingå i riskbedömningsrapporten.

8. Den behöriga myndigheten får inspektera tillgångarna i inventariet under inspektionerna.

Artikel 27

Rapportering av riskbedömning på entitetsnivå.

Varje entitet med stor eller kritisk påverkan ska, inom 12 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6, och därefter vart tredje år, tillhandahålla den behöriga myndigheten en rapport med följande information:

1. En förteckning över de kontroller som valts ut för riskreduceringsplanen på entitetsnivå enligt artikel 26.5 med angivande av det aktuella läget i genomförandet för varje kontroll.

2. För varje unionsomfattande process med stor eller kritisk påverkan, en uppskattning av risken för att konfidentialiteten, integriteten och tillgängligheten hos information och relevanta tillgångar äventyras. Uppskattningen av denna risk ska lämnas i enlighet med riskpåverkansmatrisen i artikel 19.2.

3. En förteckning över leverantörer av kritiska IKT-tjänster för deras processer med kritisk påverkan.

KAPITEL III

GEMENSAM RAM FÖR CYBERSÄKERHET I ELSEKTORN

Artikel 28

Sammansättning, funktion och översyn av den gemensamma ramen för cybersäkerhet i elsektorn

1. Den gemensamma ramen för cybersäkerhet i elsektorn ska bestå av följande kontroller och följande ledningssystem för cybersäkerhet:

a) Cybersäkerhetskontroller på lägsta nivå, utarbetade i enlighet med artikel 29.

b) Cybersäkerhetskontroller på avancerad nivå, utarbetade i enlighet med artikel 29.

c) Jämförelsematrisen, utvecklad i enlighet med artikel 34, som jämför de kontroller som avses i leden a och b med utvalda europeiska och internationella standarder och lagstiftning och regelverk på nationell nivå.

d) Det ledningssystem för cybersäkerhet som inrättats i enlighet med artikel 32.

2. Alla entiteter med stor påverkan ska tillämpa cybersäkerhetskontrollerna på lägsta nivå i enlighet med punkt 1 a inom sitt område med stor påverkan.

3. Alla entiteter med kritisk påverkan ska tillämpa cybersäkerhetskontrollerna på avancerad nivå i enlighet med punkt 1 b inom sitt område med kritisk påverkan.

4. Inom sju månader från överlämnandet av det första utkastet till rapport om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.4 ska den gemensamma ram för cybersäkerhet i elsektorn som avses i punkt 1 kompletteras med cybersäkerhetskontroller på lägsta nivå och avancerad nivå i den leveranskedja som utvecklats i enlighet med artikel 33.

Artikel 29

Cybersäkerhetskontroller på lägsta nivå och avancerad nivå

1. Inom sju månader från inlämnandet av det första utkastet till rapport om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.4 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten, utarbeta ett förslag till cybersäkerhetskontroller på lägsta nivå och avancerad nivå.

2. Inom sex månader från utarbetandet av varje rapport om bedömningen på regional nivå av cybersäkerhetsrisker i enlighet med artikel 21.2 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten, föreslå den behöriga myndigheten en ändring av cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå. Förslaget kommer att utarbetas i enlighet med artikel 8.10 och kommer att ta hänsyn till de risker som identifierats i riskbedömningen på regional nivå.

3. Cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå ska kunna verifieras genom deltagande i ett nationellt verifieringssystem i enlighet med det förfarande som fastställs i artikel 31, eller genom att genomgå oberoende säkerhetsrevisioner som utförs av tredje part i enlighet med de krav som förtecknas i artikel 25.2.

4. De ursprungliga cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå som utarbetas i enlighet med punkt 1 ska baseras på de risker som identifieras i rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker som avses i artikel 19.5. De ändrade cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå som utarbetas i enlighet med punkt 2 ska baseras på rapporten om bedömningen på regional nivå av cybersäkerhetsrisker som avses i artikel 21.2.

5. Cybersäkerhetskontrollerna på lägsta nivå ska omfatta kontroller för att skydda den information som utbyts i enlighet med artikel 46.

6. Inom 12 månader från det att cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå har godkänts i enlighet med artikel 8.5, eller efter varje uppdatering i enlighet med artikel 8.10, ska de entiteter som förtecknas i artikel 2.1, och identifieras som entiteter med stor och kritisk påverkan i enlighet med artikel 24, under upprättandet av en riskreduceringsplan på entitetsnivå i enlighet med artikel 26.5, tillämpa cybersäkerhetskontrollerna på lägsta nivå inom området med stor påverkan och cybersäkerhetskontrollerna på avancerad nivå inom området med kritisk påverkan.

Artikel 30

Undantag från cybersäkerhetskontroller på lägsta nivå och avancerad nivå

1. De entiteter som förtecknas i artikel 2.1 får begära att respektive behörig myndighet beviljar ett undantag från deras skyldighet att tillämpa de cybersäkerhetskontroller på lägsta nivå och avancerad nivå som avses i artikel 29.6. Den behöriga myndigheten får bevilja ett sådant undantag av något av följande skäl:

a) Under exceptionella omständigheter, om entiteten kan visa att kostnaderna för att genomföra lämpliga cybersäkerhetskontroller avsevärt överstiger fördelarna. Acer och Entso för el får, i samarbete med EU DSO-enheten, gemensamt utarbeta en vägledning för att hjälpa entiteterna att uppskatta kostnaderna för cybersäkerhetskontroller.

b) Om entiteten tillhandahåller en riskbehandlingsplan på entitetsnivå som reducerar cybersäkerhetsriskerna med hjälp av alternativa kontroller till en nivå som är acceptabel i enlighet med de riskacceptanskriterier som avses i artikel 26.3 b.

2. Inom tre månader från mottagandet av den begäran som avses i punkt 1 ska varje behörig myndighet besluta huruvida ett undantag från cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå ska beviljas. Undantag från cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå ska beviljas för högst tre år, med möjlighet till förlängning.

3. Aggregerad och anonymiserad information för de undantag som beviljats ska ingå som en bilaga till den övergripande rapporten om bedömning av cybersäkerhetsrisker i samband med gränsöverskridande elflöden som avses i artikel 23. Entso för el och EU DSO-enheten ska vid behov gemensamt uppdatera förteckningen.

Artikel 31

Verifiering av den gemensamma ramen för cybersäkerhet i elsektorn

1. Senast 24 månader efter antagandet av de kontroller som avses i leden a, b och c i artikel 28.1 och inrättandet av det ledningssystem för cybersäkerhet som avses i led d i den artikeln ska varje entitet med kritisk påverkan som identifierats i enlighet med artikel 24.1 på begäran av den behöriga myndigheten kunna visa att de tillämpar ledningssystemet för cybersäkerhet och cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå.

2. Varje entitet med kritisk påverkan ska fullgöra den skyldighet som avses i punkt 1 genom att genomgå oberoende säkerhetsrevisioner utförda av tredje part i enlighet med de krav som förtecknas i artikel 25.2 eller genom att delta i ett nationellt verifieringssystem i enlighet med artikel 25.1.

3. Verifieringen av att en entitet med kritisk påverkan på korrekt sätt tillämpar ledningssystemet för cybersäkerhet och cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå ska omfatta alla tillgångar inom entitetens område med kritisk påverkan.

4. Verifieringen av att en entitet med kritisk påverkan på korrekt sätt tillämpar ledningssystemet för cybersäkerhet och cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå ska upprepas regelbundet senast 36 månader efter avslutandet av den första verifieringen, och vart tredje år därefter.

5. Varje entitet med kritisk påverkan som definieras i enlighet med artikel 24 ska visa att den på korrekt sätt tillämpar de kontroller som avses i leden a, b och c i artikel 28.1 och det ledningssystem för cybersäkerhet som avses i led d i den artikeln genom att rapportera resultatet av verifieringen av tillämpningen till den behöriga myndigheten.

Artikel 32

Ledningssystem för cybersäkerhet

1. Inom 24 månader från att ha underrättats av den behöriga myndigheten om att vara identifierad som en entitet med stor eller kritisk påverkan i enlighet med artikel 24.6 ska varje entitet med stor och kritisk påverkan inrätta ett ledningssystem för cybersäkerhet, och därefter vart tredje år se över detta, för att

a) fastställa tillämpningsområdet för ledningssystemet för cybersäkerhet med beaktande av kontaktytor och beroende i förhållande till andra entiteter,

b) säkerställa att hela dess ledning informeras om de relevanta rättsliga skyldigheterna och aktivt bidrar till genomförandet av ledningssystemet för cybersäkerhet genom att fatta beslut i rätt tid och agera skyndsamt,

c) säkerställa att ledningssystemet för cybersäkerhet ges nödvändiga resurser,

d) fastställa en cybersäkerhetsstrategi som ska dokumenteras inom entiteten och kommuniceras inom entiteten och till de parter som påverkas av säkerhetsriskerna,

e) tilldela ansvarsområden för de roller som är relevanta för cybersäkerheten, och informera om detta,

f) hantera cybersäkerhetsrisker på entitetsnivå i enlighet med artikel 26,

g) fastställa vilka resurser som krävs för genomförande, underhåll och kontinuerlig förbättring av ledningssystemet för cybersäkerhet och tillhandahålla dessa, varvid den erforderliga kompetensen och medvetandet om cybersäkerhetsresurser ska beaktas,

h) fastställa den interna och externa kommunikationen av relevans för cybersäkerheten,

i) skapa, uppdatera och kontrollera dokumenterad information om ledningssystemet för cybersäkerhet,

j) utvärdera resultatet av och ändamålsenligheten hos ledningssystemet för cybersäkerhet,

k) genomföra internrevisioner med planerade intervall för att säkerställa att ledningssystemet för cybersäkerhet genomförs och underhålls på ett effektivt sätt,

l) se över genomförandet av ledningssystemet för cybersäkerhet med planerade intervall, och kontrollera att resurserna och verksamheten överensstämmer med policyerna, förfarandena och riktlinjerna i ledningssystemet för cybersäkerhet, och korrigera eventuella brister.

2. Tillämpningsområdet för ledningssystemet för cybersäkerhet ska omfatta alla tillgångar inom det område med stor och kritisk påverkan som tillhör entiteten med stor och kritisk påverkan.

3. De behöriga myndigheterna ska, utan att ålägga eller diskriminera till förmån för användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationella standarder och specifikationer som rör ledningssystem för cybersäkerhet och som är relevanta för säkerheten i nätverks- och informationssystem.

Artikel 33

Cybersäkerhetskontroller på lägsta nivå och avancerad nivå i leveranskedjan

1. Inom sju månader från inlämnandet av det första utkastet till rapport om den unionsomfattande bedömningen av cybersäkerhetsrisker i enlighet med artikel 19.4 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten, utarbeta ett förslag till cybersäkerhetskontroller på lägsta nivå och avancerad nivå i leveranskedjan som reducerar de risker i leveranskedjan som identifierats i de unionsomfattande bedömningarna av cybersäkerhetsrisker, och kompletterar de cybersäkerhetskontroller på lägsta nivå och avancerad nivå som utarbetats i enlighet med artikel 29. Cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i leveranskedjan ska utvecklas tillsammans med cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i enlighet med artikel 29. Cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i leveranskedjan ska omfatta hela livscykeln för alla IKT-produkter, IKT-tjänster och IKT-processer inom de områden med stor eller kritisk påverkan som tillhör en entitet med stor eller kritisk påverkan. Samråd ska ske med samarbetsgruppen för nät- och informationssäkerhet vid utarbetandet av förslaget till cybersäkerhetskontroller på lägsta nivå och avancerad nivå i leveranskedjan.

2. Cybersäkerhetskontrollerna på lägsta nivå i leveranskedjan ska bestå av kontroller för entiteter med stor påverkan och enheter med kritisk påverkan, som omfattar följande:

a) Rekommendationer för upphandling av IKT-produkter, IKT-tjänster och IKT-processer med hänvisning till cybersäkerhetsspecifikationer, som åtminstone omfattar följande:

   i) Säkerhetsprövning av den personal hos leverantören som deltar i leveranskedjan och hanterar känslig information eller har åtkomst till entitetens tillgångar med stor eller kritisk påverkan. Säkerhetsprövningen kan omfatta en identitets- och bakgrundskontroll av en entitets personal eller underleverantörer i enlighet med nationell rätt och nationella förfaranden och relevant och tillämplig unionsrätt, inbegripet förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU) 2016/680 ([18]). Säkerhetsprövningen ska vara proportionell och strikt begränsad till vad som är nödvändigt. Den ska utföras enbart i syfte att utvärdera en potentiell säkerhetsrisk för den berörda entiteten. Den måste stå i proportion till verksamhetskrav, klassificeringen av den information som åtkomsten gäller och de upplevda riskerna, och får utföras av entiteten själv, av ett externt företag som utför en säkerhetskontroll, eller genom en statlig klarering.

   ii) Processer för säker och kontrollerad utformning, utveckling och produktion av IKT-produkter, IKT-tjänster och IKT-processer, som främjar utformning och utveckling av IKT-produkter, IKT-tjänster och IKT-processer som inbegriper lämpliga tekniska åtgärder för att säkerställa cybersäkerhet.

   iii) Utformning av nätverks- och informationssystem med utrustning som inte är tillförlitlig, trots att den befinner sig inom ett säkert område, och som kräver verifiering av alla begäranden som den tar emot, med tillämpning av principen för begränsad behörighet.

   iv) Leverantörens åtkomst till entitetens tillgångar.

([18]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

v) Leverantörens avtalsenliga skyldigheter att skydda och begränsa åtkomsten till entitetens känsliga information.

vi) De underliggande upphandlingsspecifikationerna på cybersäkerhetsområdet för underleverantörer till leverantören.

vii) Spårbarheten hos tillämpningen av cybersäkerhetsspecifikationer från utveckling via produktion till leverans av IKT-produkter, IKT-tjänster eller IKT-processer.

viii) Stöd för säkerhetsuppdateringar under hela livscykeln för IKT-produkter, IKT-tjänster eller IKT-processer.

ix) Rätten att genomföra revision av cybersäkerheten i leverantörens utformnings-, utvecklings- och produktionsprocesser.

x) Bedömningen av leverantörens riskprofil.

b) Krav på att sådana entiteter beaktar de upphandlingsrekommendationer som avses i led a när de sluter avtal med leverantörer, samarbetspartner och andra parter i leveranskedjan, och som omfattar ordinarie leveranser av IKT-produkter, IKT-tjänster och IKT-processer, samt oplanerade händelser och omständigheter såsom uppsägning och överföring av avtal på grund av avtalspartnerns försumlighet.

c) Krav på att sådana entiteter beaktar resultaten av relevanta samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som genomförts i enlighet med artikel 22.1 i direktiv (EU) 2022/2555.

d) Kriterier för att välja ut och sluta avtal med leverantörer som kan uppfylla de cybersäkerhetsspecifikationer som anges i led a och som har en cybersäkerhetsnivå som är lämplig för cybersäkerhetsriskerna med den IKT-produkt, IKT-tjänst eller IKT-process som leverantören levererar.

e) Kriterier för att diversifiera IKT-produkternas, IKT-tjänsternas och IKT-processernas leveranskällor och minska risken för leverantörsinlåsning.

f) Kriterier för att regelbundet övervaka, se över eller granska cybersäkerhetsspecifikationerna för leverantörernas interna operativa processer under hela livscykeln för varje IKT-produkt, IKT-tjänst och IKT-process.

3. För cybersäkerhetsspecifikationerna i den rekommendation om upphandling på cybersäkerhetsområdet som avses i punkt 2 a ska entiteter med stor eller kritisk påverkan använda principerna för upphandling i enlighet med Europaparlamentets och rådets direktiv 2014/24/EU ([19]), i enlighet med artikel 35.4, eller fastställa egna specifikationer på grundval av resultaten av bedömningen på entitetsnivå av cybersäkerhetsrisker.

4. Cybersäkerhetskontrollerna på avancerad nivå i leveranskedjan ska omfatta kontroller av entiteter med kritisk påverkan för att vid upphandling verifiera att IKT-produkter, IKT-tjänster och IKT-processer som kommer att användas som tillgångar med kritisk påverkan uppfyller cybersäkerhetsspecifikationerna. IKT-produkten, IKT-tjänsten eller IKT-processen ska verifieras antingen genom en europeisk ordning för cybersäkerhetscertifiering som avses i artikel 31 eller genom verifieringsåtgärder som väljs ut och organiseras av entiteten. Verifieringsåtgärderna ska vara tillräckligt grundliga och omfattande för att det ska säkerställas att IKT-produkten, IKT-tjänsten eller IKT-processen kan användas för att reducera de risker som identifierats i riskbedömningen på entitetsnivå. Entiteten med kritisk påverkan ska dokumentera de åtgärder som vidtagits för att reducera de identifierade riskerna.

5. Cybersäkerhetskontroller på lägsta nivå och avancerad nivå i leveranskedjan ska tillämpas på upphandling av relevanta IKT-produkter, IKT-tjänster och IKT-processer. Cybersäkerhetskontrollerna på lägsta nivå och på avancerad nivå i leveranskedjan kommer att tillämpas på upphandlingsprocesser i de entiteter som identifierats som entiteter med kritisk påverkan och entiteter med stor påverkan enligt artikel 24, från sex månader efter antagandet eller uppdateringen av de cybersäkerhetskontroller på lägsta nivå och på avancerad nivå som avses i artikel 29.

([19]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

6. Inom sex månader från utarbetandet av varje rapport om bedömningen på regional nivå av cybersäkerhetsrisker i enlighet med artikel 21.2 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten, föreslå den behöriga myndigheten en ändring av cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå i leveranskedjan. Förslaget kommer att utarbetas i enlighet med artikel 8.10 och kommer att ta hänsyn till de risker som identifierats i riskbedömningen på regional nivå.

Artikel 34

Jämförelsematris för cybersäkerhetskontroller för el med standarder

1. Inom sju månader från inlämnandet av det första utkastet till rapport om unionsomfattande bedömning av cybersäkerhetsrisker i enlighet med artikel 19.4 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten och i samråd med Enisa, utarbeta ett förslag till en matris för att jämföra de kontroller som anges i artikel 28.1 leden a och b med utvalda europeiska och internationella standarder samt relevanta tekniska specifikationer (*jämförelsematrisen*). Entso för el och EU DSO-enheten ska dokumentera likvärdigheten mellan de olika kontrollerna och de kontroller som anges i artikel 28.1 leden a och b.

2. De behöriga myndigheterna får tillhandahålla Entso för el och EU DSO-enheten en jämförelse av de kontroller som anges i artikel 28.1 leden a och b med en hänvisning till tillhörande lagstiftning och regelverk på nationell nivå, inbegripet relevanta nationella standarder i medlemsstaterna i enlighet med artikel 25 i direktiv (EU) 2022/2555. Om den behöriga myndigheten i en medlemsstat tillhandahåller en sådan jämförelse, ska Entso för el och EU DSO-enheten integrera denna nationella jämförelse i jämförelsematrisen.

3. Inom sex månader från utarbetandet av varje rapport om bedömningen på regional nivå av cybersäkerhetsrisker i enlighet med artikel 21.2 ska de systemansvariga för överföringssystem, med bistånd från Entso för el och i samarbete med EU DSO-enheten och i samråd med Enisa, föreslå den behöriga myndigheten en ändring av jämförelsematrisen. Förslaget kommer att utarbetas i enlighet med artikel 8.10 och kommer att ta hänsyn till de risker som identifierats i riskbedömningen på regional nivå.

KAPITEL IV

REKOMMENDATIONER OM UPPHANDLING PÅ CYBERSÄKERHETSOMRÅDET

Artikel 35

Rekommendationer om upphandling på cybersäkerhetsområdet

1. De systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, i ett arbetsprogram som ska fastställas och uppdateras varje gång en rapport om bedömningen på regional nivå av cybersäkerhetsrisker antas, utarbeta en uppsättning icke-bindande rekommendationer om upphandling på cybersäkerhetsområdet som entiteter med stor och kritisk påverkan kan använda som grund för upphandling av IKT-produkter, IKT-tjänster och IKT-processer med stor och kritisk påverkan. Detta arbetsprogram ska omfatta följande:

a) En beskrivning och klassificering av de typer av IKT-produkter, IKT-tjänster och IKT-processer som används av entiteter med stor och kritisk påverkan inom området med stor och kritisk påverkan.

b) En förteckning över de typer av IKT-produkter, IKT-tjänster och IKT-processer för vilka en uppsättning icke-bindande cybersäkerhetsrekommendationer ska utarbetas på grundval av de relevanta rapporterna om bedömningen på regional nivå av cybersäkerhetsrisker och på grundval av prioriteringar inom entiteterna med stor och kritisk påverkan.

2. Entso för el ska, i samarbete med EU DSO-enheten, inom sex månader från antagandet eller uppdateringen av rapporten om bedömningen på regional nivå av cybersäkerhetsrisker tillhandahålla Acer en sammanfattning av arbetsprogrammet.

3. De systemansvariga för överföringssystem ska, med bistånd från Entso för el, och i samarbete med EU DSO-enheten, sträva efter att säkerställa att de icke-bindande rekommendationer om upphandling på cybersäkerhetsområdet som utarbetats på grundval av den relevanta bedömningen på regional nivå av cybersäkerhetsrisker är likartade eller jämförbara mellan olika systemdriftsregioner. Uppsättningarna rekommendationer om upphandling på cybersäkerhetsområdet ska omfatta åtminstone de specifikationer som avses i artikel 33.2 a. Där så är möjligt ska specifikationerna väljas från europeiska och internationella standarder.

4. Systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, säkerställa att uppsättningarna rekommendationer om upphandling på cybersäkerhetsområdet

a) följer principerna för upphandling i enlighet med direktiv 2014/24/EU, och

b) är förenliga med och beaktar de senast tillgängliga europeiska ordningarna för cybersäkerhetscertifiering av relevans för IKT-produkten, IKT-tjänsten eller IKT-processen.

Artikel 36

Vägledning om användning av europeiska ordningar för cybersäkerhetscertifiering vid upphandling av IKT-produkter, IKT-tjänster och IKT-processer

1. De icke-bindande rekommendationer om upphandling på cybersäkerhetsområdet som utarbetats i enlighet med artikel 35 får inbegripa sektorsspecifik vägledning om användningen av europeiska ordningar för cybersäkerhetscertifiering, närhelst en lämplig ordning finns tillgänglig för en typ av IKT-produkt, IKT-tjänst eller IKT-process som används av entiteter med kritisk påverkan, utan att det påverkar ramen för inrättandet av europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 46 i förordning (EU) 2019/881.

2. De systemansvariga för överföringssystem ska, med bistånd från Entso för el och i samarbete med EU DSO-enheten, ha ett nära samarbete med Enisa när det gäller att tillhandahålla den sektorsspecifika vägledning som ingår i icke-bindande rekommendationer om upphandling på cybersäkerhetsområdet i enlighet med punkt 1.

KAPITEL V

INFORMATIONSFLÖDEN, CYBERANGREPP OCH KRISHANTERING

Artikel 37

Regler om informationsdelning

1. Om en behörig myndighet tar emot information om ett rapporteringspliktigt cyberangrepp

a) ska den bedöma informationens konfidentialitetsnivå och informera entiteten om resultatet av sin bedömning utan onödigt dröjsmål och senast inom 24 timmar från mottagandet av informationen,

b) ska den sträva efter att finna andra liknande cyberangrepp i unionen som rapporterats till andra behöriga myndigheter, i syfte att korrelera den information som mottagits i samband med det rapporteringspliktiga cyberangreppet med information som tillhandahållits i samband med andra cyberangrepp och förbättra befintlig information, och stärka och samordna cybersäkerhetsinsatser,

c) ska den ansvara för avlägsnande av affärshemligheter och anonymisering av informationen i enlighet med relevant nationell lagstiftning och unionslagstiftning,

d) ska den dela informationen med de nationella gemensamma kontaktpunkterna, CSIRT-enheterna och alla behöriga myndigheter som utsetts i enlighet med artikel 4 i andra medlemsstater utan onödigt dröjsmål och senast 24 timmar efter mottagandet av information om ett rapporteringspliktigt cyberangrepp och regelbundet tillhandahålla uppdaterad information till dessa myndigheter eller organ,

e) ska den sprida informationen om cyberangreppet, efter anonymisering och avlägsnande av affärshemligheter i enlighet med punkt 1 c, till entiteter med kritisk och stor påverkan i sin medlemsstat utan onödigt dröjsmål och senast 24 timmar efter mottagandet av information i enlighet med punkt 1 a, och regelbundet tillhandahålla uppdaterad information som gör det möjligt för entiteterna att organisera sitt försvar på ett effektivt sätt,

f) får den begära att den rapporterande entiteten med stor eller kritisk påverkan ytterligare sprider den rapporteringspliktiga informationen om cyberangreppet på ett säkert sätt till andra entiteter som kan påverkas, i syfte att skapa situationsmedvetenhet inom elsektorn och förhindra att en risk som kan trappas upp till en gränsöverskridande cybersäkerhetsincident uppstår i elnätet,

g) ska den efter anonymisering och avlägsnande av affärshemligheter dela med sig av informationen om cyberangreppet i en sammanfattande rapport till Enisa.

2. Om en CSIRT-enhet får kännedom om en ej avhjälpt, aktivt utnyttjad sårbarhet ska den

a) utan dröjsmål meddela Enisa via en lämplig kanal för säkert informationsutbyte, om inte annat anges i annan unionslagstiftning,

b) hjälpa den berörda entiteten att från tillverkaren eller leverantören få en effektiv, samordnad och snabb hantering av den ej avhjälpta, aktivt utnyttjade sårbarheten eller av effektiva och ändamålsenliga begränsande åtgärder,

c) dela tillgänglig information med säljaren och begära att tillverkaren eller leverantören, när så är möjligt, fastställer en förteckning över CSIRT-enheter i medlemsstater som berörs av den ej avhjälpta, aktivt utnyttjade sårbarheten och som ska informeras,

d) dela tillgänglig information med de CSIRT-enheter som identifierats i föregående led, på grundval av principen om behovsenlig behörighet,

e) i förekommande fall dela med sig av strategier och åtgärder för begränsning av den rapporterade ej avhjälpta, aktivt utnyttjade sårbarheten.

3. Om en behörig myndighet får kännedom om en ej avhjälpt aktivt utnyttjad sårbarhet ska den

a) i förekommande fall dela, i samordning med CSIRT-enheterna i sin medlemsstat, strategier och åtgärder för begränsning av den rapporterade ej avhjälpta, aktivt utnyttjade sårbarheten,

b) dela informationen med en CSIRT-enhet i den medlemsstat där den ej avhjälpta, aktivt utnyttjade sårbarheten har rapporterats.

4. Om den behöriga myndigheten får kännedom om en ej avhjälpt sårbarhet, utan bevis för att den aktivt utnyttjas, ska den utan onödigt dröjsmål samordna med CSIRT-enheten för samordnat meddelande av sårbarhetsinformation i enlighet med artikel 12.1 i direktiv (EU) 2022/2555.

5. Om en CSIRT-enhet tar emot information om cyberhot från en eller flera entiteter med stor eller kritisk påverkan i enlighet med artikel 38.6, ska den sprida denna information eller annan information av betydelse för att förebygga, upptäcka, reagera på eller begränsa den tillhörande risken, till entiteter med kritisk och stor påverkan i sin medlemsstat och, när så är lämpligt, till alla berörda CSIRT-enheter och till sin nationella gemensamma kontaktpunkt, utan onödigt dröjsmål och senast fyra timmar efter mottagandet av informationen.

6. Om en behörig myndighet får kännedom om information om cyberhot från en eller flera entiteter med stor eller kritisk påverkan, ska den vidarebefordra denna information till CSIRT-enheten för tillämpning av punkt 5.

7. De behöriga myndigheterna får helt eller delvis delegera ansvaret enligt punkterna 3 och 4 avseende en eller flera entiteter med stor eller kritisk påverkan som bedriver verksamhet i mer än en medlemsstat till en annan behörig myndighet i en av dessa medlemsstater, efter överenskommelse mellan de berörda behöriga myndigheterna.

8. De systemansvariga för överföringssystem ska, med bistånd från Entso för el, och i samarbete med EU DSO-enheten, utarbeta en metod med en klassificeringsskala för cyberangrepp senast den 13 juni 2025. De systemansvariga för överföringssystem får, med bistånd från Entso för el och EU DSO-enheten, begära att de behöriga myndigheterna samråder med Enisa och andra behöriga myndigheter med ansvar för cybersäkerhet för bistånd vid utarbetandet av en sådan klassificeringsskala. Metoden ska ge en klassificering i fem nivåer av hur allvarlig ett cyberangrepp är, där de två högsta nivåerna är ”stor” och ”kritisk”. Klassificeringen ska grundas på en bedömning av följande parametrar:

a) Den möjliga påverkan med beaktande av exponerade tillgångar och områden, fastställd i enlighet med artikel 26.4 c.

b) Hur allvarligt cyberangreppet är.

9. Senast den 13 juni 2026 ska Entso för el, i samarbete med EU DSO-enheten, utföra en genomförbarhetsstudie för att bedöma möjligheten att utveckla ett gemensamt verktyg som gör det möjligt för alla entiteter att dela information med relevanta nationella myndigheter, samt de finansiella kostnader som nödvändigtvis följer med.

10. Genomförbarhetsstudien ska behandla möjligheten för ett sådant gemensamt verktyg att

a) stödja entiteter med kritisk och stor påverkan genom säkerhetsrelaterad information av relevans för driften avseende gränsöverskridande elflöden, såsom rapportering av cyberangrepp i nära realtid, förvarningar i cybersäkerhetsrelaterade frågor och ej offentliggjorda sårbarheter hos utrustning som används i elsystemet,

b) vara i drift i en lämplig och mycket tillförlitlig miljö,

c) möjliggöra datainsamling från entiteter med kritisk och stor påverkan och underlätta avlägsnande av konfidentiell information och anonymisering av data och snabb spridning av dessa till entiteter med kritisk och stor påverkan.

11. Entso för el ska, i samarbete med EU DSO-enheten,

a) vid bedömningen av genomförbarheten samråda med Enisa och samarbetsgruppen för nät- och informationssäkerhet, de nationella gemensamma kontaktpunkterna och företrädarna för de viktigaste intressenterna,

b) lägga fram resultaten av genomförbarhetsstudien för Acer och samarbetsgruppen för nät- och informationssäkerhet.

12. Entso för el får, i samarbete med EU DSO-enheten, analysera och underlätta initiativ som föreslås av entiteter med kritisk och stor påverkan för att utvärdera och testa sådana verktyg för informationsdelning.

Artikel 38

Roll för entiteter med stor och kritisk påverkan när det gäller informationsdelning

1. Varje entitet med stor och kritisk påverkan ska göra följande:

a) För alla tillgångar inom sitt cybersäkerhetsområde som fastställts i enlighet med artikel 26.4 c, fastställa åtminstone förmågan hos driftscentrumet för cybersäkerhet att

   i) säkerställa att relevanta nätsystem, informationssystem, nättillämpningar och informationstillämpningar tillhandahåller säkerhetsloggar för säkerhetsövervakning för att göra det möjligt att upptäcka avvikelser och samla in information om cyberangrepp,

   ii) utföra säkerhetsövervakning, inbegripet upptäckt av intrång och bedömning av sårbarheter i nät- och informationssystem,

   iii) analysera och vid behov vidta alla åtgärder som krävs enligt dess ansvar och kapacitet för att skydda entiteten,

   iv) delta i den insamling och delning av information som beskrivs i denna artikel.

b) Ha rätt att upphandla hela eller delar av denna förmåga i enlighet med led a genom leverantörer av utlokaliserade säkerhetstjänster (MSSP). Entiteter med kritisk och stor påverkan ska förbli ansvariga för leverantörer av utlokaliserade säkerhetstjänster och övervaka deras insatser.

c) Utse en gemensam kontaktpunkt på entitetsnivå för informationsdelning.

2. Enisa får utfärda icke-bindande vägledning om inrättande av sådan förmåga eller om att lägga ut tjänsten på entreprenad till leverantörer av utlokaliserade säkerhetstjänster, som en del av den uppgift som definieras i artikel 6.2 i förordning (EU) 2019/881.

3. Varje entitet med kritisk och stor påverkan ska dela relevant information om ett rapporteringspliktigt cyberangrepp med sina CSIRT-enheter och sin behöriga myndighet utan onödigt dröjsmål och senast fyra timmar efter att ha blivit medveten om att incidenten är rapporteringspliktig.

4. Information som rör ett cyberangrepp ska anses vara rapporteringspliktig när cyberangreppet i den berörda entitetens bedömning ger en kritikalitet som sträcker sig från ”hög” till ”kritisk” enligt metoden med en klassificeringsskala för cyberangrepp i enlighet med artikel 37.8. Den gemensamma kontaktpunkt på entitetsnivå som utsetts i enlighet med punkt 1 c ska informera om incidentklassificeringen.

5. Om entiteter med kritisk och stor påverkan anmäler relevant information om ej avhjälpta, aktivt utnyttjade sårbarheter till en CSIRT-enhet, får den senare vidarebefordra denna information till sin behöriga myndighet. Mot bakgrund av den anmälda informationens känslighetsnivå får CSIRT-enheten hålla inne informationen eller skjuta upp dess vidarebefordran av cybersäkerhetsmotiverade skäl.

6. Varje entitet med kritisk och stor påverkan ska utan onödigt dröjsmål tillhandahålla sina CSIRT-enheter all information som rör ett rapporteringspliktigt cyberhot som kan ha en gränsöverskridande påverkan. Information som rör ett cyberhot ska anses vara rapporteringspliktig om minst ett av följande villkor är uppfyllt:

a) Informationen är relevant för andra entiteter med kritisk och stor påverkan för att förebygga, upptäcka, reagera på eller begränsa påverkan av risken.

b) De identifierade typer av teknik, taktik och förfaranden som används i samband med ett angrepp leder fram till information såsom hackade URL- eller IP-adresser, hashvärden eller något annat attribut som är användbart för att kontextualisera och korrelera angreppet.

c) Ett cyberhot kan bedömas ytterligare och kontextualiseras med ytterligare information som tillhandahålls av tjänsteleverantörer eller tredje parter som inte omfattas av denna förordning.

7. Varje entitet med kritisk och stor påverkan ska, när den delar information i enlighet med denna artikel, specificera följande:

a) Att informationen lämnas i enlighet med denna förordning.

b) Huruvida informationen avser

   i) ett rapporteringspliktigt cyberangrepp som avses i punkt 3,

   ii) ej avhjälpta, aktivt utnyttjade sårbarheter som inte är allmänt kända och som avses i punkt 4,

   iii) ett rapporteringspliktigt cyberangrepp som avses i punkt 5.

c) Vid ett rapporteringspliktigt cyberangrepp, nivån på cyberangreppet enligt den metod med en klassificeringsskala för cyberangrepp som avses i artikel 37.8 och information som leder till denna klassificering, inbegripet åtminstone cyberangreppets kritikalitet.

8. När en entitet med kritisk eller stor påverkan anmäler en betydande incident i enlighet med artikel 23 i direktiv (EU) 2022/2555 och incidentrapporteringen enligt den artikeln innehåller relevant information i enlighet med punkt 3 i den här artikeln, ska entitetens rapportering enligt artikel 23.1 i det direktivet utgöra rapportering av information enligt punkt 3 i den här artikeln.

9. Varje entitet med kritisk och stor påverkan ska rapportera till sin behöriga myndighet eller CSIRT-enhet genom att tydligt identifiera specifik information som endast ska delas med den behöriga myndigheten eller CSIRT-enheten i fall där informationsdelningen skulle kunna vara källan till ett cyberangrepp. Varje entitet med kritisk och stor påverkan ska ha rätt att lämna en icke-konfidentiell version av informationen till den behöriga CSIRT-enheten.

Artikel 39

Upptäckt av cyberangrepp och hantering av tillhörande information

1. Entiteter med kritisk och stor påverkan ska utveckla den förmåga som krävs för att hantera upptäckta cyberangrepp med nödvändigt stöd från den relevanta behöriga myndigheten, Entso för el och EU DSO-enheten. Entiteterna med kritisk och stor påverkan får stödjas av den CSIRT-enhet som utsetts i deras respektive medlemsstat som en del av den uppgift som CSIRT-enheterna tilldelas genom artikel 11.5 a i direktiv (EU) 2022/2555. Entiteterna med kritisk och stor påverkan ska införa effektiva processer för att identifiera, klassificera och reagera på cyberangrepp som kommer att påverka eller kan påverka gränsöverskridande elflöden, i syfte att minimera deras påverkan.

2. Om ett cyberangrepp påverkar de gränsöverskridande elflödena, ska de gemensamma kontaktpunkterna på entitetsnivå för de berörda entiteterna med kritisk och stor påverkan samarbeta kring en ömsesidig informationsdelning, som ska samordnas av den behöriga myndigheten i den medlemsstat där cyberangreppet först rapporterades.

3. Entiteterna med kritisk och stor påverkan ska göra följande:

a) Säkerställa att deras egen gemensamma kontaktpunkt på entitetsnivå har åtkomst utifrån principen om behovsenlig behörighet till den information de tog emot från den nationella gemensamma kontaktpunkten via sin behöriga myndighet.

b) Om det inte redan har utförts i enlighet med artikel 3.4 i direktiv (EU) 2022/2555, tillhandahålla den behöriga myndigheten i den medlemsstat där de är etablerade och den nationella gemensamma kontaktpunkten en förteckning över deras gemensamma kontaktpunkter för cybersäkerhet på entitetsnivå

   i) från vilka den behöriga myndigheten och den nationella gemensamma kontaktpunkten kan förvänta sig att ta emot information om rapporteringspliktiga cyberangrepp,

   ii) till vilka behöriga myndigheter och nationella gemensamma kontaktpunkter kan behöva lämna information.

c) Inrätta förfaranden för hantering av cyberangrepp, inbegripet roller och ansvarsområden, uppgifter och reaktioner på grundval av den observerbara utvecklingen av cyberangreppet inom områdena med kritisk och stor påverkan.

d) Testa de övergripande förfarandena för hantering av cyberangrepp minst varje år genom att testa åtminstone ett scenario som direkt eller indirekt påverkar de gränsöverskridande elflödena. Det årliga testet får utföras av entiteter med kritisk och stor påverkan under de regelbundna övningar som avses i artikel 43. Alla insatser mot cyberangrepp i realtid med en konsekvens som klassificeras som minst skala 2, enligt metoden med en klassificeringsskala för cyberangrepp som avses i artikel 37.8 och där cybersäkerhet är en grundorsak, kan fungera som ett årligt test av planen för hantering av cyberangrepp.

4. Medlemsstaterna får delegera de uppgifter som avses i punkt 1 även till de regionala samordningscentrumen i enlighet med artikel 37.2 i förordning (EU) 2019/943.

Artikel 40

Krishantering

1. När den behöriga myndigheten konstaterar att en elkris är kopplad till ett cyberangrepp som påverkar mer än en medlemsstat, ska de behöriga myndigheterna i de berörda medlemsstaterna, de behöriga myndigheterna med ansvar för cybersäkerhet, den behöriga myndigheten med ansvar för riskberedskap och NIS-cyberkrishanteringsmyndigheterna i de berörda medlemsstaterna gemensamt inrätta en tillfällig gränsöverskridande krissamordningsgrupp.

2. Den tillfälliga gränsöverskridande krissamordningsgruppen ska

a) samordna effektiv hämtning av all relevant cybersäkerhetsinformation och vidarespridning av denna till de entiteter som deltar i krishanteringsprocessen,

b) organisera kommunikationen mellan alla entiteter som påverkas av krisen och de behöriga myndigheterna, i syfte att minska överlappningar och öka effektiviteten i analyserna och de tekniska insatserna för att avhjälpa de samtidiga elkriser där cybersäkerhet är en grundorsak,

c) i samarbete med de behöriga CSIRT-enheterna tillhandahålla den sakkunskap som krävs, inbegripet operativ rådgivning om genomförandet av eventuella begränsningsåtgärder hos de entiteter som påverkas av incidenten,

d) anmäla och tillhandahålla regelbundna uppdateringar om incidentens tillstånd till kommissionen och gruppen för samordning på elområdet, i enlighet med de skyddsprinciper som fastställs i artikel 46,

e) söka råd från relevanta myndigheter, byråer eller entiteter som kan bidra till att begränsa elkrisen.

3. Om cyberangreppet uppfyller kraven för eller förväntas uppfylla kraven för en storskalig cybersäkerhetsincident, ska den tillfälliga gränsöverskridande krissamordningsgruppen omedelbart informera de nationella cyberkrishanteringsmyndigheterna i enlighet med artikel 9.1 i direktiv (EU) 2022/2555 i de medlemsstater som påverkas av incidenten samt kommissionen och EU CyCLONe. I en sådan situation ska den tillfälliga gränsöverskridande krissamordningsgruppen stödja EU CyCLONe när det gäller sektorsspecifika särdrag.

4. Entiteter med kritisk och stor påverkan ska utveckla och förfoga över förmåga, interna riktlinjer, beredskapsplaner och personal för att delta i upptäckt och begränsning av gränsöverskridande kriser. Den entitet med kritisk eller stor påverkan som drabbas av en samtidig elkris ska undersöka grundorsaken till denna kris i samarbete med sin behöriga myndighet för att fastställa i vilken utsträckning krisen är kopplad till ett cyberangrepp.

5. Medlemsstaterna får delegera uppgifterna i punkt 4 även till de regionala samordningscentrumen i enlighet med artikel 37.2 i förordning (EU) 2019/943.

Artikel 41

Planer för hantering av cybersäkerhetskriser

1. Inom 24 månader från anmälan till Acer av rapporten om den unionsomfattande bedömningen av cybersäkerhetsrisker ska Acer i nära samarbete med Enisa, Entso för el, EU DSO-enheten, de behöriga myndigheterna med ansvar för cybersäkerhet, de behöriga myndigheterna, de behöriga myndigheterna med ansvar för riskberedskap, de nationella tillsynsmyndigheterna och de nationella NIS-cyberkrishanteringsmyndigheterna, utarbeta en plan för hantering av cybersäkerhetskriser på unionsnivå för elsektorn.

2. Inom 12 månader från Acers utarbetande av planen för hantering av cybersäkerhetskriser på unionsnivå för elsektorn i enlighet med punkt 1 ska varje behörig myndighet utarbeta en nationell plan för hantering av cybersäkerhetskriser för gränsöverskridande elflöden, med beaktande av planen för hantering av cybersäkerhetskriser på unionsnivå och den nationella riskberedskapsplan som inrättats i enlighet med artikel 10 i förordning (EU) 2019/941. Denna plan ska vara förenlig med planen för hantering av storskaliga cybersäkerhetsincidenter i enlighet med artikel 9.4 i direktiv (EU) 2022/2555. Den behöriga myndigheten ska samordna med entiteterna med kritisk och stor påverkan och med den behöriga myndigheten med ansvar för riskberedskap i sin medlemsstat.

3. Den nationella plan för hantering av storskaliga cybersäkerhetsincidenter som krävs enligt artikel 9.4 i direktiv (EU) 2022/2555 ska betraktas som en nationell plan för hantering av cybersäkerhetskriser enligt den här artikeln, om den omfattar bestämmelser om hantering av kriser för de gränsöverskridande elflödena.

4. Medlemsstaterna får delegera de uppgifter som förtecknas i punkterna 1 och 2 även till de regionala samordningscentrumen i enlighet med artikel 37.2 i förordning (EU) 2019/943.

5. Entiteterna med kritisk och stor påverkan ska säkerställa att deras cybersäkerhetsrelaterade krishanteringsprocesser

a) har kompatibla förfaranden för hantering av gränsöverskridande cybersäkerhetsincidenter i enlighet med definitionen i artikel 6.8 i direktiv (EU) 2022/2555 formellt införlivade i sina krishanteringsplaner,

b) ingår i den allmänna krishanteringsverksamheten.

6. Inom 12 månader från det att entiteterna med stor och kritisk påverkan underrättats i enlighet med artikel 24.6, och därefter vart tredje år, ska entiteter med kritisk och stor påverkan utarbeta en krishanteringsplan på entitetsnivå för en cybersäkerhetsrelaterad kris, och den planen ska ingå i deras allmänna krishanteringsplaner. Denna plan ska omfatta minst följande:

a) Regler för tillkännagivande av krisen enligt artikel 14.2 och 14.3 i förordning (EU) 2019/941.

b) Tydliga roller och ansvarsområden för krishantering, inbegripet rollen för andra relevanta entiteter med kritisk och stor påverkan.

c) Uppdaterad kontaktinformation samt regler för kommunikation och informationsdelning i en krissituation, inbegripet förbindelsen till CSIRT-enheterna.

7. Åtgärderna för krishantering enligt artikel 21.2 c i direktiv (EU) 2022/2555 ska betraktas som en krishanteringsplan på entitetsnivå för elsektorn enligt den här artikeln, om den uppfyller alla krav som förtecknas i punkt 6.

8. Krishanteringsplanerna ska testas under de cybersäkerhetsövningar som avses i artiklarna 43, 44 och 45.

9. Entiteterna med kritisk och stor påverkan ska inkludera sina krishanteringsplaner på entitetsnivå i sina kontinuitetsplaner för processerna med kritisk och stor påverkan. Krishanteringsplanerna på entitetsnivå ska omfatta följande:

a) Processer som är beroende av it-tjänsternas tillgänglighet, integritet och tillförlitlighet.

b) Alla platser som är nödvändiga för verksamhetens kontinuitet, inbegripet platser för maskinvara och programvara.

c) Alla interna roller och ansvarsområden som är kopplade till de processer som är nödvändiga för verksamhetens kontinuitet.

10. Entiteterna med kritisk och stor påverkan ska uppdatera sina krishanteringsplaner på entitetsnivå minst vart tredje år och när så är nödvändigt.

11. Acer ska uppdatera den plan för hantering av cybersäkerhetskriser på unionsnivå för elsektorn som utarbetats i enlighet med punkt 1 minst vart tredje år och när så är nödvändigt.

12. Varje behörig myndighet ska uppdatera den nationella planen för hantering av cybersäkerhetskriser för gränsöverskridande elflöden som utarbetats i enlighet med punkt 2 minst vart tredje år och när så är nödvändigt.

13. Entiteter med kritisk och stor påverkan ska testa sina kontinuitetsplaner minst vart tredje år eller efter större förändringar i en process med kritisk påverkan. Resultatet av testerna av kontinuitetsplanen ska dokumenteras. Entiteterna med kritisk och stor påverkan får inkludera testet av sin kontinuitetsplan i cybersäkerhetsövningarna.

14. Entiteterna med kritisk och stor påverkan ska uppdatera sin kontinuitetsplan när så är nödvändigt och minst en gång vart tredje år med beaktande av testets resultat.

15. Om det vid ett test identifieras brister i kontinuitetsplanen ska entiteten med kritisk och stor påverkan korrigera dessa inom 180 kalenderdagar från provningen och genomföra ett nytt test för att visa att de korrigerande åtgärderna är effektiva.

16. Om en entitet med kritisk och stor påverkan inte kan korrigera bristerna inom 180 kalenderdagar, ska den inkludera skälen i den rapport som ska lämnas till dess behöriga myndighet i enlighet med artikel 27.

Artikel 42

Förmåga till förvarning på cybersäkerhetsområdet för elsektorn

1. De behöriga myndigheterna ska samarbeta med Enisa för att utveckla en förmåga till förvarning på cybersäkerhetsområdet för elsektorn (ECEAC, *Electricity Cybersecurity Early Alert Capabilities*) som en del av biståndet till medlemsstaterna i enlighet med artikel 6.2 och 6.7 i förordning (EU) 2019/881.

2. Förmågan till förvarning på cybersäkerhetsområdet för elsektorn ska göra det möjligt för Enisa, vid utförandet av de uppgifter som anges i artikel 7.7 i förordning (EU) 2019/881, att

a) samla in information som delas på frivillig basis av

   i) CSIRT-enheter, behöriga myndigheter,

   ii) de entiteter som förtecknas i artikel 2 i denna förordning,

   iii) varje annan entitet som vill dela relevant information på frivillig basis,

b) bedöma och klassificera den insamlade informationen,

c) bedöma den information som Enisa har åtkomst till, för att identifiera villkor för cyberrisker och relevanta indikatorer för aspekter av gränsöverskridande elflöden,

d) identifiera villkor och indikatorer som ofta korrelerar med cyberangrepp inom elsektorn,

e) genom en bedömning och identifiering av riskfaktorerna, fastställa om det ska utföras ytterligare analyser och förebyggande åtgärder,

f) informera de behöriga myndigheterna om identifierade risker och rekommenderade förebyggande åtgärder som är specifika för de berörda entiteterna,

g) informera alla relevanta entiteter som förtecknas i artikel 2 om resultaten från bedömningen av information i enlighet med leden b, c och d i denna punkt,

h) regelbundet inkludera relevant information i den rapport om situationsmedvetenheten som utfärdas i enlighet med artikel 7.6 i förordning (EU) 2019/881,

i) härleda, när så är möjligt, tillämpliga data från den insamlade informationen som indikerar att en säkerhetsöverträdelse eller ett cyberangrepp kan föreligga (*angreppsindikatorer*).

3. CSIRT-enheterna ska utan dröjsmål sprida den information som mottagits från Enisa till de berörda entiteterna, vilket omfattas av deras uppgifter som fastställs i artikel 11.3 b i direktiv (EU) 2022/2555.

4. Acer ska övervaka effektiviteten avseende förmågan till förvarning på cybersäkerhetsområdet för elsektorn. Enisa ska bistå Acer genom att tillhandahålla all nödvändig information i enlighet med artiklarna 6.2 och 7.1 i förordning (EU) 2019/881. Analysen av denna övervakningsverksamhet ska ingå i övervakningen enligt artikel 12 i den här förordningen.

KAPITEL VI

RAM FÖR CYBERSÄKERHETSÖVNINGAR I ELSEKTORN

Artikel 43

Cybersäkerhetsövningar på entitets- och medlemsstatsnivå

1. Senast den 31 december året efter det att entiteterna med kritisk påverkan har underrättats, och därefter vart tredje år, ska varje entitet med kritisk påverkan genomföra en cybersäkerhetsövning som omfattar ett eller flera scenarier med cyberangrepp som direkt eller indirekt påverkar de gränsöverskridande elflödena och som rör de risker som identifierats under bedömningarna på medlemsstats- och entitetsnivå av cybersäkerhetsrisker i enlighet med artiklarna 20 och 27.

2. Genom undantag från punkt 1 får den behöriga myndigheten med ansvar för riskberedskap, efter samråd med den behöriga myndigheten och den relevanta cyberkrishanteringsmyndigheten, som utsetts eller inrättats i enlighet med artikel 9 i direktiv (EU) 2022/2555, besluta att organisera en cybersäkerhetsövning på medlemsstatsnivå enligt punkt 1 i stället för på entitetsnivå. I detta avseende ska den behöriga myndigheten informera

a) alla entiteter med kritisk påverkan i sin medlemsstat, den nationella tillsynsmyndigheten, CSIRT-enheterna och den behöriga myndigheten med ansvar för cybersäkerhet senast den 30 juni det år som föregår cybersäkerhetsövningen på entitetsnivå,

b) varje entitet som ska delta i cybersäkerhetsövningen på medlemsstatsnivå senast sex månader innan övningen ska äga rum.

3. Den behöriga myndigheten med ansvar för riskberedskap ska med tekniskt stöd från sina CSIRT-enheter organisera den cybersäkerhetsövning på medlemsstatsnivå som beskrivs i punkt 2, självständigt eller i samband med en annan cybersäkerhetsövning i den medlemsstaten. För att kunna gruppera dessa övningar får den behöriga myndigheten med ansvar för riskberedskap skjuta upp den i punkt 1 avsedda cybersäkerhetsövningen på medlemsstatsnivå ett år.

4. Cybersäkerhetsövningarna på entitetsnivå och på medlemsstatsnivå ska vara förenliga med de nationella ramarna för hantering av cybersäkerhetskriser i enlighet med artikel 9.4 d i direktiv (EU) 2022/2555.

5. Senast den 31 december 2026, och därefter vart tredje år, ska Entso för el, i samarbete med EU DSO-enheten, göra en mall för övningsscenarier tillgänglig för genomförande av cybersäkerhetsövningar på entitets- och medlemsstatsnivå i enlighet med punkt 1. Denna mall ska beakta resultaten av den senaste bedömningen på entitets- och medlemsstatsnivå av cybersäkerhetsrisker och ska innehålla centrala kriterier för en godkänd övning. Entso för el och EU DSO-enheten ska involvera Acer och Enisa i utarbetandet av en sådan mall.

Artikel 44

Regionala eller regionövergripande cybersäkerhetsövningar

1. Senast den 31 december 2029 och därefter vart tredje år ska Entso för el, i samarbete med EU DSO-enheten, organisera en regional cybersäkerhetsövning i varje systemdriftsregion. Entiteterna med kritisk påverkan i systemdriftsregionen ska delta i den regionala cybersäkerhetsövningen. Entso för el får, i samarbete med EU DSO-enheten, i stället för en regional cybersäkerhetsövning, organisera en regionövergripande cybersäkerhetsövning i mer än en systemdriftsregion inom samma tidsram. Övningen ska ta hänsyn till andra befintliga bedömningar av och scenarier för cybersäkerhetsrisker som utarbetats på unionsnivå.

2. Enisa ska bistå Entso för el och EU DSO-enheten i förberedelserna och organisationen av cybersäkerhetsövningen på regional eller regionövergripande nivå.

3. Entso för el ska, i samordning med EU DSO-enheten, informera de entiteter med kritisk påverkan som ska delta i den regionala eller regionövergripande cybersäkerhetsövningen sex månader innan övningen äger rum.

4. En organisatör av en regelbunden cybersäkerhetsövning på unionsnivå i enlighet med artikel 7.5 i förordning (EU) 2019/881, eller av en obligatorisk cybersäkerhetsövning som rör elsektorn inom samma geografiska område, får bjuda in Entso för el och EU DSO-enheten att delta. I sådana fall gäller inte skyldigheten i punkt 1, förutsatt att alla entiteter med kritisk påverkan i systemdriftsregionen deltar i samma övning.

5. Om Entso för el och EU DSO-enheten deltar i en cybersäkerhetsövning som avses i punkt 4, får de skjuta upp den i punkt 1 avsedda regionala eller regionövergripande cybersäkerhetsövningen ett år.

6. Senast den 31 december 2027, och vart tredje år därefter, ska Entso för el, i samordning med EU DSO-enheten, göra en övningsmall tillgänglig för genomförandet av de regionala och regionövergripande cybersäkerhetsövningarna. Denna mall ska beakta resultaten av den senaste bedömningen på regional nivå av cybersäkerhetsrisker och ska innehålla centrala kriterier för en godkänd övning. Entso för el ska samråda med kommissionen och får rådfråga Acer, Enisa och gemensamma forskningscentrumet om organisationen och genomförandet av regionala och regionövergripande cybersäkerhetsövningar.

Artikel 45

Resultat av cybersäkerhetsövningar på entitetsnivå, medlemsstatsnivå, regional eller regionövergripande nivå

1. På begäran av en entitet med kritisk påverkan ska leverantörer av kritiska tjänster delta i de cybersäkerhetsövningar som avses i artikel 43.1 och 43.2 och i artikel 44.1 när de tillhandahåller tjänster till entiteten med kritisk påverkan i det område som motsvarar omfattningen av den relevanta cybersäkerhetsövningen.

2. Organisatörerna av de cybersäkerhetsövningar som avses i artikel 43.1 och 2 och artikel 44.1 ska, med rådgivning av Enisa om de så begär och i enlighet med artikel 7.5 i förordning (EU) 2019/881, analysera och avsluta den relevanta cybersäkerhetsövningen genom en rapport som sammanfattar lärdomarna och riktar sig till alla deltagare. Denna rapport ska innehålla följande:

a) Övningsscenarier, mötesrapporter, huvudståndpunkter, godkända resultat och lärdomar på alla nivåer i värdekedjan för el.

b) Information om huruvida de centrala kriterierna för en godkänd övning uppfylldes.

c) En förteckning med rekommendationer till de entiteter som deltog i den relevanta cybersäkerhetsövningen om att korrigera, anpassa eller ändra processer, förfaranden, tillhörande styrningsmodeller och eventuella befintliga avtalsmässiga åtaganden med leverantörer av kritiska tjänster.

3. På begäran av CSIRT-nätverket eller samarbetsgruppen för nät- och informationssäkerhet eller EU CyCLONe ska organisatörerna av de cybersäkerhetsövningar som avses i artikel 43.1 och 43.2 och i artikel 44.1 dela med sig av resultatet av den relevanta cybersäkerhetsövningen. Organisatörerna ska dela med sig av den information som avses i punkt 2 a och b i denna artikel till varje entitet som deltar i övningarna. Organisatörerna ska dela med sig av den förteckning med rekommendationer som avses i led c uteslutande till de entiteter som rekommendationerna riktar sig till.

4. Organisatörerna av de cybersäkerhetsövningar som avses i artikel 43.1 och 43.2 och i artikel 44.1 ska regelbundet göra en uppföljning med de entiteter som deltar i övningarna när det gäller genomförandet av rekommendationerna i enlighet med punkt 2 c i denna artikel.

KAPITEL VII

SKYDD AV INFORMATION

Artikel 46

Principer för skydd av information i samband med informationsutbyte

1. De entiteter som förtecknas i artikel 2.1 ska säkerställa att information som tillhandahålls, tas emot, utbyts eller överförs enligt denna förordning endast är åtkomlig på grundval av behovsenlig behörighet och i enlighet med relevanta unionsbestämmelser och nationella bestämmelser om informationssäkerhet.

2. De entiteter som förtecknas i artikel 2.1 ska säkerställa att information som tillhandahålls, tas emot, utbyts eller överförs enligt denna förordning hanteras och spåras under informationens hela livscykel och att den får lämnas ut i slutet av dess livscykel först efter att ha anonymiserats.

3. De entiteter som förtecknas i artikel 2.1 ska säkerställa att alla nödvändiga skyddsåtgärder av organisatorisk och teknisk karaktär finns på plats för att skydda konfidentialiteten, integriteten, tillgängligheten och oavvisligheten hos den information som tillhandahålls, tas emot, utbyts eller överförs enligt denna förordning, oberoende av vilka medel som används. Skyddsåtgärderna ska

a) vara proportionella,

b) beakta cybersäkerhetsrisker i samband med kända tidigare och framväxande hot som sådan information kan bli föremål för inom ramen för denna förordning,

c) i möjligaste mån grundas på nationella, europeiska eller internationella standarder och bästa praxis,

d) dokumenteras.

4. De entiteter som förtecknas i artikel 2.1 ska säkerställa att varje person som beviljas åtkomst till information som tillhandahålls, tas emot, utbyts eller överförs i enlighet med denna förordning informeras om de säkerhetsbestämmelser som är tillämpliga på entitetsnivå och om de åtgärder och förfaranden som är relevanta för skyddet av information. Dessa entiteter ska säkerställa att den berörda personen bekräftar ansvaret att skydda informationen i enlighet med de instruktioner som ges.

5. De entiteter som förtecknas i artikel 2.1 ska säkerställa att åtkomsten till information som tillhandahålls, tas emot, utbyts eller överförs i enlighet med denna förordning begränsas till personer

a) som är behöriga att få åtkomst till denna information på grundval av sina funktioner och att åtkomsten begränsas till utförandet av de tilldelade uppgifterna,

b) för vilka entiteten kunde bedöma etiska principer och integritetsprinciper, samt för vilka det inte finns några belägg för negativt resultat från en säkerhetsprövning för att utvärdera individens tillförlitlighet i enlighet med entitetens bästa praxis och standardiserade säkerhetskrav och, vid behov, med nationella lagar och andra författningar.

6. De entiteter som förtecknas i artikel 2.1 ska ha skriftligt samtycke från den fysiska eller juridiska person som ursprungligen skapade eller tillhandahöll informationen, innan informationen lämnas till en tredje part som inte omfattas av denna förordning.

7. En entitet som förtecknas i artikel 2.1 får anse att denna information ska delas utan att uppfylla kraven i punkterna 1 och 4 i denna artikel för att förhindra en samtidig elkris vars bakomliggande orsak är cybersäkerhet eller en gränsöverskridande kris inom unionen i en annan sektor. I sådana fall ska den

a) samråda med och bemyndigas av den behöriga myndigheten att dela med sig av sådan information,

b) anonymisera sådan information utan att förlora de uppgifter som är nödvändiga för att informera allmänheten om en överhängande och allvarlig risk för de gränsöverskridande elflödena och eventuella begränsande åtgärder,

c) skydda identiteten på initiativtagaren och på de entiteter som har behandlat sådan information enligt denna förordning.

8. Genom undantag från punkt 6 i denna artikel får de behöriga myndigheterna tillhandahålla information som tillhandahålls, tas emot, utbyts eller överförs enligt denna förordning till en tredje part som inte förtecknas i artikel 2.1 utan skriftligt förhandsgodkännande från initiativtagaren, men så snart som möjligt informera denne. Innan den berörda behöriga myndigheten lämnar ut information som tillhandahålls, tas emot, utbyts eller överförs enligt denna förordning till en tredje part som inte förtecknas i artikel 2.1, ska den på ett rimligt sätt säkerställa att den berörda tredje parten är medveten om gällande säkerhetsbestämmelser och få rimliga garantier för att den berörda tredje parten kan skydda den mottagna informationen i enlighet med punkterna 1–5 i denna artikel. Den behöriga myndigheten ska anonymisera sådan information utan att de uppgifter förloras som är nödvändiga för att informera allmänheten om en överhängande och allvarlig risk för gränsöverskridande elflöden och möjliga begränsande åtgärder samt skydda identiteten på initiativtagaren. I detta fall ska den tredje part som inte förtecknas i artikel 2.1 skydda den mottagna informationen i enlighet med bestämmelser som redan är i kraft på entitetsnivå eller, om detta inte är möjligt, de bestämmelser och instruktioner som tillhandahålls av den relevanta behöriga myndigheten.

9. Denna artikel är inte tillämplig på entiteter som inte förtecknas i artikel 2.1 och som tillhandahålls information i enlighet med punkt 6 i denna artikel. I detta fall ska punkt 7 i denna artikel tillämpas, eller får den behöriga myndigheten tillhandahålla den entiteten skriftliga bestämmelser som ska tillämpas i fall där information tas emot i enlighet med denna förordning.

Artikel 47

Konfidentialitet för information

1. All information som tillhandahålls, tas emot, utbyts eller överförs i enlighet med denna förordning ska omfattas av de villkor om tystnadsplikt som fastställs i punkterna 2–5 i denna artikel i denna förordning och kraven i artikel 65 i förordning (EU) 2019/943. All information som tillhandahålls, tas emot, utbyts eller överförs mellan entiteter som förtecknas i artikel 2 i denna förordning ska vid tillämpningen av denna förordning skyddas, med beaktande av den konfidentialitetsnivå som initiativtagaren tillämpar för informationen.

2. Tystnadsplikt ska gälla för de entiteter som förtecknas i artikel 2.

3. De behöriga myndigheterna med ansvar för cybersäkerhet, de nationella tillsynsmyndigheterna, de behöriga myndigheterna med ansvar för riskberedskap och CSIRT-enheterna ska utbyta all information som är nödvändig för att de ska kunna utföra sina uppgifter.

4. All information som tas emot, utbyts eller överförs mellan entiteter som förtecknas i artikel 2.1 för att genomföra artikel 23 ska anonymiseras och aggregeras.

5. Information som tas emot i tjänsten av en entitet eller myndighet som omfattas av denna förordning får inte lämnas ut till någon annan entitet eller myndighet, utan att det påverkar sådana fall som omfattas av nationell lagstiftning, de övriga bestämmelserna i denna förordning eller annan tillämplig unionslagstiftning.

6. Utan att det påverkar tillämpningen av nationell lagstiftning eller unionslagstiftning får en myndighet, en entitet eller en fysisk person som tar emot information enligt denna förordning inte använda den för något annat ändamål än att fullgöra sina skyldigheter enligt denna förordning.

7. Acer ska, efter samråd med Enisa, alla behöriga myndigheter, Entso för el och EU DSO-enheten, senast den 13 juni 2025 till alla entiteter som förtecknas i artikel 2.1 utfärda riktlinjer för informationsutbytesmekanismer, i synnerhet planerade kommunikationsflöden, och metoder för anonymisering och aggregering av information i syfte att genomföra denna artikel.

8. Information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser ska utbytas med kommissionen och andra relevanta myndigheter endast om ett sådant utbyte är nödvändigt för tillämpningen av denna förordning. Den information som utbyts ska begränsas till vad som är nödvändigt och proportionerligt för utbytets ändamål. Vid sådant utbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella intressen hos entiteter med kritisk och stor påverkan skyddas.

KAPITEL VIII

SLUTBESTÄMMELSER

Artikel 48

Tillfälliga bestämmelser

1. Fram till godkännandet av de villkor eller metoder som avses i artikel 6.2 eller de planer som avses i artikel 6.3 ska Entso för el, i samarbete med EU DSO-enheten, utarbeta icke-bindande vägledning om följande:

a) Ett preliminärt index för påverkan på cybersäkerheten för el (ECII) i enlighet med punkt 2 i denna artikel.

b) En preliminär förteckning över unionsomfattande processer med stor och kritisk påverkan i enlighet med punkt 4 i denna artikel.

c) En preliminär förteckning över europeiska och internationella standarder och kontroller som föreskrivs i nationell lagstiftning och som har relevans för cybersäkerhetsaspekter av gränsöverskridande elflöden i enlighet med punkt 6 i denna artikel.

2. Senast den 13 oktober 2024 ska Entso för el, i samarbete med EU DSO-enheten, utarbeta en rekommendation om ett preliminärt ECII. Entso för el ska, i samarbete med EU DSO-enheten, anmäla det rekommenderade preliminära ECII till de behöriga myndigheterna.

3. Fyra månader efter mottagandet av det rekommenderade preliminära ECII, eller senast den 13 februari 2025, ska de behöriga myndigheterna identifiera kandidater till entiteter med stor och kritisk påverkan i sin medlemsstat på grundval av det rekommenderade ECII, och utarbeta en preliminär förteckning över entiteter med stor och kritisk påverkan. De entiteter med stor och kritisk påverkan som identifieras i den preliminära förteckningen får frivilligt fullgöra sina skyldigheter enligt denna förordning på grundval av en försiktighetsprincip. Senast den 13 mars 2025 ska de behöriga myndigheterna underrätta de entiteter som anges i den preliminära förteckningen om att de har identifierats som en entitet med stor eller kritisk påverkan.

4. Senast den 13 december 2024 ska Entso för el, i samarbete med EU DSO-enheten, utarbeta en preliminär förteckning över unionsomfattande processer med stor och kritisk påverkan. De entiteter som underrättats i enlighet med punkt 3 och som frivilligt beslutar att fullgöra sina skyldigheter enligt denna förordning på grundval av en försiktighetsprincip ska använda den preliminära förteckningen över processer med stor och kritisk påverkan för att fastställa de preliminära områdena med stor och kritisk påverkan och för att fastställa vilka tillgångar som ska ingå i den första bedömningen på entitetsnivå av cybersäkerhetsrisker.

5. Senast den 13 september 2024 ska varje behörig myndighet i enlighet med artikel 4.1 tillhandahålla Entso för el och EU DSO-enheten en förteckning över den nationella lagstiftning som är relevant för cybersäkerhetsaspekter av gränsöverskridande elflöden.

6. Senast den 13 juni 2025 ska Entso för el, i samarbete med EU DSO-enheten, utarbeta en preliminär förteckning över europeiska och internationella standarder och kontroller som föreskrivs i nationell lagstiftning och som har relevans för cybersäkerhetsaspekter av gränsöverskridande elflöden, med beaktande av den information som tillhandahålls av de behöriga myndigheterna.

7. Den preliminära förteckningen över europeiska och internationella standarder och kontroller ska innehålla

a) europeiska och internationella standarder och nationell lagstiftning som ger vägledning om metoder för hantering av cybersäkerhetsrisker på entitetsnivå, och

b) cybersäkerhetskontroller som motsvarar de kontroller som förväntas ingå i cybersäkerhetskontrollerna på lägsta nivå och avancerad nivå.

8. Entso för el och EU DSO-enheten ska beakta synpunkterna från Enisa och Acer när de slutför den preliminära förteckningen över standarder. Entso för el och EU DSO-enheten ska offentliggöra den preliminära förteckningen över europeiska och internationella standarder och kontroller på sina webbplatser.

9. Entso för el och EU DSO-enheten ska samråda med Enisa och Acer om de förslag till icke-bindande riktlinjer som utarbetats i enlighet med punkt 1.

10. Fram till dess att cybersäkerhetskontroller på lägsta och avancerad nivå utvecklas i enlighet med artikel 29 och antas i enlighet med artikel 8 ska alla entiteter som förtecknas i artikel 2.1 sträva efter att gradvis tillämpa den icke-bindande vägledning som utarbetats i enlighet med punkt 1.

Artikel 49

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 11 mars 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande