2024/1366

24.5.2024.

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1366

od 11. ožujka 2024.

o dopuni Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća uspostavom mrežnog kodeksa sa sektorskim pravilima za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2019/943 Europskog parlamenta i Vijeća od 5. lipnja 2019. o unutarnjem tržištu električne energije ([1]), a posebno njezin članak 59. stavak 2. točku (e),

budući da:

(1) Upravljanje kibernetičkosigurnosnim rizicima izrazito je važno za održavanje sigurnosti opskrbe električnom energijom i osiguravanje visoke razine kibernetičke sigurnosti u elektroenergetskom sektoru.

(2) Digitalizacija i kibernetička sigurnost presudno su važne za pružanje osnovnih usluga pa su stoga od strateške važnosti za ključnu energetsku infrastrukturu.

(3) Direktivom (EU) 2022/2555 Europskog parlamenta i Vijeća ([2]) utvrđuju se mjere za visoku zajedničku razinu kibernetičke sigurnosti u cijeloj Uniji. Uredba (EU) 2019/941 Europskog parlamenta i Vijeća ([3]) je dopuna Direktive (EU) 2022/2555 kojom se osigurava da su kibernetičkosigurnosni incidenti u elektroenergetskom sektoru ispravno identificirani kao rizik i da u planovima za pripravnost na rizike postoje mjere kojima su ti incidenti ispravno obuhvaćeni. Uredbom (EU) 2019/943 dopunjuju se Direktiva (EU) 2022/2555 i Uredba (EU) 2019/941 utvrđivanjem posebnih pravila za elektroenergetski sektor na razini Unije. Osim toga, ovom se Delegiranom uredbom dopunjuju odredbe Direktive (EU) 2022/2555 o elektroenergetskom sektoru kad se odnose na prekogranične protoke električne energije.

(4) U kontekstu međusobno povezanih digitaliziranih elektroenergetskih sustava sprečavanje elektroenergetskih kriza povezanih s kibernetičkim napadima i upravljanje njima ne može se smatrati isključivo nacionalnom zadaćom. Trebalo bi u potpunosti razviti učinkovitije i jeftinije mjere putem regionalne suradnje i suradnje na razini Unije. Stoga su potrebni zajednički okvir pravila i bolje koordinirani postupci kako bi se osigurala učinkovita prekogranična suradnja država članica i drugih dionika u duhu veće transparentnosti, povjerenja i solidarnosti između država članica i nadležnih tijela odgovornih za električnu energiju i kibernetičku sigurnost.

(5) Za upravljanje kibernetičkosigurnosnim rizicima u području primjene ove Uredbe potreban je strukturirani proces koji uključuje, među ostalim, utvrđivanje rizika koje za prekogranične protoke električne energije predstavljaju kibernetički napadi, s njima povezane operativne procese i područja te odgovarajuće mehanizme kibernetičkosigurnosnih kontrola i provjera. Iako se planira da se sve to napravi u roku od nekoliko godina, svaki bi korak procesa trebao doprinijeti tome da se u ovom sektoru postigne visok zajednički stupanj kibernetičke sigurnosti i ublaže kibernetičkosigurnosni rizici. Svi sudionici u procesu trebali bi učiniti sve u svojoj moći kako bi što prije i bez nepotrebne odgode razvili i prihvatili metodologije, a u svakom slučaju najkasnije u rokovima utvrđenima u ovoj Uredbi.

([1]) SL L 158, 14.6.2019., str. 54.

([2]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

([3]) Uredba (EU) 2019/941 Europskog parlamenta i Vijeća od 5. lipnja 2019. o pripravnosti na rizike u sektoru električne energije i stavljanju izvan snage Direktive 2005/89/EZ (SL L 158, 14.6.2019., str. 1.).

(6) Procjene kibernetičkosigurnosnih rizika na razini Unije, država članica, regija i subjekata u ovoj Uredbi mogu se ograničiti na one zbog kibernetičkih napada kako su definirani u Uredbi (EU) 2022/2554 Europskog parlamenta i Vijeća ([4]), što isključuje, npr., fizičke napade, prirodne katastrofe i operativne ispade zbog gubitka infrastrukture ili ljudskih resursa. Rizici na razini Unije i regionalni rizici povezani s fizičkim napadima ili prirodnim katastrofama u području električne energije već su obuhvaćeni drugim postojećim zakonodavstvom Unije, uključujući članak 5. Uredbe (EU) 2019/941 ili Uredbu Komisije (EU) 2017/1485 ([5]). Direktivom (EU) 2022/2557 Europskog parlamenta i Vijeća ([6]) o otpornosti kritičnih subjekata nastoje se smanjiti ranjivosti i ojačati fizička otpornost kritičnih subjekata. Ta direktiva obuhvaća sve relevantne prirodne i ljudskim djelovanjem uzrokovane rizike koji mogu utjecati na pružanje ključnih usluga, uključujući nesreće, prirodne katastrofe, izvanredna stanja u području javnog zdravlja kao što su pandemije i hibridne ili druge neprijateljske prijetnje, među ostalim kaznena djela terorizma, infiltracija kriminala i sabotaža.

(7) Koncept „subjekti s velikim i kritičnim utjecajem” definiran u ovoj Uredbi je temelj za utvrđivanje opsega subjekata koji će podlijegati obvezama na temelju ove Uredbe. Cilj je pristupa u njezinim odredbama koji se temelji na procjeni rizika utvrditi procese, popratnu imovinu i subjekte koji njima upravljaju koji utječu na prekogranične protoke električne energije. Ti se subjekti mogu smatrati subjektima s „velikim utjecajem” ili „kritičnim utjecajem”, ovisno o stupnju utjecaja koji bi mogući kibernetički napadi imali na njihovu ulogu u funkcioniranju prekograničnih protoka električne energije. U članku 3. Direktive (EU) 2022/2555 utvrđuju se koncepti ključnih i važnih subjekata i kriteriji za utvrđivanje subjekata u tim kategorijama. Iako će se mnogi subjekti istodobno smatrati „ključnim” subjektima u smislu članka 3. Direktive (EU) 2022/2555 i subjektima s velikim ili kritičnim utjecajem u skladu s člankom 24. ove Uredbe, kriteriji utvrđeni u ovoj Uredbi odnose se samo na njihovu ulogu i utjecaj u procesima u elektroenergetskom sektoru koji utječu na prekogranične protoke, pri čemu se ne uzimaju u obzir kriteriji utvrđeni u članku 3. Direktive (EU) 2022/2555.

(8) Subjekti obuhvaćeni područjem primjene ove Uredbe, koji se smatraju subjektima s velikim ili kritičnim utjecajem u skladu s člankom 24. ove Uredbe i koji podliježu obvezama utvrđenima u njoj, prvenstveno su subjekti koji imaju izravan utjecaj na prekogranične protoke električne energije u EU-u.

(9) U ovoj se Uredbi koriste postojeći mehanizmi i instrumenti, koji su već uspostavljeni drugim zakonodavstvima, kako bi se osigurala učinkovitost i izbjeglo udvostručavanje mjera potrebnih za postizanje ciljeva.

(10) Pri primjeni ove Uredbe države članice, relevantna tijela i operatori sustava trebali bi uzeti u obzir dogovorene europske norme i tehničke specifikacije europskih organizacija za normizaciju i djelovati u skladu sa zakonodavstvom Unije koje se odnosi na stavljanje na tržište ili u uporabu proizvoda obuhvaćenih tim zakonodavstvom Unije.

([4]) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1.).

([5]) Uredba Komisije (EU) 2017/1485 od 2. kolovoza 2017. o uspostavljanju smjernica za pogon elektroenergetskog prijenosnog sustava (SL L 220, 25.8.2017., str. 1.).

([6]) Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L 333, 27.12.2022., str. 164.).

(11) Kako bi se ublažili kibernetičkosigurnosni rizici, potrebno je uspostaviti detaljan pravilnik o mjerama i suradnji među relevantnim dionicima čije se aktivnosti odnose na kibernetičkosigurnosne aspekte prekograničnih protoka električne energije radi osiguravanja sigurnosti sustava. Ta bi organizacijska i tehnička pravila trebala osigurati da se većina elektroenergetskih incidenata čiji su temeljni uzroci povezani s kibernetičkom sigurnošću djelotvorno rješava na operativnoj razini. Potrebno je utvrditi što bi ti relevantni dionici trebali učiniti kako bi spriječili takve krize i koje mjere mogu poduzeti ako pravila o radu sustava više nisu dovoljna. Stoga je potrebno uspostaviti zajednički okvir pravila o tome kako spriječiti istodobne elektroenergetske krize čiji su temeljni uzroci povezani s kibernetičkom sigurnošću, pripremiti se za njih i upravljati njima. Time se povećava transparentnost u pripremnoj fazi i tijekom istodobne elektroenergetske krize te osigurava koordinirano i djelotvorno poduzimanje mjera zajedno s tijelima nadležnima za kibernetičku sigurnost u državama članicama. Od država članica i relevantnih subjekata trebalo bi zahtijevati da surađuju na regionalnoj razini i, prema potrebi, bilateralno, u duhu solidarnosti. Ta suradnja i pravila namijenjeni su postizanju bolje pripravnosti za kibernetičkosigurnosne rizike uz manje troškove i u skladu s ciljevima Direktive (EU) 2022/2555. Također se čini kako treba ojačati unutarnje tržište električne energije povećanjem povjerenja u državama članicama, posebno ublažavanjem rizika od neopravdanog ograničavanja prekograničnih protoka električne energije, čime se smanjuje rizik od negativnih učinaka prelijevanja na susjedne države članice.

(12) Sigurnost opskrbe električnom energijom podrazumijeva djelotvornu suradnju između država članica, institucija, tijela, ureda i agencija Unije te relevantnih dionika. Operatori distribucijskih sustava i operatori prijenosnih sustava imaju ključnu ulogu u osiguravanju sigurnog, pouzdanog i učinkovitog elektroenergetskog sustava u skladu s člancima 31. i 40. Direktive (EU) 2019/944 Europskog parlamenta i Vijeća ([7]). Različita regulatorna tijela i druga relevantna nadležna nacionalna tijela također imaju važnu ulogu u osiguravanju i praćenju kibernetičke sigurnosti u opskrbi električnom energijom u okviru zadaća koje su im dodijeljene direktivama (EU) 2019/944 i (EU) 2022/2555. Države članice trebale bi odrediti postojeći ili novi subjekt kao svoje nadležno nacionalno tijelo za provedbu ove Uredbe kako bi se osiguralo transparentno i uključivo sudjelovanje svih dionika, učinkovita priprema i pravilna provedba ove Uredbe, suradnja među različitim relevantnim dionicima i nadležnim tijelima u području električne energije i kibernetičke sigurnosti, kao i olakšavanje sprečavanja i *ex post* evaluacije elektroenergetskih kriza čiji su temeljni uzroci povezani s kibernetičkom sigurnošću i s tim povezane razmjene informacija.

(13) Ako subjekt s velikim utjecajem ili kritičnim utjecajem pruža usluge u više država članica ili ima sjedište ili drugi poslovni nastan ili predstavnika u državi članici, ali se njegovi mrežni i informacijski sustavi nalaze u jednoj ili više drugih država članica, te bi države članice trebale poticati svoja nadležna tijela da, prema potrebi, poduzmu sve što je u njihovoj moći da surađuju i međusobno si pomažu.

(14) Države članice trebale bi osigurati da nadležna tijela imaju potrebne ovlasti u odnosu na subjekte s velikim i kritičnim utjecajem radi promicanja usklađenosti s ovom Uredbom. Tim bi se ovlastima nadležnim tijelima trebalo omogućiti provođenje inspekcija na lokaciji i neizravnog nadzora. To može uključivati nasumične provjere, provođenje redovitih revizija, ciljanih revizija sigurnosti na temelju procjena rizika ili dostupnih informacija u vezi s rizikom i analiza sigurnosti povezanih s rizikom na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, što uključuje traženje informacija potrebnih za procjenu mjera kibernetičke sigurnosti koje je subjekt donio. Te bi informacije trebale uključivati dokumentirane politike kibernetičke sigurnosti, podatke o pristupu, dokumente ili sve informacije potrebne za obavljanje njihovih nadzornih zadaća i dokaze o provedbi politika kibernetičke sigurnosti, kao što su rezultati revizija sigurnosti koje je proveo kvalificirani revizor i odgovarajući temeljni dokazi.

([7]) Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14.6.2019., str. 125.).

(15) Kako bi se izbjegli nedostaci ili udvostručavanje obveza upravljanja kibernetičkosigurnosnim rizicima nametnutih subjektima s velikim i kritičnim utjecajem, nacionalna tijela na temelju Direktive (EU) 2022/2555 i nadležna tijela na temelju ove Uredbe trebala bi surađivati u provedbi mjera upravljanja tim rizicima i nadzoru usklađenosti s tim mjerama na nacionalnoj razini. Nadležna tijela na temelju Direktive (EU) 2022/2555 mogla bi smatrati usklađenost subjekta sa zahtjevima za upravljanje kibernetičkosigurnosnim rizicima utvrđenima u ovoj Uredbi kao osiguravanje usklađenosti s odgovarajućim zahtjevima utvrđenima u toj direktivi ili obrnuto.

(16) Za zajednički pristup istodobnom sprečavanju elektroenergetskih kriza i upravljanju njima potrebno je da države članice postignu zajedničko razumijevanje o tome što čini istodobnu elektroenergetsku krizu i kad je kibernetički napad važan čimbenik. Konkretno, trebalo bi olakšati koordinaciju među državama članicama i relevantnim subjektima radi rješavanja situacije u kojoj postoji potencijalni rizik od znatne nestašice električne energije ili nemogućnosti opskrbe kupaca električnom energijom, i to zbog kibernetičkog napada.

(17) U uvodnoj izjavi 1. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća ([8]) prepoznaje se važna uloga mrežnih i informacijskih sustava te elektroničkih komunikacijskih mreža i usluga za funkcioniranje gospodarstva u ključnim sektorima kao što je energetika, dok se u uvodnoj izjavi 44. objašnjava da bi Agencija Europske unije za kibersigurnost („ENISA”) trebala surađivati s Agencijom Europske unije za suradnju energetskih regulatora („ACER”).

(18) Uredbom (EU) 2019/943 dodjeljuju se posebne odgovornosti u pogledu kibernetičke sigurnosti operatorima prijenosnih sustava i operatorima distribucijskih sustava („ODS-ovi”). Njihova europska udruženja, odnosno europska mreža operatora prijenosnih sustava za električnu energiju („ENTSO za električnu energiju”) i europsko tijelo za ODS-ove („tijelo EU-a za ODS-ove”) promiču kibernetičku sigurnost u skladu s člancima 30. i 55. te uredbe u suradnji s relevantnim tijelima i reguliranim subjektima.

(19) Zajednički pristup sprečavanju i upravljanju istodobnim elektroenergetskim krizama čiji su temeljni uzroci povezani s kibernetičkom sigurnošću zahtijeva i da svi relevantni dionici primjenjuju usklađene metode i definicije kako bi utvrdili rizike povezane s kibernetičkom sigurnošću opskrbe električnom energijom. Također je potrebno moći učinkovito uspoređivati uspješnost tih zemalja i njihovih susjeda u tom području. Stoga je potrebno utvrditi postupke, uloge i odgovornosti za razvoj i ažuriranje metodologija upravljanja rizicima, ljestvice za klasifikaciju incidenata i mjere kibernetičke sigurnosti prilagođene kibernetičkosigurnosnim rizicima koji utječu na prekogranične protoke električne energije.

(20) Države članice putem nadležnog tijela imenovanog za potrebe ove Uredbe odgovorne su za utvrđivanje subjekata koji ispunjavaju kriterije da bi ih se smatralo subjektima s velikim i kritičnim utjecajem. Kako bi se uklonile razlike među državama članicama u tom pogledu i osigurala pravna sigurnost za mjere upravljanja kibernetičkosigurnosnim rizicima i obveze izvješćivanja za sve relevantne subjekte, trebalo bi uspostaviti skup kriterija za određivanje subjekata obuhvaćenih područjem primjene ove Uredbe. Taj skup kriterija trebalo bi definirati i redovito ažurirati tijekom postupka razvoja i donošenja odredaba, uvjeta i metodologija utvrđenih u ovoj Uredbi.

(21) Odredbama ove Uredbe ne bi se trebalo dovoditi u pitanje pravo Unije kojim se predviđaju posebna pravila o certifikaciji proizvoda informacijske i komunikacijske tehnologije („IKT”), IKT usluga i IKT procesa, posebno ne dovodeći u pitanje Uredbu (EU) 2019/881 u pogledu okvira za uspostavu europskog programa certifikacije kibernetičke sigurnosti. U kontekstu ove Uredbe IKT proizvodi trebali bi uključivati i tehničke uređaje i softver koji omogućuju izravnu interakciju s elektrotehničkom mrežom, posebno industrijske kontrolne sustave koji se mogu upotrebljavati za prijenos, distribuciju i proizvodnju energije, kao i za prikupljanje i prijenos povezanih informacija. Odredbama bi trebalo osigurati da IKT proizvodi, usluge i procesi koji se nabavljaju ispunjavaju relevantne sigurnosne ciljeve iz članka 51. Uredbe (EU) 2019/881.

([8]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

(22) Nedavni kibernetički napadi pokazuju da su subjekti sve češća meta napada u lancu opskrbe. Takvi napadi u lancu opskrbe ne utječu samo na pojedinačne subjekte obuhvaćene područjem primjene, već mogu imati i kaskadni utjecaj na veće napade na subjekte na koje su priključeni u elektroenergetskoj mreži. Stoga su dodane odredbe i preporuke za ublažavanje kibernetičkosigurnosnih rizika povezanih s procesima koji se odnose na lanac opskrbe, posebno nabavu, koji utječu na prekogranične protoke električne energije.

(23) Budući da iskorištavanje ranjivosti u mrežnim i informacijskim sustavima može uzrokovati znatne energetske poremećaje i štetu za gospodarstvo i potrošače, te bi ranjivosti trebalo brzo utvrditi i otkloniti kako bi se smanjili rizici. Kako bi se olakšala djelotvorna provedba ove Uredbe, relevantni subjekti i nadležna tijela trebali bi surađivati u izvršavanju i testiranju aktivnosti koje se smatraju primjerenima za tu svrhu, uključujući razmjenu informacija o kibernetičkim prijetnjama, kibernetičkim napadima, ranjivostima, alatima i metodama, taktikama, tehnikama i postupcima, pripravnosti za upravljanje kibernetičkosigurnosnim krizama i drugim vježbama. Budući da se tehnologija stalno razvija, a digitalizacija elektroenergetskog sektora brzo napreduje, provedba donesenih odredbi ne bi trebala imati negativne posljedice na inovacije i ne bi smjela činiti prepreku pristupu tržištu električne energije i naknadnoj upotrebi inovativnih rješenja koja doprinose učinkovitosti i održivosti elektroenergetskog sustava.

(24) Informacije prikupljene radi praćenja provedbe ove Uredbe trebale bi biti razumno ograničene na temelju načela nužnosti pristupa podacima. Dionicima bi trebalo omogućiti ostvarive i učinkovite rokove za podnošenje takvih informacija. Trebalo bi izbjegavati dvostruko obavješćivanje.

(25) Zaštita kibernetičke sigurnosti ne prestaje na granicama Unije. Kako bi sustav bio siguran, potrebno je sudjelovanje susjednih trećih zemalja. Unija i njezine države članice trebale bi nastojati podupirati susjedne treće zemlje čija je elektroenergetska infrastruktura priključena na europsku mrežu u primjeni pravila o kibernetičkoj sigurnosti sličnih onima utvrđenima u ovoj Uredbi.

(26) Kako bi se unaprijedila koordinacija sigurnosti i testirali budući obvezujući uvjeti i metodologije, ENTSO za električnu energiju, tijelo EU-a za ODS-ove i nadležna tijela trebali bi početi izrađivati neobvezujuće smjernice odmah nakon stupanja na snagu ove Uredbe. Te smjernice poslužit će kao osnova za razvoj budućih odredaba, uvjeta i metodologija. Istodobno, nadležna tijela trebala bi utvrditi subjekte koji su kandidati za subjekte s velikim i kritičnim utjecajem kako bi dobrovoljno započeli s ispunjavanjem obveza.

(27) Ova je Uredba razvijena u bliskoj suradnji s Agencijom za suradnju energetskih regulatora (ACER), ENISA-om, ENTSO-om za električnu energiju, tijelom EU-a za ODS-ove i drugim dionicima radi transparentnog i participativnog donošenja učinkovitih, uravnoteženih i razmjernih pravila.

(28) Ovom se Uredbom dopunjuju i poboljšavaju mjere za upravljanje krizama uspostavljene u sklopu okvira EU-a za odgovor na kiberkrize kako je utvrđen u Preporuci Komisije (EU) 2017/1584 ([9]). Kibernetički napad mogao bi i uzrokovati elektroenergetsku krizu, pridonijeti joj ili se dogoditi istodobno kad i takva kriza kako je definirana u članku 2. stavku 9. Uredbe (EU) 2019/941, uz utjecaj na prekogranične protoke električne energije. Ta elektroenergetska kriza mogla bi dovesti do istodobne elektroenergetske krize kako je definirana u članku 2. stavku 10. Uredbe (EU) 2019/941. Takav bi incident mogao utjecati i na druge sektore koji ovise o sigurnosti opskrbe električnom energijom. Ako takav incident eskalira u kibernetičkosigurnosni incident velikih razmjera u smislu članka 16. Direktive (EU) 2022/2555, trebale bi se primjenjivati odredbe tog članka kojima se uspostavlja europska mreža organizacija za vezu za kibernetičke krize („EU-CyCLONe”). Za upravljanje krizama na razini Unije relevantne stranke trebale bi koristiti aranžmane EU-a za integrirani politički odgovor na krizu na temelju Provedbene odluke Vijeća (EU) 2018/1993 („aranžmani za IPCR”) ([10]).

(29) Ova Uredba ne utječe na mogućnost država članica da poduzmu potrebne mjere za osiguravanje zaštite osnovnih interesa svoje sigurnosti, zaštitu javnog poretka i javne sigurnosti te omogućivanje istrage, otkrivanja i progona kaznenih djela, u skladu s pravom Unije. U skladu s člankom 346. UFEU-a nijedna država članica nije obvezna davati informacije ako smatra da bi njihovo otkrivanje bilo suprotno osnovnim interesima njezine javne sigurnosti.

([9]) Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

([10]) Provedbena odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu (SL L 320, 17.12.2018., str. 28.).

(30) Iako se ova Uredba primjenjuje na subjekte koji obavljaju djelatnosti proizvodnje električne energije iz nuklearnih elektrana, neke od tih djelatnosti mogu biti povezane s nacionalnom sigurnošću.

(31) Pravo Unije o zaštiti podataka i pravo Unije o zaštiti privatnosti primjenjuje se na svaku obradu osobnih podataka na temelju ove Uredbe. Konkretno, ovom se Uredbom ne dovode u pitanje Uredba (EU) 2016/679 Europskog parlamenta i Vijeća ([11]), Direktiva 2002/58/EZ ([12]) Europskog parlamenta i Vijeća ni Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća ([13]). Ova Uredba stoga ne bi trebala utjecati, među ostalim, na zadaće i ovlasti tijela nadležnih za praćenje usklađenosti s primjenjivim pravom Unije o zaštiti podataka i pravom Unije o zaštiti privatnosti.

(32) S obzirom na važnost međunarodne suradnje u području kibernetičke sigurnosti nadležna tijela odgovorna za obavljanje zadaća koje su im dodijeljene ovom Uredbom i koja su imenovale države članice trebala bi moći sudjelovati u međunarodnim mrežama suradnje. Stoga bi za potrebe obavljanja svojih zadaća nadležna tijela trebala moći razmjenjivati informacije, uključujući osobne podatke, s nadležnim tijelima trećih zemalja pod uvjetom da su ispunjeni uvjeti iz prava Unije o zaštiti podataka za prijenose osobnih podataka trećim zemljama, među ostalim uvjeti iz članka 49. Uredbe (EU) 2016/679.

(33) Obrada osobnih podataka u mjeri u kojoj je to potrebno i razmjerno za potrebe osiguravanja sigurnosti mrežnih i informacijskih sustava koju provode subjekti s velikim ili kritičnim utjecajem mogla bi se smatrati zakonitom na temelju toga što je takva obrada usklađena s pravnom obvezom kojoj podliježe voditelj obrade, a u skladu sa zahtjevima iz članka 6. stavka 1. točke (c) i članka 6. stavka 3. Uredbe (EU) 2016/679. Obrada osobnih podataka mogla bi biti potrebna i zbog legitimnih interesa subjekata s velikim ili kritičnim utjecajem, kao i pružatelja sigurnosnih tehnologija i usluga koji djeluju u ime tih subjekata, u skladu s člankom 6. stavkom 1. točkom (f) Uredbe (EU) 2016/679, među ostalim ako je takva obrada nužna za potrebe mehanizama razmjene informacija o kibernetičkoj sigurnosti ili dobrovoljno obavješćivanje o relevantnim informacijama u skladu s ovom Uredbom. Mjere za sprečavanje, otkrivanje, identifikaciju, suzbijanje, analizu i odgovor na kibernetičke napade, mjere za informiranje o određenim kibernetičkim prijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim kibernetičkim napadima, kibernetičkim prijetnjama i ranjivostima, pokazatelji ugroženosti, taktike, tehnike i postupci, kibernetičkosigurnosna upozorenja i konfiguracijski alati mogli bi zahtijevati obradu određenih kategorija osobnih podataka, kao što su IP adrese, jedinstveni lokatori resursa (URL-ovi), nazivi domena, e-adrese te vremenski žigovi ako se njima otkrivaju osobni podaci. Obrada osobnih podataka koju provode nadležna tijela, jedinstvene kontaktne točke i CSIRT-ovi mogla bi predstavljati pravnu obvezu ili se smatrati nužnom za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade podataka u skladu s člankom 6. stavkom 1. točkom (c) ili (e) te člankom 6. stavkom 3. Uredbe (EU) 2016/679 ili za ostvarivanje legitimnog interesa subjekata s velikim ili kritičnim utjecajem, kako je navedeno u članku 6. stavku 1. točki (f) te uredbe. Nadalje, nacionalnim pravom mogla bi se utvrditi pravila kojima se nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima, u mjeri u kojoj je to potrebno i razmjerno u svrhu jamčenja sigurnosti mrežnih i informacijskih sustava subjekata s velikim ili kritičnim utjecajem, omogućuje obrada posebnih kategorija osobnih podataka u skladu s člankom 9. Uredbe (EU) 2016/679, u prvom redu na temelju predviđanja odgovarajućih i posebnih mjera za zaštitu temeljnih prava i interesa fizičkih osoba, uključujući tehnička ograničenja ponovne uporabe takvih podataka i primjenu najsuvremenijih mjera sigurnosti i zaštite privatnosti, kao što su pseudonimizacija ili kriptiranje ako anonimizacija može znatno utjecati na svrhu koja se želi postići.

([11]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([12]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

([13]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

(34) U mnogim su slučajevima osobni podaci ugroženi zbog kibernetičkih napada. U tom kontekstu nadležna tijela trebala bi surađivati i razmjenjivati informacije o svim relevantnim pitanjima s tijelima iz Uredbe (EU) 2016/679 i Direktive 2002/58/EZ.

(35) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725, koji je dao mišljenje 17. studenog 2023.,

DONIJELA JE OVU UREDBU:

Poglavlje I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom uspostavlja mrežni kodeks kojim se utvrđuju sektorska pravila za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije, uključujući pravila o zajedničkim minimalnim zahtjevima, planiranju, praćenju, izvješćivanju i upravljanju krizama.

Članak 2.

Područje primjene

1. Ova se Uredba primjenjuje na kibernetičkosigurnosne aspekte prekograničnih protoka električne energije u aktivnostima sljedećih subjekata ako su ti subjekti utvrđeni kao subjekti s velikim ili kritičnim utjecajem u skladu s člankom 24.:

(a) elektroenergetska poduzeća kako su definirana u članku 2. stavku 57. Direktive (EU) 2019/944;

(b) nominirani operatori tržišta električne energije (NEMO-i) kako su definirani u članku 2. stavku 8. Uredbe (EU) 2019/943;

(c) organizirana tržišta kako su definirana u članku 2. stavku 4. Provedbene uredbe Komisije (EU) br. 1348/2014 ([14]) na kojima se dogovaraju transakcije proizvodima relevantnima za prekogranične protoke električne energije;

(d) ključni pružatelji IKT usluga iz članka 3. točke 9. ove Uredbe;

(e) ENTSO za električnu energiju osnovan na temelju članka 28. Uredbe (EU) 2019/943;

(f) tijelo EU-a za ODS-ove osnovano u skladu s člankom 52. Uredbe (EU) 2019/943;

(g) subjekti odgovorni za odstupanje kako su definirani u članku 2. točki 14. Uredbe (EU) 2019/943;

(h) operatori mjesta za punjenje kako su definirani u Prilogu I. Direktivi (EU) 2022/2555;

(i) regionalni koordinacijski centri kako su uspostavljeni u skladu s člankom 35. Uredbe (EU) 2019/943;

(j) pružatelji upravljanih sigurnosnih usluga kako su definirani u članku 6. stavku 40. Direktive (EU) 2022/2555;

(k) svi drugi subjekti ili treće strane s odgovornostima delegiranima ili dodijeljenima na temelju ove Uredbe.

2. Za obavljanje zadaća dodijeljenih ovom Uredbom odgovorna su u okviru svojih trenutačnih mandata sljedeća tijela:

(a) Agencija Europske unije za suradnju energetskih regulatora („ACER”), osnovana Uredbom (EU) 2019/942 Europskog parlamenta i Vijeća ([15]);

(b) nacionalna nadležna tijela odgovorna za obavljanje zadaća dodijeljenih na temelju ove Uredbe koja su imenovale države članice na temelju članka 4., odnosno „nadležna tijela”;

(c) nacionalna regulatorna tijela koja su imenovale pojedinačne države članice na temelju članka 57. stavkom 1. Direktive (EU) 2019/944;

([14]) Provedbena uredba Komisije (EU) br. 1348/2014 od 17. prosinca 2014. o izvješćivanju o podacima i provedbi članka 8. stavaka 2. i 6. Uredbe (EU) br. 1227/2011 Europskog parlamenta i Vijeća o cjelovitosti i transparentnosti veleprodajnog tržišta energije (SL L 363, 18.12.2014., str. 121.).

([15]) Uredba (EU) 2019/942 Europskog parlamenta i Vijeća od 5. lipnja 2019. o osnivanju Agencije Europske unije za suradnju energetskih regulatora (SL L 158, 14.6.2019., str. 22.).

(d) nadležna tijela za pripravnost za rizike osnovana na temelju članka 3. Uredbe (EU) 2019/941;

(e) timovi za odgovor na računalne sigurnosne incidente („CSIRT-ovi”) imenovani ili uspostavljeni na temelju članka 10. Direktive (EU) 2022/2555;

(f) nadležna tijela odgovorna za kibernetičku sigurnost imenovana ili uspostavljena na temelju članka 8. Direktive (EU) 2022/2555;

(g) Agencija Europske unije za kibersigurnost osnovana na temelju Uredbe (EU) 2019/881;

(h) sva druga tijela ili treće strane s odgovornostima delegiranima ili dodijeljenima na temelju članka 4. stavkom 3.

3. Ova se Uredba primjenjuje i na sve subjekte koji nemaju poslovni nastan u Uniji, ali koji pružaju usluge subjektima u Uniji, pod uvjetom da su ih nadležna tijela utvrdila kao subjekte s velikim ili kritičnim utjecajem u skladu s člankom 24. stavkom 2.

4. Ovom se Uredbom ne dovodi u pitanje odgovornost država članica za zaštitu nacionalne sigurnosti ni njihove ovlasti za zaštitu drugih temeljnih državnih funkcija, uključujući osiguravanje teritorijalne cjelovitosti države i održavanje javnog poretka.

5. Ovom se Uredbom ne dovodi u pitanje odgovornost država članica za zaštitu nacionalne sigurnosti s obzirom na aktivnosti u proizvodnji električne energije iz nuklearnih elektrana, uključujući aktivnosti unutar nuklearnog lanca vrijednosti u skladu s Ugovorima.

6. Subjekti, nadležna tijela, subjektove jedinstvene kontaktne točke i CSIRT-ovi obrađuju osobne podatke u mjeri u kojoj je to potrebno za svrhe ove Uredbe i u skladu s Uredbom (EU) 2016/679, pri čemu se takva obrada posebno oslanja na njezin članak 6.

Članak 3.

Definicije

Primjenjuju se sljedeće definicije:

(1) „imovina” znači svaki softver, informacija ili hardver u mrežnim i informacijskim sustavima, neovisno o tome je li materijalan ili nematerijalan, koji ima vrijednost za nekog pojedinca, organizaciju ili vladu;

(2) „nadležno tijelo za pripravnost za rizike” znači nadležno tijelo imenovano u skladu s člankom 3. Uredbe (EU) 2019/941;

(3) „tim za odgovor na računalne sigurnosne incidente” znači tim odgovoran za rješavanje rizika i incidenata u skladu s člankom 10. Direktive (EU) 2022/2555;

(4) „imovina s kritičnim utjecajem” znači imovina koja je potrebna za procese s kritičnim utjecajem;

(5) „subjekt s kritičnim utjecajem” znači subjekt koji vodi procese s kritičnim utjecajem kojeg su nadležna tijela utvrdila u skladu s člankom 24.;

(6) „područje od kritičnog utjecaja” znači područje koje utvrđuje subjekt iz članka 2. stavka 1. unutar kojeg se nalazi sva imovina s kritičnim utjecajem, unutar kojeg se može kontrolirati pristup toj imovini i unutar kojeg se primjenjuju napredne kontrole kibernetičke sigurnosti;

(7) „proces s kritičnim utjecajem” znači poslovni proces koji vodi subjekt čiji su indeksi utjecaja na kibernetičku sigurnost elektroenergetskog sektora iznad praga kritičnog utjecaja;

(8) „prag kritičnog utjecaja” znači vrijednosti indeksa utjecaja na kibernetičku sigurnost elektroenergetskog sektora iz članka 19. stavka 3. točke (b), iznad kojih će kibernetički napad na poslovni proces uzrokovati kritične poremećaje prekograničnih protoka električne energije;

(9) „ključni pružatelj IKT usluga” znači subjekt koji pruža IKT uslugu ili proces nužan za proces s kritičnim ili velikim utjecajem koji utječe na kibernetičkosigurnosne aspekte prekograničnih protoka električne energije i koji, ako je ugrožen, može dovesti do kibernetičkog napada s posljedicama iznad praga kritičnog ili velikog utjecaja;

(10) „prekogranični protok električne energije” znači prekogranični protok kako je definiran u članku 2. stavku 3. Uredbe (EU) 2019/943;

(11) „kibernetički napad” znači incident kako je definiran u članku 3. točki 14. Uredbe (EU) 2022/2554;

(12) „kibernetička sigurnost” znači kibernetička sigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881;

(13) „kontrola kibernetičke sigurnosti” znači radnje ili postupci koji se provode u svrhu izbjegavanja, otkrivanja, suzbijanja ili minimiziranja kibernetičkosigurnosnih rizika;

(14) „kibernetičkosigurnosni incident” znači incident kako je definiran u članku 6. točki 6. Direktive (EU) 2022/2555;

(15) „sustav za upravljanje kibernetičkom sigurnošću” znači politike, postupci, smjernice i povezani resursi i aktivnosti kojima subjekt zajednički upravlja radi zaštite svoje informacijske imovine od kibernetičkih prijetnji kojima se sustavno uspostavlja, uvodi, upravlja, prati, preispituje, održava i poboljšava sigurnost mrežnog i informacijskog sustava organizacije;

(16) „operativni centar za kibernetičku sigurnost” znači specijalizirani centar u kojem tehnički tim, koji se sastoji od najmanje jednog stručnjaka s potporom IT sustava za kibernetičku sigurnost, obavlja zadaće povezane sa sigurnošću (usluge operativnog centra za kibernetičku sigurnost („CSOC”)), kao što su odgovaranje na kibernetičke napade i pogreške u konfiguraciji sigurnosti, praćenje sigurnosti, analiza evidencijskih zapisa i otkrivanje kibernetičkih napada;

(17) „kibernetička prijetnja” znači kibernetička prijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;

(18) „upravljanje kibernetičkosigurnosnim ranjivostima” znači praksa utvrđivanja i uklanjanja ranjivosti;

(19) „subjekt” znači subjekt kako je definiran u članku 6. točki 38. Direktive (EU) 2022/2555;

(20) „rano uzbunjivanje” znači informacije potrebne za utvrđivanje sumnje da je ozbiljan incident uzrokovan nezakonitim ili zlonamjernim radnjama ili da bi mogao imati prekogranični utjecaj;

(21) „indeks utjecaja na kibernetičku sigurnost elektroenergetskog sektora” ili „ECII” znači indeks ili klasifikacijska ljestvica u kojoj se rangiraju moguće posljedice kibernetičkog napada na poslovne procese uključene u prekogranične protoke električne energije;

(22) „europski program certifikacije kibernetičke sigurnosti” znači program kako je definiran u članku 2. točki 9. Uredbe (EU) 2019/881;

(23) „subjekt s velikim utjecajem” znači subjekt koji vodi proces s velikim utjecajem kojeg su nadležna tijela utvrdila u skladu s člankom 24.;

(24) „proces s velikim utjecajem” znači svaki poslovni proces koji provodi subjekt čiji su indeksi utjecaja na kibernetičku sigurnost elektroenergetskog sektora iznad praga velikog utjecaja;

(25) „imovina s velikim utjecajem” znači imovina koja je potrebna za procese s velikim utjecajem;

(26) „prag velikog utjecaja” znači vrijednosti indeksa utjecaja na kibernetičku sigurnost elektroenergetskog sektora iz članka 19. stavka 3. točke (b) iznad kojih će uspješan kibernetički napad na proces uzrokovati velike poremećaje u prekograničnim protocima električne energije;

(27) „područje od velikog utjecaja” znači područje koje utvrđuje subjekt iz članka 2. stavka 1. unutar kojeg se nalazi sva imovina s velikim utjecajem, unutar kojeg se može kontrolirati pristup toj imovini i unutar kojeg se primjenjuju minimalne kontrole kibernetičke sigurnosti;

(28) „IKT proizvod” znači IKT proizvod kako je definiran u članku 2. točki 12. Uredbe (EU) 2019/881;

(29) „IKT usluga” znači IKT usluga kako je definirana u članku 2. točki 13. Uredbe (EU) 2019/881;

(30) „IKT proces” znači IKT proces kako je definiran u članku 2. točki 14. Uredbe (EU) 2019/881;

(31) „zastarjeli sustav” znači zastarjeli IKT sustav kako je definiran u članku 3. točki 3. Uredbe (EU) 2022/2554;

(32) „nacionalna jedinstvena kontaktna točka” znači jedinstvena kontaktna točka koju je država članica imenovala ili uspostavila u skladu s člankom 8. stavkom 3. Direktive (EU) 2022/2555;

(33) „tijela za upravljanje kibernetičkosigurnosnim krizama u području mrežne i informacijske sigurnosti” znači tijela imenovana ili uspostavljena u skladu s člankom 9. stavkom 1. Direktive (EU) 2022/2555;

(34) „inicijator” znači subjekt koji pokreće razmjenu, dijeljenje ili pohranu informacija;

(35) „specifikacije nabave” znači specifikacije koje subjekti definiraju za nabavu novih ili moderniziranih IKT proizvoda, procesa ili usluga;

(36) „zastupnik” znači fizička ili pravna osoba s poslovnim nastanom u Uniji koja je izričito imenovana da zastupa subjekta s velikim ili kritičnim utjecajem koji nema poslovni nastan u Uniji, ali koji pruža usluge subjektima u Uniji, i kojoj se nadležno tijelo ili CSIRT mogu obratiti umjesto samom subjektu s velikim odnosno kritičnim utjecajem u pogledu obveza tog subjekta na temelju ove Uredbe;

(37) „rizik” znači rizik kako je definiran u članku 6. točki 9. Direktive (EU) 2022/2555;

(38) „matrica utjecaja rizika” znači matrica koja u procjeni rizika služi kako bi se utvrdio stupanj posljedica svakog procijenjenog rizika;

(39) „istodobna elektroenergetska kriza” znači elektroenergetska kriza kako je definirana u članku 2. točki 10. Uredbe (EU) 2019/941;

(40) „subjektova jedinstvena kontaktna točka” znači jedinstvena točka za kontakt subjekta imenovana na temelju članka 38. stavka 1. točke (c);

(41) „dionik” znači svaka strana čiji je interes uspjeh i kontinuirano funkcioniranje organizacije ili procesa, npr. zaposlenici, direktori, dioničari, regulatorna tijela, udruženja, dobavljači i klijenti;

(42) „norma” znači norma kako je definirana u članku 2. stavku 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([16]);

(43) „regija pogona sustava” znači regije pogona sustava kako su definirane u Prilogu I. Odluci ACER-a 05-2022 o definiciji regija pogona sustava i uspostavljene u skladu s člankom 36. Uredbe (EU) 2019/943;

(44) „operatori sustava” znači „operator distribucijskog sustava” (ODS) i „operator prijenosnog sustava” (OPS) kako su definirani u članku 2. točkama 29. i 35. Direktive (EU) 2019/944;

(45) „proces s kritičnim utjecajem na razini Unije” znači svaki proces u elektroenergetskom sektoru, koji može uključivati više subjekata, za koji se u procjeni kibernetičkosigurnosnih rizika na razini Unije može smatrati da bi posljedice kibernetičkog napada na njega bile kritične;

(46) „proces s velikim utjecajem na razini Unije” znači svaki proces u elektroenergetskom sektoru, koji može uključivati više subjekata, za koji se u procjeni kibernetičkosigurnosnih rizika na razini Unije može smatrati da bi posljedice kibernetičkog napada na njega bile velike;

(47) „neuklonjena iskorištena ranjivost” znači ranjivost čije postojanje još nije javno otkriveno, a koja nije uklonjena i za koju postoje pouzdani dokazi da je akter izvršio zlonamjerni kod u sustavu bez dopuštenja vlasnika sustava;

(48) „ranjivost” znači ranjivost kako je definirana u članku 6. točki 15. Direktive (EU) 2022/2555.

Članak 4.

Nadležno tijelo

1. Što prije, a u svakom slučaju najkasnije 13. prosinca 2024., svaka država članica imenuje nacionalno vladino ili regulatorno tijelo odgovorno za obavljanje zadaća koje su mu dodijeljene ovom Uredbom („nadležno tijelo”). Dok se nadležnom tijelu ne dodijele zadaće na temelju ove Uredbe, regulatorno tijelo koje je imenovala svaka država članica na temelju članka 57. stavka 1. Direktive (EU) 2019/944 obavlja zadaće nadležnog tijela u skladu s ovom Uredbom.

2. Države članice bez odgode obavješćuju Komisiju, ACER, ENISA-u, skupinu za suradnju u području mrežne i informacijske sigurnosti osnovanu na temelju članka 14. Direktive (EU) 2022/2555 i Koordinacijsku skupinu za električnu energiju osnovanu na temelju članka 1. Odluke Komisije od 15. studenog 2012. ([17]) te im dostavljaju naziv i podatke za kontakt svojeg nadležnog tijela imenovanog u skladu sa stavkom 1. ovog članka i sve njihove naknadne promjene.

([16]) Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

([17]) Odluka Komisije od 15. studenoga 2012. o osnivanju Koordinacijske skupine za električnu energiju (2012/C 353/02) (SL C 353, 17.11.2012., str. 2.).

3. Države članice mogu dopustiti svojem nadležnom tijelu da zadaće koje su mu dodijeljene ovom Uredbom delegira drugim nacionalnim tijelima, osim zadaća navedenih u članku 5. Svako nadležno tijelo prati primjenu ove Uredbe od strane tijela kojima je delegiralo zadaće. Nadležno tijelo priopćuje Komisiji, ACER-u, Koordinacijskoj skupini za električnu energiju, ENISA-i i skupini za suradnju u području mrežne i informacijske sigurnosti naziv, podatke za kontakt, dodijeljene zadaće i sve njihove naknadne promjene.

Članak 5.

Suradnja među relevantnim tijelima i nadležnim tijelima na nacionalnoj razini

Nadležna tijela koordiniraju i osiguravaju odgovarajuću suradnju između tijela nadležnih za kibernetičku sigurnost, tijela za upravljanje kibernetičkim krizama, nacionalnih regulatornih tijela, tijela nadležnih za pripravnost za rizike i CSIRT-ova za potrebe ispunjavanja relevantnih obveza utvrđenih u ovoj Uredbi. Nadležna tijela surađuju i sa svim drugim tijelima koja odredi svaka država članica kako bi se osigurali učinkoviti postupci i izbjeglo udvostručavanje zadaća i obveza. Nadležna tijela mogu naložiti odgovarajućim nacionalnim regulatornim tijelima da od ACER-a zatraže mišljenje u skladu s člankom 8. stavkom 3.

Članak 6.

Uvjeti ili metodologije ili planovi

1. OPS-ovi u suradnji s tijelom EU-a za ODS-ove izrađuju prijedloge uvjeta ili metodologija u skladu sa stavkom 2. ili planova u skladu sa stavkom 3.

2. Sljedeći uvjeti ili metodologije i sve njihove izmjene podliježu odobrenju svih nadležnih tijela:

(a) metodologije procjene kibernetičkosigurnosnih rizika u skladu s člankom 18. stavkom 1.;

(b) izvješće o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor u skladu s člankom 23.;

(c) minimalne i napredne kibernetičkosigurnosne kontrole u skladu s člankom 29., specificiranje kibernetičkosigurnosnih kontrola u elektroenergetskom sektoru u odnosu na norme u skladu s člankom 34., uključujući minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe u skladu s člankom 33.;

(d) preporuke za nabavu u području kibernetičke sigurnosti u skladu s člankom 35.;

(e) metodologija s klasifikacijskom ljestvicom za kibernetičke napade u skladu s člankom 37. stavkom 8.

3. Prijedloge regionalnih planova za ublažavanje kibernetičkosigurnosnih rizika u skladu s člankom 22. moraju odobriti sva nadležna tijela predmetne regije pogona sustava.

4. Prijedlozi uvjeta i metodologija navedenih u stavku 2. ili za planove navedene u stavku 3. uključuju predloženi rok za njihovu provedbu i opis njihova očekivanog učinka na ciljeve ove Uredbe.

5. Tijelo EU-a za ODS-ove može predmetnim OPS-ovima dostaviti obrazloženo mišljenje do tri tjedna prije roka za podnošenje prijedloga uvjeta, metodologija ili planova nadležnim tijelima. OPS-ovi odgovorni za prijedlog uvjeta, metodologija ili planova uzimaju u obzir obrazloženo mišljenje tijela EU-a za ODS-ove prije njegova podnošenja na odobrenje nadležnim tijelima. OPS-ovi dostavljaju obrazloženje ako se mišljenje tijela EU-a za ODS-ove ne uzima u obzir.

6. Uključeni OPS-ovi blisko surađuju pri zajedničkoj izradi uvjeta, metodologija i planova. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, redovito obavješćuju nadležna tijela i ACER o napretku u izradi uvjeta, metodologija ili planova.

Članak 7.

Pravila glasovanja u OPS-ovima

1. Ako OPS-ovi koji odlučuju o prijedlozima uvjeta ili metodologija ne mogu postići dogovor, odlučuju glasovanjem kvalificiranom većinom. Kvalificirana većina za takve prijedloge izračunava se na sljedeći način:

(a) OPS-ovi koji predstavljaju barem 55 % država članica; i

(b) OPS-ovi koji predstavljaju države članice koje obuhvaćaju najmanje 65 % stanovništva Unije.

2. Blokirajuća manjina za odluke o prijedlozima odredaba i uvjeta ili metodologija navedenima u članku 6. stavku 2. mora uključivati OPS-ove koji predstavljaju barem četiri države članice, a ako nije ostvarena, smatra se da je postignuta kvalificirana većina.

3. Ako OPS-ovi iz regije pogona sustava koji odlučuju o prijedlozima planova iz članka 6. stavka 2. ne mogu postići dogovor i ako se predmetna regija pogona sustava sastoji od više od pet država članica, OPS-ovi odlučuju glasovanjem kvalificiranom većinom. Za kvalificiranu većinu za prijedloge navedene u članku 6. stavku 2. nužna je sljedeća većina:

(a) OPS-ova koji predstavljaju barem 72 % predmetnih država članica; i

(b) OPS-ova koji predstavljaju države članice koje obuhvaćaju barem 65 % stanovništva predmetnog područja.

4. Blokirajuća manjina za odluke o prijedlozima planova mora uključivati barem minimalni broj OPS-ova koji predstavljaju više od 35 % stanovništva uključenih država članica, uz OPS-ove koji predstavljaju barem jednu dodatnu predmetnu državu članicu, a ako se ta manjina ne postigne, smatra se da je postignuta kvalificirana većina.

5. Za odluke OPS-ova o prijedlozima uvjeta ili metodologija u skladu s člankom 6. stavkom 2. dodjeljuje se jedan glas po državi članici. Ako na državnom području države članice postoji više OPS-ova, država članica raspodjeljuje glasačke ovlasti među OPS-ovima.

6. Ako OPS-ovi u suradnji s tijelom EU-a za ODS-ove ne podnesu početni ili izmijenjeni prijedlog uvjeta, metodologija ili planova relevantnim nadležnim tijelima u rokovima utvrđenima u ovoj Uredbi, dostavljaju relevantnim nadležnim tijelima i ACER-u relevantne nacrte uvjeta, metodologija ili planova. U njima se objašnjava što je spriječilo postizanje dogovora. Nadležna tijela zajednički poduzimaju odgovarajuće korake za donošenje potrebnih uvjeta, metodologija ili planova. To se može učiniti, na primjer, traženjem izmjena nacrta u skladu s ovim stavkom, revizijom i dopunom tih nacrta ili, ako nacrti nisu dostavljeni, utvrđivanjem i odobravanjem potrebnih uvjeta, metodologija ili planova.

Članak 8.

Podnošenje prijedloga nadležnim tijelima

1. OPS-ovi podnose prijedloge uvjeta, metodologija ili planova na odobrenje relevantnim nadležnim tijelima u rokovima utvrđenima u člancima 18., 23., 29., 33., 34., 35. i 37. Nadležna tijela mogu zajednički produljiti te rokove u iznimnim okolnostima, posebno ako se rok ne može ispuniti zbog okolnosti izvan nadležnosti OPS-ova ili tijela EU-a za ODS-ove.

2. Prijedlozi uvjeta, metodologija ili planova na temelju stavka 1. dostavljaju se ACER-u radi obavijesti istodobno kad i nadležnim tijelima.

3. Na zajednički zahtjev nacionalnih regulatornih tijela ACER izdaje mišljenje o prijedlogu uvjeta, metodologija ili planova u roku od šest mjeseci od primitka prijedloga uvjeta, metodologija ili planova te o tom mišljenju obavješćuje nacionalna regulatorna tijela i nadležna tijela. Nacionalna regulatorna tijela, nadležna tijela odgovorna za kibernetičku sigurnost i sva druga tijela koja su imenovana nadležnim tijelima međusobno se koordiniraju prije nego što nacionalna regulatorna tijela zatraže mišljenje ACER-a. ACER u takvo mišljenje može uključiti preporuke. ACER se savjetuje s ENISA-om prije izdavanja mišljenja o prijedlozima iz članka 6. stavka 2.

4. Nadležna tijela međusobno se savjetuju i koordiniraju te blisko surađuju kako bi postigla dogovor o predloženim uvjetima, metodologijama ili planovima. Prije odobravanja uvjeta, metodologija ili planova, prema potrebi, revidiraju i dopunjuju prijedloge, nakon savjetovanja s ENTSO-om za električnu energiju i tijelom EU-a za ODS-ove, kako bi se osiguralo da su prijedlozi u skladu s ovom Uredbom i da doprinose visokoj zajedničkoj razini kibernetičke sigurnosti u cijeloj Uniji.

5. Nadležna tijela odlučuju o uvjetima, metodologijama ili planovima u roku od šest mjeseci nakon što relevantno nadležno tijelo ili, prema potrebi, posljednje relevantno nadležno tijelo primi uvjete, metodologije ili planove.

6. Ako ACER izda mišljenje, relevantna nadležna tijela uzimaju u obzir to mišljenje i donose svoje odluke u roku od šest mjeseci od primitka mišljenja ACER-a.

7. Ako nadležna tijela zajednički zatraže izmjenu predloženih uvjeta, metodologija ili planova kako bi ih mogla odobriti, OPS-ovi u suradnji s tijelom EU-a za ODS-ove izrađuju prijedlog takve izmjene uvjeta, metodologija ili planova. OPS-ovi podnose izmijenjeni prijedlog na odobrenje u roku od dva mjeseca od zahtjeva nadležnih tijela. Nadležna regulatorna tijela odlučuju o izmijenjenim uvjetima ili metodologijama u roku od dva mjeseca nakon podnošenja.

8. Ako nadležna tijela ne postignu dogovor u roku iz stavka 5. ili 7., o tome obavješćuju Komisiju. Komisija može poduzeti odgovarajuće korake kako bi omogućila donošenje potrebnih uvjeta, metodologija ili planova.

9. OPS-ovi, uz pomoć ENTSO-a za električnu energiju, i tijela EU-a za ODS-ove objavljuju uvjete, metodologije ili planove na svojim internetskim stranicama nakon odobrenja relevantnih nadležnih tijela, osim ako se takve informacije smatraju povjerljivima u skladu s člankom 47.

10. Nadležna tijela mogu zajednički zatražiti prijedloge izmjena odobrenih uvjeta, metodologija ili planova od operatora prijenosnih sustava i tijela EU-a za ODS-ove i odrediti rok za podnošenje tih prijedloga. OPS-ovi, u suradnji s tijelom EU-a za ODS-ove, mogu predložiti izmjene nadležnim tijelima i na vlastitu inicijativu. Prijedlozi za izmjenu uvjeta, metodologija ili planova izrađuju se i odobravaju u skladu s postupkom utvrđenim u ovom članku.

11. Najmanje svake tri godine nakon prvog donošenja odgovarajućih uvjeta, metodologija ili donesenih planova OPS-ovi u suradnji s tijelom EU-a za ODS-ove preispituju djelotvornost donesenih uvjeta, metodologija ili planova i bez nepotrebne odgode izvješćuju nadležna tijela i ACER o nalazima preispitivanja.

Članak 9.

Savjetovanja

1. OPS-ovi se, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, savjetuju s dionicima, uključujući ACER, ENISA-u i nadležno tijelo svake države članice, o nacrtima prijedloga uvjeta ili metodologija navedenih u članku 6. stavku 2. i o planovima iz članka 6. stavka 3. Savjetovanje ne traje kraće od mjesec dana.

2. Prijedlozi uvjeta ili metodologija iz članka 6. stavka 2. koje podnose OPS-ovi u suradnji s tijelom EU-a za ODS-ove objavljuju se i podnose na savjetovanje na razini Unije. Prijedlozi planova iz članka 6. stavka 3. koje podnose nadležni OPS-ovi u suradnji s tijelom EU-a za ODS-ove na regionalnoj razini podnose se na savjetovanje barem na regionalnoj razini.

3. OPS-ovi, uz pomoć ENTSO-a za električnu energiju, i tijelo EU-a za ODS-ove odgovorno za prijedlog uvjeta, metodologija ili planova uzimaju u obzir stajališta dionika proizašla iz savjetovanja provedenih u skladu sa stavkom 1. prije njihova podnošenja na regulatorno odobrenje. U svim se slučajevima zajedno s podneskom prijedloga daje utemeljeno obrazloženje za uvrštavanje ili neuvrštavanje stajališta proizašlih iz savjetovanja koje se pravodobno objavljuje istodobno s prijedlogom uvjeta ili metodologija ili prije njega.

Članak 10.

Sudjelovanje dionika

ACER u bliskoj suradnji s ENTSO-om za električnu energiju i tijelom EU-a za ODS-ove organizira uključivanje dionika, uključujući redovite sastanke s dionicima kako bi se utvrdili problemi i predložila poboljšanja povezana s provedbom ove Uredbe.

Članak 11.

Povrat troškova

1. Troškove koje snose OPS-ovi i ODS-ovi koji podliježu propisima o mrežnoj tarifi i koji proizlaze iz obveza utvrđenih u ovoj Uredbi, uključujući troškove koje snose ENTSO za električnu energiju i tijelo EU-a za ODS-ove, procjenjuje relevantno nacionalno regulatorno tijelo svake države članice.

2. Troškovi za koje se procijeni da su razumni, učinkoviti i razmjerni nadoknađuju se mrežnim tarifama ili drugim odgovarajućim mehanizmima, kako je utvrdilo relevantno nacionalno regulatorno tijelo.

3. Ako to zatraže relevantna nacionalna regulatorna tijela, OPS-ovi i ODS-ovi iz stavka 1. dostavljaju, u razumnom roku koji odredi nacionalno regulatorno tijelo, informacije potrebne za lakšu procjenu nastalih troškova.

Članak 12.

Praćenje

1. ACER prati provedbu ove Uredbe u skladu s člankom 32. stavkom 1. Uredbe (EU) 2019/943 i člankom 4. stavkom 2. Uredbe (EU) 2019/942. U provedbi tog praćenja ACER može surađivati s ENISA-om i zatražiti potporu ENTSO-a za električnu energiju i tijela EU-a za ODS-ove. ACER redovito obavješćuje Koordinacijsku skupinu za električnu energiju i skupinu za suradnju u području mrežne i informacijske sigurnosti o provedbi ove Uredbe.

2. ACER najmanje svake tri godine nakon stupanja na snagu ove Uredbe objavljuje izvješće o

(a) preispitivanju statusa provedbe primjenjivih mjera upravljanja kibernetičkosigurnosnim rizicima s obzirom na subjekte s velikim i kritičnim utjecajem,

(b) utvrđuje mogu li biti potrebna dodatna pravila o zajedničkim zahtjevima, planiranju, praćenju, izvješćivanju i upravljanju krizama kako bi se spriječili rizici za elektroenergetski sektor i

(c) utvrđuje područja u kojima su potrebna poboljšanja za reviziju ove Uredbe ili određuje neobuhvaćena područja i nove prioritete koji se mogu pojaviti zbog tehnološkog razvoja.

3. Do 13. lipnja 2025. ACER, u suradnji s ENISA-om i nakon savjetovanja s ENTSO-om za električnu energiju i tijelom EU-a za ODS-ove, može izdati smjernice o relevantnim informacijama koje treba dostaviti ACER-u za potrebe praćenja te o postupku i učestalosti prikupljanja, na temelju pokazatelja uspješnosti utvrđenih u skladu sa stavkom 5.

4. Nadležna tijela mogu imati pristup relevantnim informacijama kojima raspolaže ACER, a koje je prikupio u skladu s ovim člankom.

5. ACER u suradnji s ENISA-om i uz potporu ENTSO-a za električnu energiju i tijela EU-a za ODS-ove izdaje neobvezujuće pokazatelje uspješnosti za procjenu operativne pouzdanosti koji su povezani s kibernetičkosigurnosnim aspektima prekograničnih protoka električne energije.

6. Subjekti iz članka 2. stavka 1. ove Uredbe dostavljaju ACER-u informacije koje su mu potrebne za obavljanje zadaća navedenih u stavku 2.

Članak 13.

Utvrđivanje referentnih vrijednosti

1. ACER je u suradnji s ENISA-om dužan do 13. lipnja 2025. sastaviti neobvezujući vodič za vrednovanje kibernetičke sigurnosti na temelju referentnih vrijednosti. U vodiču se nacionalnim regulatornim tijelima objašnjavaju načela kako se na temelju referentnih vrijednosti vrednuju kibernetičkosigurnosne kontrole uvedene u skladu sa stavkom 2. ovog članka, uzimajući u obzir troškove uvođenja kontrola i djelotvornost funkcije procesa, proizvoda, usluga, sustava i rješenja koji služe da bi se uvele takve kontrole. U sastavljanju neobvezujućeg vodiča za vrednovanje kibernetičke sigurnosti na temelju referentnih vrijednosti ACER uzima u obzir postojeća izvješća o vrednovanju. ACER nacionalnim regulatornim tijelima informativno dostavlja neobvezujući vodič za vrednovanje kibernetičke sigurnosti na temelju referentnih vrijednosti.

2. U roku od 12 mjeseci od sastavljanja vodiča za vrednovanje na temelju referentnih vrijednosti u skladu sa stavkom 1. nacionalna regulatorna tijela provode analizu vrednovanja na temelju referentnih vrijednosti kako bi procijenila postižu li trenutačna ulaganja u kibernetičku sigurnost:

(a) ublažavanje rizika koji utječu na prekogranične protoke električne energije;

(b) željene rezultate i poticanje učinkovitosti u razvoju elektroenergetskih sustava;

(c) učinkovitost i integriranost u općoj nabavi imovine i usluga.

3. Za potrebe analize na temelju referentnih vrijednosti nacionalna regulatorna tijela mogu uzeti u obzir neobvezujući vodič za vrednovanje kibernetičke sigurnosti na temelju referentnih vrijednosti koji je izradio ACER te prvenstveno ocjenjuju:

(a) prosječne rashode povezane s kibernetičkom sigurnošću za ublažavanje rizika koji utječu na prekogranične protoke električne energije, posebno u pogledu subjekata s velikim i kritičnim utjecajem;

(b) u suradnji s ENTSO-om za električnu energiju i tijelom EU-a za ODS-ove, prosječne cijene usluga, sustava i proizvoda u području kibernetičke sigurnosti koji u velikoj mjeri doprinose poboljšanju i održavanju mjera upravljanja kibernetičkosigurnosnim rizicima u različitim regijama pogona sustava;

(c) postojanje i razinu usporedivosti troškova i funkcija usluga, sustava i rješenja u području kibernetičke sigurnosti prikladnih za provedbu ove Uredbe uz utvrđivanje mogućih mjera potrebnih za poticanje učinkovitosti potrošnje, posebno ako bi mogla biti potrebna tehnološka ulaganja u kibernetičku sigurnost.

4. Postupanje sa svakom informacijom povezanom s analizom vrednovanja na temelju referentnih vrijednosti i obrađivanje tih informacija provodi se u skladu sa zahtjevima za klasifikaciju podataka iz ove Uredbe, minimalnim kontrolama kibernetičke sigurnosti i izvješćem o procjeni prekograničnih rizika za kibernetičku sigurnost elektroenergetskog sektora. Analiza vrednovanja na temelju referentnih vrijednosti iz stavaka 2. i 3. se ne objavljuje.

5. Ne dovodeći u pitanje zahtjeve za povjerljivost iz članka 47. i potrebu za zaštitom sigurnosti subjekata koji podliježu odredbama ove Uredbe, analiza vrednovanja na temelju referentnih vrijednosti iz stavaka 2. i 3. ovog članka dostavlja se svim nacionalnim regulatornim tijelima, svim nadležnim tijelima, ACER-u, ENISA-i i Komisiji.

Članak 14.

Sporazumi s OPS-ovima iz trećih zemalja

1. U roku od 18 mjeseci od stupanja na snagu ove Uredbe OPS-ovi iz regije pogona sustava koja graniči s trećom zemljom nastoje s OPS-ovima susjedne treće zemlje sklopiti sporazume koji su u skladu s relevantnim pravom Unije u kojima se s tim OPS-ovima utvrđuju osnova za suradnju i dogovori o suradnji u području kibernetičke sigurnosti.

2. OPS-ovi obavješćuju nadležno tijelo o sporazumima sklopljenima u skladu sa stavkom 1.

Članak 15.

Pravni zastupnici

1. Subjekti koji nemaju poslovni nastan u Uniji, ali koji pružaju usluge subjektima u Uniji i koji su obaviješteni da su određeni kao subjekti s velikim ili kritičnim utjecajem u skladu s člankom 24. stavkom 6. u roku od tri mjeseca nakon obavješćivanja imenuju zastupnika u Uniji i o tome obavješćuju nadležno tijelo koje je poslalo obavijest.

2. Taj zastupnik ovlašćuje se kako bi mu se, uz subjekt s velikim utjecajem ili kritičnim utjecajem ili umjesto njega, moglo obratiti bilo koje nadležno tijelo ili CSIRT iz Unije u pogledu obveza tog subjekta na temelju ove Uredbe. Subjekt s velikim ili kritičnim utjecajem svojem pravnom zastupniku daje potrebne ovlasti i dostatna sredstva kako bi on mogao učinkovito i pravodobno surađivati s relevantnim nadležnim tijelima ili CSIRT-ovima.

3. Zastupnik ima poslovni nastan u jednoj od država članica u kojima subjekt pruža svoje usluge. Smatra se da takav subjekt pripada nadležnosti one države članice u kojoj njegov zastupnik ima poslovni nastan. Subjekti s velikim ili kritičnim utjecajem obavješćuju nadležno tijelo u državi članici u kojoj njihov pravni zastupnik ima boravište ili poslovni nastan o imenu, poštanskoj adresi, e-adresi i telefonskom broju svojeg pravnog zastupnika.

4. Imenovani pravni zastupnik može se smatrati odgovornim za neispunjavanje obveza na temelju ove Uredbe, ne dovodeći u pitanje odgovornost i pravne postupke koji bi mogli biti pokrenuti protiv samog subjekta s velikim ili kritičnim utjecajem.

5. Ako nije imenovan zastupnik unutar Unije u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne mjere protiv subjekta zbog nepoštovanja obveza iz ove Uredbe.

6. Imenovanje pravnog zastupnika unutar Unije na temelju stavka 1. ne čini poslovni nastan u Uniji.

Članak 16.

Suradnja ENTSO-a za električnu energiju i tijela EU-a za ODS-ove

1. ENTSO za električnu energiju i tijelo EU-a za ODS-ove surađuju u provedbi procjena kibernetičkosigurnosnih rizika u skladu s člancima 19. i 21., a posebno sljedećih zadaća:

(a) razvoj metodologija procjene kibernetičkosigurnosnih rizika u skladu s člankom 18. stavkom 1.;

(b) izrada izvješća o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor u skladu s člankom 23.;

(c) razvoj zajedničkog okvira za kibernetičku sigurnost elektroenergetskog sektora u skladu s poglavljem III.;

(d) izrada preporuke za nabavu u području kibernetičke sigurnosti u skladu s člankom 35.;

(e) razvoj metodologije s klasifikacijskom ljestvicom za kibernetičke napade u skladu s člankom 37. stavkom 8.;

(f) razvoj privremenog indeksa utjecaja na kibernetičku sigurnost elektroenergetskog sektora („ECII”) u skladu s člankom 48. stavkom 1. točkom (a);

(g) izrada konsolidiranog privremenog popisa subjekata s velikim i kritičnim utjecajem u skladu s člankom 48. stavkom 3.;

(h) izrada privremenog popisa procesa s velikim i kritičnim utjecajem na razini Unije u skladu s člankom 48. stavkom 4.;

(i) izrada privremenog popisa europskih i međunarodnih normi i kontrola u skladu s člankom 48. stavkom 6.;

(j) provedba procjene kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19.;

(k) uspješnost regionalnih procjena kibernetičkosigurnosnih rizika u skladu s člankom 21.;

(l) definiranje regionalnih planova za ublažavanje kibernetičkosigurnosnih rizika u skladu s člankom 22.;

(m) razvoj smjernica o europskim programima certifikacije kibernetičke sigurnosti za IKT proizvode, usluge i procese u skladu s člankom 36.;

(n) izrada smjernica za provedbu ove Uredbe uz savjetovanje s ACER-om i ENISA-om.

2. Suradnja između ENTSO-a za električnu energiju i tijela EU-a za ODS-ove može biti u obliku radne skupine za kibernetičkosigurnosne rizike.

3. ENTSO za električnu energiju i tijelo EU-a za ODS-ove redovito obavješćuju ACER, ENISA-u, skupinu za suradnju u području mrežne i informacijske sigurnosti i Koordinacijsku skupinu za električnu energiju o napretku u provedbi procjena kibernetičkosigurnosnih rizika na razini Unije i na regionalnoj razini u skladu s člancima 19. i 21.

Članak 17.

Suradnja između ACER-a i nadležnih tijela

ACER u suradnji sa svakim nadležnim tijelom:

(1) prati provedbu mjera upravljanja kibernetičkosigurnosnim rizicima u skladu s člankom 12. stavkom 2. točkom (a) i obveza izvješćivanja u skladu s člancima 27. i 39.; i

(2) prati postupak donošenja i provedbu uvjeta, metodologija ili planova u skladu s člankom 6. stavcima 2. i 3. Suradnja između ACER-a, ENISA-e i svakog nadležnog tijela može biti u obliku tijela za praćenje kibernetičkosigurnosnih rizika.

POGLAVLJE II.

PROCJENA RIZIKA I UTVRĐIVANJE RELEVANTNIH KIBERNETIČKOSIGURNOSNIH RIZIKA

Članak 18.

Metodologije procjene kibernetičkosigurnosnih rizika

1. OPS-ovi su, uz pomoć ENTSO-a za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja sa skupinom za suradnju u području mrežne i informacijske sigurnosti, dužni do 13. ožujka 2025. podnijeti prijedlog metodologija za procjenu kibernetičkosigurnosnih rizika na razini Unije, na regionalnoj razini i na razini država članica.

2. Metodologije procjene kibernetičkosigurnosnih rizika na razini Unije, na regionalnoj razini i na razini država članica uključuju:

(a) popis kibernetičkih prijetnji koje treba razmotriti, među ostalim barem sljedeće prijetnje u lancu opskrbe:

i. teške i neočekivane smetnje u lancu opskrbe;

ii. nedostupnost IKT proizvoda, usluga ili procesa iz lanca opskrbe;

iii. kibernetičke napade koji dođu kroz aktere u lancu opskrbe;

iv. curenje osjetljivih informacija kroz lanac opskrbe, uključujući praćenje lanca opskrbe;

v. uvođenje slabosti ili stražnjih vrata u IKT proizvode, usluge ili procese kroz aktere u lancu opskrbe;

(b) kriterije za ocjenjivanje kibernetičkosigurnosnih rizika kao visokih ili kritičnih na temelju definiranih pragova za posljedice i vjerojatnost;

(c) pristup analizi kibernetičkosigurnosnih rizika koji proizlaze iz zastarjelih sustava, kaskadnih posljedica kibernetičkih napada i prirode sustava koji upravljaju mrežom u stvarnom vremenu;

(d) pristup analizi kibernetičkosigurnosnih rizika koji proizlaze iz ovisnosti o jednom dobavljaču IKT proizvoda, usluga ili procesa.

3. U metodologijama procjene kibernetičkosigurnosnih rizika na razini Unije, na regionalnoj razini i na razini država članica kibernetičkosigurnosni rizici procjenjuju se na temelju iste matrice utjecaja rizika. Matrica utjecaja rizika služi za:

(a) mjerenje posljedica kibernetičkog napada na temelju sljedećih kriterija:

i. gubitak opterećenja;

ii. smanjenje proizvodnje energije;

iii. gubitak kapaciteta u primarnoj rezervi za održavanje frekvencije;

iv. gubitak kapaciteta za ponovnu uspostavu rada električne mreže bez oslanjanja na vanjsku prijenosnu mrežu za oporavak nakon potpunog ili djelomičnog isključivanja (tzv. „crni start”);

v. očekivano trajanje isključenja električne energije koje utječe na kupce u kombinaciji s razmjerom isključenja prema broju isključenih kupaca; i

vi. svi drugi kvantitativni ili kvalitativni kriteriji koji bi mogli razumno poslužiti kao pokazatelj utjecaja kibernetičkog napada na prekogranične protoke električne energije;

(b) mjerenje vjerojatnosti incidenta u smislu godišnje učestalosti kibernetičkih napada.

4. U metodologijama procjene kibernetičkosigurnosnih rizika na razini Unije opisuje se kako će se definirati vrijednosti ECII-ja za pragove velikog i kritičnog utjecaja. ECII omogućuje subjektima da na temelju kriterija iz stavka 2. točke (b) procijene utjecaj rizika na svoje poslovne procese procjenama utjecaja na poslovanje koje provode u skladu s člankom 26. stavkom 4. točkom (c) podtočkom i.

5. ENTSO za električnu energiju, u koordinaciji s tijelom EU-a za ODS-ove, obavješćuje Koordinacijsku skupinu za električnu energiju o prijedlozima metodologija za procjenu kibernetičkosigurnosnih rizika koje su razvijene u skladu sa stavkom 1.

Članak 19.

Procjena kibernetičkosigurnosnih rizika na razini Unije

1. U roku od devet mjeseci od odobrenja metodologija u skladu s člankom 8. i svake tri godine nakon toga ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i uz savjetovanje sa skupinom za suradnju NIS, ne dovodeći u pitanje članak 22. Direktive (EU) 2022/2555, provodi procjenu kibernetičkosigurnosnih rizika na razini Unije i sastavlja nacrt izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije. Za to će koristiti metodologije razvijene u skladu s člankom 18. i odobrene u skladu s člankom 8. kako bi utvrdili, analizirali i ocijenili moguće posljedice kibernetičkih napada koji utječu na operativnu sigurnost elektroenergetskog sustava i remete prekogranične protoke električne energije. U procjeni kibernetičkosigurnosnih rizika na razini Unije ne uzimaju se u obzir pravna i financijska šteta ni narušavanje ugleda prouzročeno kibernetičkim napadima.

2. Izvješće o procjeni kibernetičkosigurnosnih rizika na razini Unije uključuje sljedeće elemente:

(a) procese s velikim utjecajem na razini Unije i procese s kritičnim utjecajem na razini Unije;

(b) matricu utjecaja rizika koju subjekti i nadležna tijela upotrebljavaju za procjenu kibernetičkosigurnosnog rizika utvrđenog u procjeni kibernetičkosigurnosnih rizika na razini države članice koja se provodi u skladu s člankom 20. i procjenu kibernetičkosigurnosnih rizika na razini subjekta u skladu s člankom 26. stavkom 2. točkom (b).

3. Kad je riječ o procesima s velikim utjecajem na razini Unije i procesima s kritičnim utjecajem na razini Unije, izvješće o procjeni kibernetičkosigurnosnih rizika na razini Unije uključuje:

(a) procjenu mogućih posljedica kibernetičkog napada primjenom parametara definiranih u metodologiji procjene kibernetičkosigurnosnih rizika izrađenoj u skladu s člankom 18. stavcima 2., 3. i 4. i odobrenoj u skladu s člankom 8.;

(b) ECII i pragove velikog i kritičnog utjecaja koje nadležna tijela primjenjuju u skladu s člankom 24. stavcima 1. i 2. kako bi utvrdila subjekte s velikim utjecajem i kritičnim utjecajem koji sudjeluju u procesima s velikim i kritičnim utjecajem na razini Unije.

4. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, podnosi nacrt izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije s rezultatima procjene kibernetičkosigurnosnih rizika na razini Unije ACER-u na mišljenje. ACER izdaje mišljenje o nacrtu izvješća u roku od tri mjeseca od njegova primitka. ENTSO za električnu energiju i tijelo EU-a za ODS-ove pri dovršavanju tog izvješća u najvećoj mjeri uzimaju u obzir mišljenje ACER-a.

5. U roku od tri mjeseca od primitka mišljenja ACER-a ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, ACER-u, Komisiji, ENISA-i i nadležnim tijelima dostavlja završno izvješće o procjeni kibernetičkosigurnosnih rizika na razini Unije.

Članak 20.

Procjena kibernetičkosigurnosnih rizika na razini države članice

1. Svako nadležno tijelo provodi procjenu kibernetičkosigurnosnih rizika države članice za sve subjekte s velikim i kritičnim utjecajem u svojoj državi članici primjenom metodologija razvijenih u skladu s člankom 18. i odobrenih u skladu s člankom 8. U procjeni kibernetičkosigurnosnih rizika države članice utvrđuju se i analiziraju rizici od kibernetičkih napada koji utječu na operativnu sigurnost elektroenergetskog sustava i remete prekogranične protoke električne energije. U procjeni kibernetičkosigurnosnih rizika države članice ne uzima se u obzir pravna ni financijska šteta ni narušavanje ugleda prouzročeno kibernetičkim napadima.

2. U roku od 21 mjeseca nakon primitka obavijesti o subjektima s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. i svake tri godine nakon tog datuma te nakon savjetovanja s nadležnim tijelima odgovornima za kibernetičku sigurnost elektroenergetskog sektora svako nadležno tijelo, uz potporu CSIRT-a, dostavlja ENTSO-u za električnu energiju i tijelu EU-a za ODS-ove izvješće o procjeni kibernetičkosigurnosnih rizika države članice koje sadržava sljedeće informacije za svaki poslovni proces s velikim ili kritičnim utjecajem:

(a) status provedbe minimalnih i naprednih kibernetičkosigurnosnih kontrola u skladu s člankom 29.;

(b) popis svih kibernetičkih napada prijavljenih u prethodne tri godine u skladu s člankom 38. stavkom 3.;

(c) sažetak informacija o kibernetičkim prijetnjama prijavljenima u prethodne tri godine u skladu s člankom 38. stavkom 6.;

(d) za svaki proces s velikim ili kritičnim utjecajem na razini Unije, procjenu rizika od ugrožavanja povjerljivosti, cjelovitosti i dostupnosti informacija i relevantnih resursa;

(e) prema potrebi, popis dodatnih subjekata za koje je utvrđeno da imaju velik ili kritični utjecaj u skladu s člankom 24. stavcima 1., 2., 3. i 5.

3. U izvješću države članice o procjeni kibernetičkosigurnosnih rizika uzima se u obzir plan pripravnosti države članice na rizike uspostavljen u skladu s člankom 10. Uredbe (EU) 2019/941.

4. Informacije sadržane u izvješću države članice o procjeni kibernetičkosigurnosnih rizika u skladu sa stavkom 2. točkama od (a) do (d) nisu povezane s određenim subjektima ili imovinom. Izvješće o procjeni kibernetičkosigurnosnih rizika na razini države članice uključuje i procjenu rizika privremenih odstupanja koja su izdala nadležna tijela u državama članicama u skladu s člankom 30.

5. ENTSO za električnu energiju i tijelo EU-a za ODS-ove mogu zatražiti dodatne informacije od nadležnih tijela u vezi sa zadaćama iz stavka 2. točaka (a) i (c).

6. Nadležna tijela osiguravaju da su informacije koje pružaju točne i ispravne.

Članak 21.

Regionalne procjene kibernetičkosigurnosnih rizika

1. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i uz savjetovanje s relevantnim regionalnim koordinacijskim centrom, provodi regionalnu procjenu kibernetičkosigurnosnih rizika za svaku regiju pogona sustava tako što primjenjuje metodologije koje su razvijene u skladu s člankom 19. i odobrene u skladu s člankom 8. kako bi se utvrdili, analizirali i ocijenili rizici od kibernetičkih napada koji utječu na operativnu sigurnost elektroenergetskog sustava i remete prekogranične protoke električne energije. U regionalnim procjenama kibernetičkosigurnosnih rizika ne uzima se u obzir pravna ni financijska šteta ni narušavanje ugleda prouzročeno kibernetičkim napadima.

2. U roku od 30 mjeseci nakon primanja obavijesti o subjektima s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. i svake tri godine nakon toga ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja sa skupinom za suradnju u području mrežne i informacijske sigurnosti, sastavlja regionalno izvješće o procjeni kibernetičkosigurnosnih rizika za svaku regiju pogona sustava.

3. U regionalnom izvješću o procjeni kibernetičkosigurnosnih rizika uzimaju se u obzir relevantne informacije sadržane u izvješćima o procjeni kibernetičkosigurnosnih rizika na razini Unije i izvješćima država članica o procjenama kibernetičkosigurnosnih rizika.

4. U regionalnoj procjeni kibernetičkosigurnosnih rizika uzimaju se u obzir regionalni scenariji elektroenergetskih kriza povezani s kibernetičkom sigurnošću utvrđeni u skladu s člankom 6. Uredbe (EU) 2019/941.

Članak 22.

Regionalni planovi za ublažavanje kibernetičkosigurnosnih rizika

1. U roku od 36 mjeseci od primanja obavijesti o subjektima s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. i najkasnije 13. lipnja 2031. i svake tri godine nakon tog datuma OPS-ovi, uz pomoć ENTSO-a za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja s regionalnim koordinacijskim centrima i skupinom za suradnju u području mrežne i informacijske sigurnosti, izrađuju regionalni plan za ublažavanje kibernetičkosigurnosnih rizika za svaku regiju pogona sustava.

2. Regionalni planovi za ublažavanje kibernetičkosigurnosnih rizika uključuju:

(a) minimalne i napredne kibernetičkosigurnosne kontrole koje subjekti s velikim utjecajem i subjekti kritičnim utjecajem primjenjuju u regiji pogona sustava;

(b) preostale kibernetičkosigurnosne rizike u regijama pogona sustava nakon primjene kontrola iz točke (a).

3. ENTSO za električnu energiju podnosi regionalne planove za ublažavanje rizika relevantnim operatorima prijenosnih sustava, nadležnim tijelima i Koordinacijskoj skupini za električnu energiju. Koordinacijska skupina za električnu energiju može preporučiti izmjene.

4. OPS-ovi, uz pomoć ENTSO-a za električnu energiju u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja sa skupinom za suradnju u području mrežne i informacijske sigurnosti, ažuriraju regionalne planove za ublažavanje rizika svake tri godine, osim ako okolnosti zahtijevaju češće ažuriranje.

Članak 23.

Izvješće o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor

1. U roku od 40 mjeseci od primanja obavijesti subjektima s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. i nakon toga svake tri godine OPS-ovi, uz pomoć ENTSO-a za električnu energiju, u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja sa skupinom za suradnju u području mrežne i informacijske sigurnosti, dostavljaju Koordinacijskoj skupini za električnu energiju izvješće o ishodu procjene kibernetičkosigurnosnih rizika u odnosu na prekogranične protoke električne energije („izvješće o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor”).

2. Izvješće o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor temelji se na izvješću o procjeni kibernetičkosigurnosnih rizika na razini Unije, izvješćima o procjeni kibernetičkosigurnosnih rizika na razini država članica i regionalnim izvješćima o procjeni kibernetičkosigurnosnih rizika te sadržava sljedeće informacije:

(a) popis procesa s velikim i kritičnim utjecajem na razini Unije utvrđenih u izvješću o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 2. točkom (a), uključujući procjenu vjerojatnosti i posljedica kibernetičkosigurnosnih rizika ocijenjenih u okviru izrade regionalnih izvješća o procjeni kibernetičkosigurnosnih rizika u skladu s člankom 21. stavkom 2. i člankom 19. stavkom 3. točkom (a);

(b) trenutačne kibernetičke prijetnje, pri čemu se posebna pozornost posvećuje novim prijetnjama i rizicima za elektroenergetski sustav;

(c) kibernetičke napade iz prethodnog razdoblja na razini Unije, pri čemu se kritički sagledavaju načini na koje su takvi kibernetički napadi mogli utjecati na prekogranične protoke električne energije;

(d) opći status provedbe mjera kibernetičke sigurnosti;

(e) status provedbe protoka informacija u skladu s člancima 37. i 38.;

(f) popis informacija ili posebnih kriterija za klasifikaciju informacija u skladu s člankom 46.;

(g) utvrđene i istaknute rizike koji mogu proizaći iz nesigurnog upravljanja lancem opskrbe;

(h) rezultate i prikupljena iskustva iz regionalnih i međuregionalnih vježbi u području kibernetičke sigurnosti organiziranih u skladu s člankom 44.;

(i) analizu razvoja ukupnih kibernetičkosigurnosnih rizika u elektroenergetskom sektoru u pogledu prekograničnih protoka energije od posljednjih regionalnih procjena tih rizika;

(j) sve druge informacije koje bi mogle biti korisne za utvrđivanje mogućih poboljšanja ove Uredbe ili potrebe za revizijom ove Uredbe ili bilo kojeg od njezinih instrumenata; i

(k) agregirane i anonimizirane informacije o odstupanjima odobrenima u skladu s člankom 30. stavkom 3.

3. Subjekti iz članka 2. stavka 1. mogu pridonijeti izradi izvješća o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor uz poštovanje povjerljivosti informacija u skladu s člankom 47. OPS-ovi se, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, savjetuju s tim subjektima od rane faze.

4. Na izvješće o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor primjenjuju se pravila o zaštiti razmjene informacija u skladu s člankom 46. Ne dovodeći u pitanje članak 10. stavak 4. i članak 47. stavak 4., ENTSO za električnu energiju i tijelo EU-a za ODS-ove objavljuju verziju tog izvješća koja ne sadržava informacije koje mogu uzrokovati štetu subjektima navedenima u članku 2. stavku 1. Javna verzija tog izvješća objavljuje se samo uz suglasnost skupine za suradnju u području mrežne i informacijske sigurnosti i Koordinacijske skupine za električnu energiju. ENTSO za električnu energiju u koordinaciji s tijelom EU-a za ODS-ove odgovoran je za izradu i objavljivanje javne verzije izvješća.

Članak 24.

Utvrđivanje subjekata s velikim i kritičnim utjecajem

1. Svako nadležno tijelo utvrđuje na temelju ECII-ja i pragova velikog i kritičnog utjecaja iz izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 3. točkom (b) subjekte s velikim i kritičnim utjecajem u svojoj državi članici koji su uključeni u procese s velikim i kritičnim utjecajem na razini Unije. Nadležna tijela mogu zatražiti informacije od subjekta u svojoj državi članici kako bi utvrdila vrijednosti ECII-ja tog subjekta. Ako je vrijednost ECII-ja utvrđena za subjekt veća od praga velikog ili kritičnog utjecaja, subjekt se navodi u izvješću države članice o procjeni kibernetičkosigurnosnih rizika iz članka 20. stavka 2.

2. Svako nadležno tijelo utvrđuje na temelju ECII-ja i pragova velikog i kritičnog utjecaja iz izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 3. točkom (b) subjekte s velikim i kritičnim utjecajem koji nemaju poslovni nastan u Uniji u mjeri u kojoj su aktivni u Uniji. Nadležno tijelo može zatražiti informacije od subjekta koji nema poslovni nastan u Uniji kako bi utvrdilo njegove vrijednosti ECII-ja.

3. Svako nadležno tijelo može utvrditi dodatne subjekte u svojoj državi članici kao subjekte s velikim ili kritičnim utjecajem ako su ispunjeni sljedeći kriteriji:

(a) subjekt je dio skupine subjekata za koje postoji znatan rizik da bi mogli biti istodobno zahvaćeni kibernetičkim napadom;

(b) agregirani ECII skupine subjekata je iznad praga velikog ili kritičnog utjecaja.

4. Ako nadležno tijelo utvrdi dodatne subjekte u skladu sa stavkom 3., svi procesi u tim subjektima za koje je agregirani ECII skupine veći od praga velikog utjecaja smatraju se procesima s velikim utjecajem, a svi procesi u tim subjektima za koje je agregirani ECII skupine veći od praga kritičnog utjecaja smatraju se procesima s kritičnim utjecajem.

5. Ako nadležno tijelo utvrdi subjekte iz stavka 3. točke (a) u više država članica, o tome obavješćuje druga nadležna tijela, ENTSO za električnu energiju i tijelo EU-a za ODS-ove. ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove na temelju informacija dobivenih od svih nadležnih tijela dostavlja nadležnim tijelima analizu dobivene skupine subjekata u više država članica koja može uzrokovati distribuirane poremećaje u prekograničnim protocima električne energije i dovesti do kibernetičkih napada. Ako se utvrdi da je skupina subjekata u nekoliko država članica utvrđena kao skupina za koju je ECII veći od praga velikog ili kritičnog utjecaja, sva ta nadležna tijela utvrđuju subjekte takve skupine kao subjekte s velikim ili kritičnim utjecajem za svoju državu članicu na temelju agregiranog ECII-ja skupine subjekata te se utvrđeni subjekti unose u izvješće o procjeni kibernetičkosigurnosnih rizika na razini Unije.

6. U roku od devet mjeseci nakon što ga ENTSO za električnu energiju i tijelo EU-a za ODS-ove obavijeste o izvješću o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 5., a u svakom slučaju najkasnije do 13. lipnja 2028., svako nadležno tijelo dužno je obavijestiti subjekte s popisa o tome da su u njegovoj državi članici utvrđeni kao subjekti s velikim ili kritičnim utjecajem.

7. Ako je pružatelj usluga prijavljen nekom nadležnom tijelu kao ključni pružatelj IKT usluga u skladu s člankom 27. točkom (c), to nadležno tijelo o tome obavješćuje nadležna tijela država članica na čijem se državnom području nalazi njegovo sjedište ili zastupnik. Potonja nadležna tijeka obavješćuju pružatelja usluga da je utvrđen kao pružatelj ključnih usluga.

Članak 25.

Nacionalni programi provjere

1. Nadležna tijela mogu uspostaviti nacionalni sustav provjere kako bi provjerila jesu li subjekti s kritičnim utjecajem utvrđeni u skladu s člankom 24. stavkom 1. proveli nacionalni zakonodavni okvir koji je uključen u korelacijsku matricu iz članka 34. Nacionalni program provjere može se temeljiti na inspekciji koju provodi nadležno tijelo, neovisnim revizijama sigurnosti ili na uzajamnim istorazinskim ocjenjivanjima subjekata s kritičnim utjecajem u istoj državi članici koje nadzire nadležno tijelo.

2. Ako nadležno tijelo odluči uspostaviti nacionalni sustav provjere, to nadležno tijelo osigurava da se provjera provodi u skladu sa sljedećim zahtjevima:

(a) svaka strana koja provodi istorazinsko ocjenjivanje, reviziju ili inspekciju neovisna je o subjektu s kritičnim utjecajem koji se provjerava i nije u sukobu interesa;

(b) osoblje koje provodi istorazinsko ocjenjivanje, reviziju ili inspekciju mora posjedovati dokazivo znanje o:

  i. kibernetičkoj sigurnosti u elektroenergetskom sektoru;

  ii. sustavima za upravljanje kibernetičkom sigurnošću;

  iii. načelima revizije;

  iv. procjeni kibernetičkosigurnosnih rizika;

  v. zajedničkom okviru za kibernetičku sigurnost elektroenergetskog sektora;

  vi. nacionalnom zakonodavnom i regulatornom okviru te europskim i međunarodnim normama obuhvaćenima opsegom provjere;

  vii. procesima s kritičnim utjecajem obuhvaćenima opsegom provjere;

(c) strana koja provodi istorazinsko ocjenjivanje, reviziju ili inspekciju ima dovoljno vremena za obavljanje tih aktivnosti;

(d) strana koja provodi istorazinsko ocjenjivanje, reviziju ili inspekciju poduzima odgovarajuće mjere za zaštitu informacija koje prikuplja tijekom provjere, u skladu s njihovom razinom povjerljivosti; i

(e) istorazinsko ocjenjivanje, revizije ili inspekcije provode se najmanje jednom godišnje i obuhvaćaju cijeli opseg provjere najmanje svake tri godine.

3. Ako nadležno tijelo odluči uspostaviti nacionalni program provjere, jednom godišnje izvješćuje ACER o tome koliko je često provodilo inspekcije u okviru tog programa.

Članak 26.

Upravljanje kibernetičkosigurnosnim rizicima na razini subjekta

1. Svaki subjekt s velikim i kritičnim utjecajem kojeg je nadležno tijelo utvrdilo kao takvog u skladu s člankom 24. stavkom 1. upravlja kibernetičkosigurnosnim rizicima za svu svoju imovinu u područjima od velikog i kritičnog utjecaja. Svaki subjekt s velikim i kritičnim utjecajem svake tri godine provodi postupak upravljanja rizicima koji se sastoji od faza iz stavka 2.

2. Upravljanje kibernetičkosigurnosnim rizicima svakog subjekta s velikim i kritičnim utjecajem temelji se na pristupu čiji je cilj zaštititi njegove mrežne i informacijske sustave i koji se sastoji od sljedećih faza:

(a) definiranje konteksta;

(b) procjena kibernetičkosigurnosnih rizika na razini subjekta;

(c) obrada kibernetičkosigurnosnih rizika;

(d) prihvaćanje kibernetičkosigurnosnih rizika.

3. U fazi definiranja konteksta svaki subjekt s velikim ili kritičnim utjecajem:

(a) utvrđuje područje primjene procjene kibernetičkosigurnosnih rizika, uključujući procese s velikim i kritičnim utjecajem koje su utvrdili ENTSO za električnu energiju i tijelo EU-a za ODS-ove druge procese koji mogu biti mete kibernetičkih napada s velikim ili kritičnim utjecajem na prekogranične protoke električne energije; i

(b) utvrđuje kriterije za procjenu i prihvaćanje rizika u skladu s matricom utjecaja rizika koju subjekti i nadležna tijela upotrebljavaju u procjeni kibernetičkosigurnosnih rizika u metodologijama procjene kibernetičkosigurnosnih rizika na razini Unije, na regionalnoj razini i na razini država članica koje su razvili ENTSO za električnu energiju i tijelo EU-a za ODS-ove u skladu s člankom 19. stavkom 2.

4. U fazi procjene kibernetičkosigurnosnih rizika svaki subjekt s velikim ili kritičnim utjecajem:

(a) utvrđuje kibernetičkosigurnosne rizike uzimajući u obzir:

i. svu imovinu koja služi u procesima s velikim i kritičnim utjecajem na razini Unije uz procjenu mogućeg utjecaja na prekogranične protoke električne energije ako imovina bude ugrožena;

ii. moguće kibernetičke prijetnje uzimajući u obzir kibernetičke prijetnje utvrđene u najnovijem izvješću o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor iz članka 23. i prijetnje u lancu opskrbe;

iii. ranjivosti, uključujući ranjivosti u zastarjelim sustavima;

iv. moguće scenarije kibernetičkog napada, uključujući kibernetičke napade koji utječu na sigurnost pogona elektroenergetskog sustava i ometaju prekogranične protoke električne energije;

v. relevantne evaluacije i procjene rizika provedene na razini Unije, uključujući koordinirane procjene rizika ključnih lanaca opskrbe u skladu s člankom 22. Direktive (EU) 2022/2555; i

vi. postojeće kontrole;

(b) analizira vjerojatnost i posljedice kibernetičkosigurnosnih rizika utvrđenih u točki (a) i utvrđuje stupanj tog rizika na temelju matrice utjecaja rizika koja služi za procjenu kibernetičkosigurnosnih rizika u metodologijama procjene kibernetičkosigurnosnih rizika na razini Unije, na regionalnoj razini i na razini država članica koje su razvili operatori prijenosnih sustava uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove u skladu s člankom 19. stavkom 2.;

(c) klasificira imovinu prema mogućim posljedicama u slučaju ugrožavanja kibernetičke sigurnosti i određuje područje od velikog i kritičnog utjecaja prolaskom kroz sljedeće korake:

i. provodi procjenu utjecaja na poslovanje na temelju ECII-ja za sve procese koji podliježu procjeni kibernetičkosigurnosnih rizika;

ii. klasificira proces kao proces s velikim ili kritičnim utjecajem ako je njegov ECII veći od praga velikog odnosno kritičnog utjecaja;

iii. utvrđuje svu imovinu s velikim i kritičnim utjecajem kao imovinu potrebnu za procese s velikim odnosno kritičnim utjecajem;

iv. utvrđuje područja od velikog i kritičnog utjecaja koja obuhvaćaju sve elemente imovine s velikim odnosno kritičnim utjecajem kako bi se mogao kontrolirati pristup tim područjima;

(d) ocjenjuje rizike za kibernetičku sigurnost tako da odredi prioritete na temelju kriterija za procjenu i prihvaćanje rizika iz stavka 3. točke (b).

5. U fazi obrade kibernetičkosigurnosnih rizika svaki subjekt s velikim ili kritičnim utjecajem dužan je uspostaviti plan za ublažavanje rizika na razini subjekta tako što će odabrati među mogućnostima pristupa riziku primjerenima za upravljanje rizicima i utvrđivanje preostalih rizika.

6. U fazi prihvaćanja kibernetičkosigurnosnih rizika svaki subjekti s velikim ili kritičnim utjecajem odlučuje hoće li prihvatiti preostali rizik na temelju kriterija prihvatljivosti rizika utvrđenih u stavku 3. točki (b).

7. Svaki subjekt s velikim i kritičnim utjecajem dužan je registrirati imovinu utvrđenu u stavku 1. u popisu imovine. Taj popis imovine nije dio izvješća o procjeni rizika.

8. Nadležno tijelo može obaviti inspekcijski pregled imovine na popisu.

Članak 27.

Izvješćivanje o procjeni rizika na razini subjekta

Svi subjekti s velikim i kritičnim utjecajem u roku od 12 mjeseci nakon što prime obavijest o tome da su utvrđeni kao subjekti s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. te svake tri godine nakon toga nadležnom tijelu dostavljaju izvješće koje sadržava sljedeće informacije:

(1) popis kontrola odabranih za plan ublažavanja rizika na razini subjekta u skladu s člankom 26. stavkom 5. s trenutačnim statusom provedbe svake kontrole;

(2) za svaki postupak s velikim ili kritičnim utjecajem na razini Unije, procjenu rizika od ugrožavanja povjerljivosti, cjelovitosti i dostupnosti informacija i relevantnih resursa. Procjena tog rizika provodi se u skladu s matricom utjecaja rizika iz članka 19. stavka 2.;

(3) popis ključnih pružatelja IKT usluga za njihove procese s kritičnim utjecajem.

POGLAVLJE III.

ZAJEDNIČKI OKVIR ZA KIBERNETIČKU SIGURNOST ELEKTROENERGETSKOG SEKTORA

Članak 28.

Sastav, funkcioniranje i preispitivanje zajedničkog okvira za kibernetičku sigurnost elektroenergetskog sektora

1. Zajednički okvir za kibernetičku sigurnost elektroenergetskog sektora sastoji se od sljedećih kontrola i sustava upravljanja kibernetičkom sigurnošću:

(a) minimalne kibernetičkosigurnosne kontrole razvijene u skladu s člankom 29.;

(b) napredne kibernetičkosigurnosne kontrole razvijene u skladu s člankom 29.;

(c) korelacijska matrica, razvijena u skladu s člankom 34. kojom se specificiraju kontrole iz točaka (a) i (b) prema odabranim europskim i međunarodnim normama i nacionalnim zakonodavnim ili regulatornim okvirima;

(d) sustav upravljanja kibernetičkom sigurnošću uspostavljen u skladu s člankom 32.

2. Svi subjekti s velikim utjecajem primjenjuju minimalne kibernetičkosigurnosne kontrole u skladu sa stavkom 1. točkom (a) unutar svojeg područja od velikog utjecaja.

3. Svi subjekti s kritičnim utjecajem primjenjuju napredne kibernetičkosigurnosne kontrole u skladu sa stavkom 1. točkom (b) unutar svojeg područja od kritičnog utjecaja.

4. U roku od sedam mjeseci od podnošenja prvog nacrta izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 4. zajednički okvir za kibernetičku sigurnost elektroenergetskog sektora iz stavka 1. dopunjuje se minimalnim i naprednim kibernetičkosigurnosnim kontrolama u lancu opskrbe razvijenima u skladu s člankom 33.

Članak 29.

Minimalne i napredne kibernetičkosigurnosne kontrole

1. U roku od sedam mjeseci od podnošenja prvog nacrta izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 4. operatori prijenosnih sustava, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, izrađuju prijedlog minimalnih i naprednih kibernetičkosigurnosnih kontrola.

2. U roku od šest mjeseci od sastavljanja regionalnog izvješća o procjeni kibernetičkosigurnosnih rizika u skladu s člankom 21. stavkom 2., operatori prijenosnih sustava, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, nadležnom tijelu predlažu izmjenu minimalnih naprednih kibernetičkosigurnosnih kontrola. Prijedlog se izrađuje u skladu člankom 8. stavkom 10. i njime se uzimaju u obzir rizici utvrđeni u regionalnoj procjeni rizika.

3. Minimalne i napredne kibernetičkosigurnosne kontrole mogu se provjeriti sudjelovanjem u nacionalnom programu provjere u skladu s postupkom iz članka 31. ili revizijama sigurnosti koje provodi neovisna treća strana u skladu sa zahtjevima iz članka 25. stavka 2.

4. Početne minimalne i napredne kibernetičkosigurnosne kontrole razvijene u skladu sa stavkom 1. temelje se na rizicima utvrđenima u izvješću o procjeni kibernetičkosigurnosnih rizika na razini Unije iz članka 19. stavka 5. Izmijenjene minimalne i napredne kibernetičkosigurnosne kontrole razvijene u skladu sa stavkom 2. temelje se na regionalnom izvješću o procjeni kibernetičkosigurnosnih rizika iz članka 21. stavka 2.

5. Minimalne kibernetičkosigurnosne kontrole uključuju kontrole za zaštitu informacija razmijenjenih u skladu s člankom 46.

6. U roku od 12 mjeseci nakon odobrenja minimalnih i naprednih kibernetičkosigurnosnih kontrola u skladu s člankom 8. stavkom 5. ili nakon svakog ažuriranja u skladu s člankom 8. stavkom 10. subjekti iz članka 2. stavka 1. koji su utvrđeni kao subjekti s kritičnim i velikim utjecajem u skladu s člankom 24. tijekom uspostave plana za smanjenje rizika na razini subjekta u skladu s člankom 26. stavkom 5. primjenjuju minimalne kibernetičkosigurnosne kontrole unutar područja od velikog utjecaja i napredne kibernetičkosigurnosne kontrole unutar područja od kritičnog utjecaja.

Članak 30.

Odstupanja od minimalnih i naprednih kibernetičkosigurnosnih kontrola

1. Subjekti iz članka 2. stavka 1. mogu zatražiti od odgovarajućeg nadležnog tijela da im odobri odstupanje od obveze primjene minimalnih i naprednih kibernetičkosigurnosnih kontrola iz članka 29. stavka 6. Nadležno tijelo može odobriti takvo odstupanje zbog jednog od sljedećih razloga:

(a) u iznimnim okolnostima, ako subjekt može dokazati da troškovi provedbe odgovarajućih kibernetičkosigurnosnih kontrola znatno premašuju koristi. ACER i ENTSO za električnu energiju u suradnji s tijelom za ODS-ove mogu zajednički izraditi smjernice za procjenu troškova kibernetičkosigurnosnih kontrola kako bi pomogli subjektima;

(b) ako subjekt dostavlja plan postupanja s rizicima na razini subjekta kojim se ublažavaju kibernetičkosigurnosni rizici primjenom alternativnih kontrola do razine koja je prihvatljiva u skladu s kriterijima prihvatljivosti rizika iz članka 26. stavka 3. točke (b).

2. U roku od tri mjeseca od primitka zahtjeva iz stavka 1. svako nadležno tijelo odlučuje treba li odobriti odstupanje od minimalnih i naprednih kibernetičkosigurnosnih kontrola. Odstupanja od minimalnih ili naprednih kibernetičkosigurnosnih kontrola odobravaju se na najviše tri godine te ih je moguće produljiti.

3. Agregirane i anonimizirane informacije o odobrenim odstupanjima uključuju se kao prilog izvješću o sveobuhvatnoj procjeni prekograničnih kibernetičkosigurnosnih rizika za elektroenergetski sektor iz članka 23. ENTSO za električnu energiju i tijelo EU-a za ODS-ove zajednički ažuriraju popis, prema potrebi.

Članak 31.

Provjera zajedničkog okvira za kibernetičku sigurnost elektroenergetskog sektora

1. Najkasnije 24 mjeseca nakon donošenja kontrola iz članka 28. stavka 1. točaka (a), (b) i (c) i uspostave sustava upravljanja kibernetičkom sigurnošću iz točke (d) tog članka svaki subjekt s kritičnim utjecajem utvrđen u skladu s člankom 24. stavkom 1. mora, na zahtjev nadležnog tijela, moći dokazati svoju usklađenost sa sustavom upravljanja kibernetičkom sigurnošću i minimalnim ili naprednim kibernetičkosigurnosnim kontrolama.

2. Svaki subjekt s kritičnim utjecajem ispunjava obvezu iz stavka 1. pristupanjem reviziji sigurnosti koju provodi neovisna treća strana u skladu sa zahtjevima iz članka 25. stavka 2. ili sudjelovanjem u nacionalnom programu provjere u skladu s člankom 25. stavkom 1.

3. Provjera usklađenosti subjekta s kritičnim utjecajem sa sustavom upravljanja kibernetičkom sigurnošću te minimalnim ili naprednim kibernetičkosigurnosnim kontrolama provodi se na svoj imovini unutar područja od kritičnog utjecaja subjekta s kritičnim utjecajem.

4. Provjera usklađenosti subjekta s kritičnim utjecajem sa sustavom upravljanja kibernetičkom sigurnošću te minimalnim ili naprednim kibernetičkosigurnosnim kontrolama redovito se ponavlja najkasnije 36 mjeseci nakon prve provjere i svake tri godine nakon toga.

5. Svaki subjekt s kritičnim utjecajem definiran u skladu s člankom 24. dokazuje svoju usklađenost s kontrolama iz članka 28. stavka 1. točaka (a), (b) i (c) i uspostavu sustava upravljanja kibernetičkom sigurnošću iz točke (d) tog članka izvješćivanjem nadležnog tijela o ishodu provjere usklađenosti.

Članak 32.

Sustav upravljanja kibernetičkom sigurnošću

1. U roku od 24 mjeseca nakon što ih nadležno tijelo obavijesti da su utvrđeni kao subjekti s velikim ili kritičnim utjecajem u skladu člankom 24. stavkom 6., svi subjekti s velikim i kritičnim utjecajem uspostavljaju sustav upravljanja kibernetičkom sigurnošću i nakon toga ga svake tri godine preispituju kako bi:

(a) utvrdili opseg sustava upravljanja kibernetičkom sigurnošću uzimajući u obzir sučelja s drugim subjektima i ovisnosti o njima;

(b) osigurali da je njihovo više rukovodstvo obaviješteno o relevantnim pravnim obvezama i da aktivno doprinosi provedbi sustava upravljanja kibernetičkom sigurnošću pravodobnim odlukama i brzim reakcijama;

(c) osigurali da imaju na raspolaganju dovoljno resursa potrebnih za sustav upravljanja kibernetičkom sigurnošću;

(d) uspostavili politiku kibernetičke sigurnosti koja se dokumentira i priopćuje subjektu i stranama na koje utječu sigurnosni rizici;

(e) dodijelili i priopćili odgovornosti za uloge relevantne za kibernetičku sigurnost;

(f) upravljali kibernetičkosigurnosnim rizicima na razini subjekta kako je definirano u članku 26.;

(g) utvrdili i osigurali resurse potrebne za provedbu, održavanje i kontinuirano poboljšanje sustava upravljanja kibernetičkom sigurnošću, uzimajući u obzir potrebnu stručnost i informiranost o resursima za kibernetičku sigurnost;

(h) utvrdili unutarnje i vanjske komunikacije relevantne za kibernetičku sigurnost;

(i) izradili, ažurirali i kontrolirali dokumentirane informacije povezane sa sustavom upravljanja kibernetičkom sigurnošću;

(j) ocijenili učinkovitost i djelotvornost sustava upravljanja kibernetičkom sigurnošću;

(k) proveli unutarnje revizije u planiranim vremenskim razmacima kako bi se osiguralo da se sustav upravljanja kibernetičkom sigurnošću djelotvorno provodi i održava;

(l) preispitali provedbu sustava upravljanja kibernetičkom sigurnošću u planiranim vremenskim razmacima; te kontrolirali i ispravili neusklađenosti resursa i aktivnosti s politikama, postupcima i smjernicama u sustavu upravljanja kibernetičkom sigurnošću.

2. Sustav upravljanja kibernetičkom sigurnošću primjenjuje se na svu imovinu unutar područja od velikog i kritičnog utjecaja subjekta s velikim i kritičnim utjecajem.

3. Nadležna tijela, bez nametanja ili diskriminacije u korist uporabe određene vrste tehnologije, potiču primjenu europskih ili međunarodnih normi i specifikacija povezanih sa sustavima upravljanja koje su relevantne za sigurnost mrežnih i informacijskih sustava.

Članak 33.

Minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe

1. U roku od sedam mjeseci od podnošenja prvog nacrta izvješća o procjeni kibernetičkosigurnosnog rizika na razini Unije u skladu s člankom 19. stavkom 4. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, izrađuju prijedlog minimalnih i naprednih kibernetičkosigurnosnih kontrola u lancu opskrbe kojima se ublažavaju rizici u tom lancu utvrđeni u procjenama kibernetičkosigurnosnih rizika na razini Unije, čime dopunjuju minimalne i napredne kibernetičkosigurnosne kontrole razvijene u skladu s člankom 29. Minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe razvijaju se zajedno s minimalnim i naprednim kibernetičkosigurnosnim kontrolama u skladu s člankom 29. Minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe obuhvaćaju cijeli životni ciklus svih IKT proizvoda, usluga i procesa u područjima od velikog ili kritičnog utjecaja subjekta s velikim ili kritičnim utjecajem. U izradi prijedloga za minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe savjetuje se sa skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava.

2. Minimalne kibernetičkosigurnosne kontrole u lancu opskrbe sastoje se od kontrola za subjekte s velikim i kritičnim utjecajem koje ispunjavaju sljedeće zahtjeve:

(a) provjerava se primjena preporuka za nabavu IKT proizvoda, usluga i procesa koje se odnose na specifikacije kibernetičke sigurnosti, pri čemu se obuhvaćaju barem:

i. sigurnosne provjere osoblja dobavljača uključenog u lanac opskrbe koje obrađuje osjetljive informacije ili ima pristup imovini subjekta s velikim ili kritičnim utjecajem. Sigurnosna provjera može uključivati provjeru identiteta i podataka osoblja ili izvoditelja subjekta u skladu s nacionalnim pravom i postupcima te relevantnim i primjenjivim pravom Unije, uključujući Uredbu (EU) 2016/679 i Direktivu (EU) 2016/680 Europskog parlamenta i Vijeća ([18]). Provjere podobnosti moraju biti razmjerne i strogo ograničene na ono što je nužno. Provode se isključivo u svrhu evaluacije potencijalnog sigurnosnog rizika za predmetni subjekt. Moraju biti razmjerne poslovnim zahtjevima, klasifikaciji informacija kojima subjekt treba pristupiti i uočenim rizicima, a može ih obaviti sam subjekt ili vanjsko društvo koje provodi provjeru ili mogu biti napravljene u okviru državne sigurnosne provjere;

ii. procesi za sigurno i kontrolirano projektiranje, razvoj i proizvodnju IKT proizvoda, usluga i procesa, pri čemu se potiče projektiranje i razvoj tih proizvoda, usluga i procesa koji uključuju odgovarajuće tehničke mjere za jamčenje kibernetičke sigurnosti;

iii. projektiranje mrežnih i informacijskih sustava u kojima se uređaji ne smatraju pouzdanima čak i kad su unutar sigurnog područja, unutar kojih se svaki zahtjev mora provjeriti i u kojima se primjenjuje načelo minimalnih potrebnih ovlasti;

iv. pristup dobavljača imovini subjekta;

([18]) Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).

v. ugovorne obveze dobavljača da zaštiti i ograniči pristup osjetljivim informacijama subjekta;

vi. temeljne specifikacije za nabavu u području kibernetičke sigurnosti za podugovaratelje dobavljača;

vii. sljedivost primjene specifikacija kibernetičke sigurnosti od razvoja preko proizvodnje do isporuke IKT proizvoda, usluga ili procesa;

viii. davanje sigurnosnih ažuriranja tijekom cijelog životnog vijeka IKT proizvoda, usluga ili procesa;

ix. pravo na reviziju kibernetičke sigurnosti u dobavljačevim procesima projektiranja, razvoja i proizvodnje; i

x. procjena profila rizičnosti dobavljača;

(b) od takvih subjekata zahtijevaju da prilikom sklapanja ugovora s dobavljačima, partnerima i drugim stranama u lancu opskrbe uzmu u obzir preporuke o nabavi iz točke (a), kojima su obuhvaćene redovne isporuke IKT proizvoda, usluga i procesa i nepredviđeni događaji i okolnosti kao što su raskid i prijenos ugovora drugim stranama zbog nemara ugovornog partnera;

(c) od takvih subjekata zahtijevaju da uzmu u obzir rezultate relevantnih koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe provedenih u skladu s člankom 22. stavkom 1. Direktive (EU) 2022/2555;

(d) obuhvaćaju kriterije za odabir i ugovaranje dobavljača koji mogu ispuniti specifikacije kibernetičke sigurnosti kako je navedeno u točki (a) i koji imaju razinu kibernetičke sigurnosti primjerenu kibernetičkosigurnosnim rizicima IKT proizvoda, usluge ili procesa koje dobavljač isporučuje;

(e) obuhvaćaju kriterije za diversifikaciju izvora opskrbe IKT proizvodima, uslugama i procesima i smanjenje rizika od ovisnosti o pojedinačnom pružatelju usluga;

(f) obuhvaćaju kriterije za redovito praćenje, preispitivanje ili reviziju specifikacija kibernetičke sigurnosti za dobavljačeve unutarnje operativne procese tijekom cijelog životnog ciklusa svakog IKT proizvoda, usluge i procesa.

3. Kad je riječ o specifikacijama kibernetičke sigurnosti u preporuci za nabavu u području kibernetičke sigurnosti iz stavka 2. točke (a), subjekti s velikim ili kritičnim utjecajem primjenjuju načela nabave na temelju Direktive 2014/24/EU Europskog parlamenta i Vijeća ([19]), u skladu s člankom 35. stavkom 4., ili definiraju vlastite specifikacije na temelju rezultata procjene kibernetičkosigurnosnih rizika na razini subjekta.

4. Napredne kibernetičkosigurnosne kontrole u lancu opskrbe uključuju kontrole subjekata s kritičnim utjecajem kako bi se u okviru nabave provjerilo da su IKT proizvodi, usluge i procesi koji će biti imovina s kritičnim utjecajem u skladu sa specifikacijama kibernetičke sigurnosti. IKT proizvod, usluga ili proces provjerava se u okviru europskog programa certifikacije kibernetičke sigurnosti iz članka 31. ili kroz aktivnosti provjere koje odabere i organizira subjekt. Detaljnost i opseg aktivnosti provjere moraju biti dovoljni kako bi se osiguralo da IKT proizvod, usluga ili proces može poslužiti za ublažavanje rizika utvrđenih u procjeni rizika na razini subjekta. Subjekt s kritičnim utjecajem dužan je dokumentirati mjere poduzete za smanjenje utvrđenih rizika.

5. Minimalne i napredne kibernetičkosigurnosne kontrole u lancu opskrbe primjenjuju se na nabavu relevantnih IKT proizvoda, usluga i procesa. Minimalne i napredne kibernetičkosigurnosne kontrole lanca opskrbe primjenjivat će se na postupke nabave u subjektima koji su utvrđeni kao subjekti s velikim i kritičnim utjecajem u skladu s člankom 24. koji počinju šest mjeseci nakon donošenja ili ažuriranja minimalnih i naprednih kibernetičkosigurnosnih kontrola iz članka 29.

([19]) Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

6. U roku od šest mjeseci od sastavljanja svakog regionalnog izvješća o procjeni kibernetičkosigurnosnih rizika u skladu s člankom 21. stavkom 2., operatori prijenosnih sustava uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove nadležnom tijelu predlažu izmjenu minimalnih i naprednih kibernetičkosigurnosnih kontrola u lancu opskrbe. Prijedlog se sastavlja u skladu s člankom 8. stavkom 10. i u njemu se uzimaju u obzir rizici utvrđeni u regionalnoj procjeni rizika.

Članak 34.

Korelacijska matrica za specificiranje kibernetičkosigurnosnih kontrola u području električne energije u odnosu na norme

1. U roku od sedam mjeseci od podnošenja prvog nacrta izvješća o procjeni kibernetičkosigurnosnih rizika na razini Unije u skladu s člankom 19. stavkom 4. OPS-ovi su, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja s ENISA-om, dužni sastaviti prijedlog matrice za specificiranje kontrola iz članka 28. stavka 1. točaka (a) i (b) u odnosu na odabrane europske i međunarodne norme i relevantne tehničke specifikacije („korelacijska matrica"). ENTSO za električnu energiju i tijelo EU-a za ODS-ove dokumentiraju da su različite kontrole ekvivalentne onima iz članka 28. stavka 1. točaka (a) i (b).

2. Nadležna tijela mogu ENTSO-u za električnu energiju i tijelu EU-a za ODS-ove dostaviti pregled kontrola iz članka 28. stavka 1. točaka (a) i (b) upućivanjem na povezane nacionalne zakonodavne ili regulatorne okvire, uključujući relevantne nacionalne norme država članica u skladu s člankom 25. Direktive (EU) 2022/2555. Ako nadležno tijelo države članice dostavi takav korelacijski pregled, ENTSO za električnu energiju i tijelo EU-a za ODS-ove uvrštavaju taj pregled u korelacijsku matricu.

3. U roku od šest mjeseci od izrade svakog regionalnog izvješća o procjeni kibernetičkosigurnosnih rizika u skladu s člankom 21. stavkom 2. operatori prijenosnih sustava dužni su uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove i nakon savjetovanja s ENISA-om predložiti nadležnom tijelu izmjenu korelacijske matrice. Prijedlog se sastavlja u skladu s člankom 8. stavkom 10. i u njemu se uzimaju u obzir rizici utvrđeni u regionalnoj procjeni rizika.

POGLAVLJE IV.

PREPORUKE ZA NABAVU U PODRUČJU KIBERNETIČKE SIGURNOSTI

Članak 35.

Preporuke za nabavu u području kibernetičke sigurnosti

1. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, u okviru programa rada koji će se uspostaviti i ažurirati svaki put kad se donese regionalno izvješće o procjeni kibernetičkosigurnosnih rizika izrađuju skup neobvezujućih preporuka za nabavu u području kibernetičke sigurnosti koje subjekti s velikim i kritičnim utjecajem mogu upotrijebiti kao temelj za nabavu IKT proizvoda, usluga i procesa u područjima od velikog i kritičnog utjecaja. Taj program rada uključuje sljedeće:

(a) opis i klasifikaciju vrsta IKT proizvoda, usluga i procesa koje upotrebljavaju subjekti s velikim i kritičnim utjecajem u području od velikog i kritičnog utjecaja;

(b) popis vrsta IKT proizvoda, usluga i procesa za koje se izrađuje skup neobvezujućih preporuka za nabavu u području kibernetičke sigurnosti na temelju relevantnih regionalnih izvješća o procjeni kibernetičkosigurnosnih rizika i prioriteta subjekata s velikim i kritičnim utjecajem.

2. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, u roku od šest mjeseci nakon donošenja ili ažuriranja regionalnog izvješća o procjeni kibernetičkosigurnosnih rizika dostavlja sažetak tog programa rada ACER-u.

3. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, nastoje osigurati da neobvezujuće preporuke za nabavu u području kibernetičke sigurnosti izrađene na temelju relevantne regionalne procjene kibernetičkosigurnosnih rizika budu slične ili usporedive u svim regijama pogona sustava. Skupovi preporuka za nabavu u području kibernetičke sigurnosti obuhvaćaju barem specifikacije iz članka 33. stavka 2. točke (a). Ako je moguće, specifikacije se odabiru iz europskih i međunarodnih normi.

4. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, osiguravaju da su skupovi preporuka za nabavu u području kibernetičke sigurnosti:

(a) usklađeni s načelima nabave u skladu s Direktivom 2014/24/EU; i

(b) kompatibilni s najnovijim dostupnim europskim programima certifikacije kibernetičke sigurnosti relevantnima za IKT proizvod, uslugu ili proces te uzimaju u obzir te programe.

Članak 36.

Smjernice za upotrebu europskih programa certifikacije kibernetičke sigurnosti za nabavu IKT proizvoda, usluga i procesa

1. Neobvezujuće preporuke za nabavu u području kibernetičke sigurnosti izrađene u skladu s člankom 35. mogu uključivati sektorske smjernice o upotrebi europskih programa certifikacije kibernetičke sigurnosti kad god je dostupan odgovarajući program za određenu vrstu IKT proizvoda, usluge ili procesa koje upotrebljavaju subjekti s kritičnim utjecajem, ne dovodeći u pitanje okvir za uspostavu europskih programa certifikacije kibernetičke sigurnosti u skladu s člankom 46. Uredbe (EU) 2019/881.

2. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, blisko surađuju s ENISA-om pri izradi konkretnih smjernica za sektor koje su uključene u neobvezujuće preporuke za nabavu u području kibernetičke sigurnosti u skladu sa stavkom 1.

POGLAVLJE V.

PROTOK INFORMACIJA, KIBERNETIČKI NAPADI I UPRAVLJANJE KRIZAMA

Članak 37.

Pravila o razmjeni informacija

1. Ako nadležno tijelo primi informacije o kibernetičkom napadu o kojem se izvješćuje, to nadležno tijelo:

(a) procjenjuje razinu povjerljivosti tih informacija i obavješćuje subjekt o ishodu svoje procjene bez nepotrebne odgode, a najkasnije u roku od 24 sata od primitka informacija;

(b) pokušava pronaći svaki drugi sličan kibernetički napad u Uniji koji je prijavljen drugim nadležnim tijelima kako bi se informacije o kibernetičkom napadu o kojem se izvješćuje povezale s informacijama o drugim kibernetičkim napadima te kako bi se obogatile postojeće informacije, ojačali i koordinirali odgovori u području kibernetičke sigurnosti;

(c) odgovorno je za brisanje poslovnih tajni i anonimizaciju informacija u skladu s relevantnim nacionalnim pravilima i pravilima Unije;

(d) bez nepotrebne odgode, a najkasnije 24 sata nakon primitka informacija o kibernetičkom napadu o kojem se izvješćuje, razmjenjuje informacije s nacionalnim jedinstvenim kontaktnim točkama, CSIRT-ovima i svim nadležnim tijelima imenovanima u skladu s člankom 4. u drugim državama članicama te redovito dostavlja ažurirane informacije tim vlastima ili tijelima;

(e) dostavlja informacije o kibernetičkom napadu, nakon anonimizacije i brisanja poslovnih tajni u skladu sa stavkom 1. točkom (c), subjektima s kritičnim utjecajem i velikim utjecajem u svojoj državi članici bez nepotrebne odgode i najkasnije 24 sata nakon primitka informacija u skladu sa stavkom 1. točkom (a) te redovito dostavlja ažurirane informacije kako bi subjekti mogli djelotvorno organizirati svoju obranu;

(f) može zatražiti od izvještajnog subjekta s velikim ili kritičnim utjecajem da informacije o kibernetičkom napadu o kojem se izvješćuje na siguran način dostavi i drugim subjektima koji bi mogli biti pogođeni kako bi se informirali o stanju u elektroenergetskom sektoru i kako bi se spriječilo da dođe do rizika koji bi mogao eskalirati u prekogranični kibernetičkosigurnosni incident u elektroenergetskom sektoru;

(g) nakon anonimizacije i brisanja poslovnih tajni s ENISA-om dostavlja sažeto izvješće s informacijama o kibernetičkom napadu.

2. Ako CSIRT dobije informacije o nezakrpanoj ranjivosti koja se aktivno iskorištava, on:

(a) o tome bez odgode obavješćuje ENISA-u putem odgovarajućeg sigurnog kanala za razmjenu informacija, osim ako je drukčije navedeno u drugim pravnim aktima Unije;

(b) pomaže predmetnom subjektu da od proizvođača ili pružatelja usluga dobije djelotvorno, koordinirano i brzo upravljanje nezakrpanom ranjivošću koja se aktivno iskorištava ili učinkovite i djelotvorne mjere ublažavanja;

(c) razmjenjuje dostupne informacije s dobavljačem i zahtijeva od proizvođača ili pružatelja, ako je to moguće, da utvrdi popis CSIRT-ova u državama članicama na koje bi mogla utjecati nezakrpana ranjivost koja se aktivno iskorištava i koje se o tome obavješćuju;

(d) razmjenjuje dostupne informacije s CSIRT-ovima utvrđenima u prethodnoj točki na temelju načela nužnosti pristupa informacijama;

(e) razmjenjuje, ako postoje, strategije i mjere ublažavanja prijavljene nezakrpane ranjivosti koja se aktivno iskorištava.

3. Ako nadležno tijelo dobije informacije o nezakrpanoj ranjivosti koja se aktivno iskorištava, to nadležno tijelo:

(a) razmjenjuje, ako postoje, strategije i mjere ublažavanja prijavljene nezakrpane ranjivosti koja se aktivno iskorištava u koordinaciji s CSIRT-ovima;

(b) razmjenjuje informacije s CSIRT-om u državi članici u kojoj je prijavljena nezakrpana ranjivost koja se aktivno iskorištava.

4. Ako nadležno tijelo sazna za nezakrpanu ranjivost za koju nema dokaza da se već aktivno iskorištava, bez nepotrebne odgode surađuje s CSIRT-om za potrebe koordiniranog otkrivanja ranjivosti kako je utvrđeno u članku 12. stavku 1. Direktive (EU) 2022/2555.

5. Ako CSIRT primi informacije o kibernetičkim prijetnjama od jednog ili više subjekata s velikim ili kritičnim utjecajem u skladu s člankom 38. stavkom 6., on te informacije ili sve druge informacije koje su važne za sprečavanje, otkrivanje, ublažavanje povezanog rizika ili odgovaranje na taj rizik dostavlja subjektima s kritičnim i velikim utjecajem u svojoj državi članici te, prema potrebi, svim predmetnim CSIRT-ovima i svojoj nacionalnoj jedinstvenoj kontaktnoj točki bez nepotrebne odgode i najkasnije četiri sata nakon primitka informacija.

6. Ako dobije informacije o kibernetičkim prijetnjama od jednog ili više subjekata s velikim ili kritičnim utjecajem, nadležno tijelo te informacije prosljeđuje CSIRT-u za potrebe stavka 5.

7. Nadležna tijela mogu u cijelosti ili djelomično delegirati odgovornosti iz stavaka 3. i 4. koje se odnose na jedan ili više subjekata s velikim ili kritičnim utjecajem koji posluju u više država članica drugom nadležnom tijelu u jednoj od tih država članica, nakon što predmetna nadležna tijela postignu dogovor.

8. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i u suradnji s tijelom EU-a za ODS-ove, razvijaju metodologiju s klasifikacijskom ljestvicom za kibernetičke napade do 13. lipnja 2025. OPS-ovi, uz pomoć ENTSO-a za električnu energiju i tijela EU-a za ODS-ove, mogu zatražiti od nadležnih tijela da se savjetuju s ENISA-om i nacionalnim tijelima nadležnima za kibernetičku sigurnost kako bi im pomogli u izradi takve klasifikacijske ljestvice. Metodologija omogućuje klasifikaciju ozbiljnosti kibernetičkog napada na pet razina, pri čemu su dvije najviše razine „velika" i „kritična". Klasifikacija se temelji na procjeni sljedećih parametara:

(a) mogućeg utjecaja s obzirom na izloženu imovinu i područja utvrđena u skladu s člankom 26. stavkom 4. točkom (c); i

(b) ozbiljnosti kibernetičkog napada.

9. Do 13. lipnja 2026. ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove provodi studiju izvedivosti kako bi procijenio mogućnost i financijske troškove potrebne za razvoj zajedničkog alata kojim se svim subjektima omogućuje razmjena informacija s relevantnim nacionalnim tijelima.

10. U studiji izvedivosti razmatra se mogućnost da se takav zajednički alat:

(a) koristi kako bi se subjektima s kritičnim i velikim utjecajem dostavile relevantne informacije koje se odnose na sigurnost operacija prekograničnih protoka električne energije, kao što su izvješćivanje o kibernetičkim napadima u gotovo stvarnom vremenu, rano uzbunjivanje u vezi s pitanjima kibernetičke sigurnosti i informacije o nezakrpanim ranjivostima na opremi koja se upotrebljava u elektroenergetskom sustavu;

(b) održava u prikladnom i vrlo pouzdanom okruženju;

(c) koristi za prikupljanje podataka od subjekata s kritičnim i velikim utjecajem te olakšavanje brisanja povjerljivih informacija i anonimizaciju podataka te njihovo brzo dostavljanje subjektima s kritičnim i velikim utjecajem.

11. ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove:

(a) pri procjeni izvedivosti savjetuje se s ENISA-om i skupinom za suradnju u području mrežne i informacijske sigurnosti, nacionalnim jedinstvenim kontaktnim točkama i predstavnicima glavnih dionika;

(b) predstavlja rezultate studije izvedivosti ACER-u i skupini za suradnju u području sigurnosti mrežnih i informacijskih sustava.

12. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, može analizirati i olakšati inicijative koje predlažu subjekti s kritičnim i velikim utjecajem radi evaluacije i ispitivanja takvih alata za razmjenu informacija.

Članak 38.

Uloga subjekata s velikim i kritičnim utjecajem u razmjeni informacija

1. Svaki subjekt s velikim ili kritičnim utjecajem:

(a) utvrđuje, za svu imovinu u okviru svojeg područja kibernetičke sigurnosti određenog u skladu s člankom 26. stavkom 4. točkom (c), barem kapacitete operativnog centra za kibernetičku sigurnost („CSOC") za:

   i. osiguravanje da se u okviru relevantnih mrežnih i informacijskih sustava i aplikacija vode sigurnosni zapisi za praćenje sigurnosti kako bi se omogućilo otkrivanje nepravilnosti i prikupljanje informacija o kibernetičkim napadima;

   ii. provedbu praćenja sigurnosti, uključujući otkrivanje neovlaštenih ulazaka i procjenu ranjivosti mrežnih i informacijskih sustava;

   iii. analizu i, prema potrebi, poduzimanje svih potrebnih mjera u okviru svoje odgovornosti i sposobnosti zaštite subjekta;

   iv. sudjelovanje u prikupljanju i razmjeni informacija koje su opisane u ovom članku;

(b) ima pravo nabaviti sve te kapacitete ili njihove dijelove u skladu s točkom (a) putem MSSP-ova. Subjekti s kritičnim i velikim utjecajem i dalje su odgovorni za MSSP-ove i nadziru mjere koje poduzimaju;

(c) određuje subjektovu jedinstvenu kontaktnu točku za potrebe razmjene informacija.

2. ENISA može izdati neobvezujuće smjernice o uspostavi takvih kapaciteta ili podugovaranju usluge pružateljima usluga u državama članicama, kao dio zadaće utvrđene u članku 6. stavku 2. Uredbe (EU) 2019/881.

3. Svaki subjekt s kritičnim i velikim utjecajem razmjenjuje relevantne informacije povezane s kibernetičkim napadom o kojem se izvješćuje sa svojim CSIRT-ovima i svojim nadležnim tijelom bez nepotrebne odgode, a najkasnije četiri sata nakon što je saznao da se o incidentu mora izvijestiti.

4. Smatra se da se mora izvijestiti o informacijama o kibernetičkom napadu ako pogođeni subjekt ocijeni kritičnost kibernetičkog napada u rasponu od „velike" do „kritične" u skladu s metodologijom s klasifikacijskom ljestvicom za kibernetičke napade u skladu s člankom 37. stavkom 8. Subjektova jedinstvena kontaktna točka imenovana u skladu sa stavkom 1. točkom (c) obavješćuje o klasifikaciji incidenta.

5. Ako subjekti s kritičnim utjecajem i subjekti s velikim utjecajem dostave CSIRT-u relevantne informacije o nezakrpanim ranjivostima koje se aktivno iskorištavaju, on te informacije može proslijediti svojem nadležnom tijelu. S obzirom na razinu osjetljivosti dostavljenih informacija CSIRT može uskratiti informacije ili odgoditi njihovo prosljeđivanje zbog opravdanih razloga povezanih s kibernetičkom sigurnošću.

6. Svaki subjekt s kritičnim utjecajem i subjekt s velikim utjecajem bez nepotrebne odgode svojim CSIRT-ovima dostavlja sve informacije o kibernetičkim prijetnjama o kojima se izvješćuje i koje bi mogle imati prekogranični utjecaj. Smatra se da se mora izvijestiti o informacijama o kibernetičkom napadu ako je ispunjen barem jedan od sljedećih uvjeta:

(a) sadržavaju informacije relevantne drugim subjektima s kritičnim utjecajem ili velikim utjecajem radi sprečavanja, otkrivanja rizika ili odgovaranja na njega ili ublažavanja njegovih posljedica;

(b) utvrđene tehnike, taktike i postupci koji se upotrebljavaju u okviru napada dovode do informacija kao što su ugrožene URL adrese ili IP adrese, kontrolni identifikacijski brojevi ili bilo koji drugi podatak koristan za kontekstualizaciju i povezivanje napada;

(c) kibernetička prijetnja može se dodatno procijeniti i kontekstualizirati dodatnim informacijama koje pružaju pružatelji usluga ili treće strane koje ne podliježu ovoj Uredbi.

7. Svi subjekti s kritičnim utjecajem i subjekti s velikim utjecajem pri razmjeni informacija u skladu s ovim člankom navode sljedeće:

(a) da su informacije dostavljene u skladu s ovom Uredbom;

(b) odnose li se informacije na:

i. kibernetički napad o kojem se izvješćuje iz stavka 3.;

ii. nezakrpane ranjivosti koje se aktivno iskorištavaju i koje nisu javno poznate iz stavka 4.;

iii. kibernetičku prijetnju o kojoj se izvješćuje iz stavka 5.

(c) za kibernetički napad o kojem se izvješćuje, njegovu razinu prema metodologiji s klasifikacijskom ljestvicom za kibernetičke napade iz članka 37. stavka 8. i informacije koje dovode do te klasifikacije, uključujući barem kritičnost kibernetičkog napada.

8. Ako subjekt s kritičnim ili velikim utjecajem obavijesti o značajnom incidentu u skladu s člankom 23. Direktive (EU) 2022/2555, a izvješćivanje o incidentima na temelju tog članka sadržava relevantne informacije kako je propisano stavkom 3. ovog članka, izvješćivanje subjekta u skladu s člankom 23. stavkom 1. te direktive predstavlja izvješćivanje o informacijama iz stavka 3. ovog članka.

9. Svi subjekti s kritičnim utjecajem i subjekti s velikim utjecajem izvješćuju svoje nadležno tijelo ili CSIRT tako što jasno utvrđuju konkretne informacije koje se dijele s nadležnim tijelom ili CSIRT-om samo ako bi razmjena informacija mogla dovesti do kibernetičkog napada. Svi subjekti s kritičnim utjecajem i subjekti s velikim utjecajem imaju pravo nadležnom CSIRT-u dostaviti verziju informacija koja nije povjerljiva.

Članak 39.

Otkrivanje kibernetičkih napada i postupanje s povezanim informacijama

1. Subjekti s kritičnim utjecajem i subjekti s velikim utjecajem uspostavljaju potrebne kapacitete za postupanje s otkrivenim kibernetičkim napadima uz potrebnu potporu relevantnog nadležnog tijela, ENTSO-a za električnu energiju i tijela EU-a za ODS-ove. Subjekte s kritičnim utjecajem i subjekte s velikim utjecajem može podupirati CSIRT imenovan u njihovoj pojedinačnoj državi članici u okviru zadaće dodijeljene CSIRT-ovima na temelju članka 11. stavka 5. točke (a) Direktive (EU) 2022/2555. Subjekti s kritičnim utjecajem i subjekti s velikim utjecajem provode djelotvorne postupke za utvrđivanje i klasifikaciju kibernetičkih napada koji će utjecati ili bi mogli utjecati na prekogranične protoke električne energije te odgovor na njih kako bi se njihove posljedice svele na najmanju mjeru.

2. Ako kibernetički napad utječe na prekogranične protoke električne energije, jedinstvene kontaktne točke pogođenih subjekata s kritičnim utjecajem i subjekata s velikim utjecajem surađuju radi međusobne razmjene informacija koju koordinira nadležno tijelo države članice u kojoj je prvi put izviješteno o kibernetičkom napadu.

3. Subjekti s kritičnim utjecajem i subjekti s velikim utjecajem:

(a) osiguravaju da njihova jedinstvena kontaktna točka na razini subjekta ima pristup informacijama koje su primili od nacionalne jedinstvene kontaktne točke preko svojeg nadležnog tijela na temelju nužnosti pristupa informacijama;

(b) osim ako je to već učinjeno u skladu s člankom 3. stavkom 4. Direktive (EU) 2022/2555, obavješćuju nadležno tijelo države članice u kojoj imaju poslovni nastan i nacionalnu jedinstvenu kontaktnu točku o popisu svojih jedinstvenih kontaktnih točaka za kibernetičku sigurnost na razini subjekta:

   i. od kojih to nadležno tijelo i nacionalna jedinstvena kontaktna točka mogu očekivati da će primiti informacije o kibernetičkim napadima o kojima se mora izvijestiti;

   ii. kojima će nadležna tijela i nacionalne jedinstvene kontaktne točke možda morati dostaviti informacije;

(c) uspostavljaju postupke za upravljanje kibernetičkim napadima za kibernetičke napade, uključujući uloge i odgovornosti, zadaće i reakcije na temelju zabilježenog razvoja kibernetičkih napada u područjima od kritičnog i velikog utjecaja;

(d) testiraju opće postupke za upravljanje kibernetičkim napadima najmanje svake godine tako što testiraju barem jedan scenarij koji izravno ili neizravno utječe na prekogranične protoke električne energije. To godišnje testiranje mogu provoditi subjekti s kritičnim i velikim utjecajem tijekom redovitih vježbi iz članka 43. Sve aktivnosti odgovaranja u stvarnom vremenu na kibernetičke napade s posljedicama koji se klasificiraju kao najmanje druga razina prema metodologiji s klasifikacijskom ljestvicom za kibernetičke napade iz članka 37. stavka 8. i čiji je temeljni uzrok povezan s kibernetičkom sigurnošću mogu poslužiti kao godišnje testiranje plana odgovora na kibernetičke napade.

4. Države članice mogu delegirati zadaće iz stavka 1. i regionalnim koordinacijskim centrima u skladu s člankom 37. stavkom 2. Uredbe (EU) 2019/943.

Članak 40.

Upravljanje krizom

1. Ako nadležno tijelo utvrdi da je elektroenergetska kriza povezana s kibernetičkim napadom koji ima posljedice u više država članica, nadležna tijela iz pogođenih država članica, nadležna tijela odgovorna za kibernetičku sigurnost, nadležna tijela za pripravnost za rizike i tijela za upravljanje kibernetičkosigurnosnim krizama u području mrežne i informacijske sigurnosti iz pogođenih država članica zajednički osnivaju *ad hoc* skupinu za koordinaciju prekograničnih kriznih situacija.

2. *Ad hoc* skupina za koordinaciju prekograničnih kriznih situacija:

(a) koordinira učinkovito prikupljanje i daljnju razmjenu svih relevantnih informacija o kibernetičkoj sigurnosti subjektima uključenima u proces upravljanja krizama;

(b) organizira komunikaciju između svih subjekata pogođenih krizom i nadležnih tijela kako bi se smanjila preklapanja i povećala učinkovitost analiza i tehničkih odgovora za rješavanje istodobnih elektroenergetskih kriza čiji je temeljni uzrok povezan s kibernetičkom sigurnošću;

(c) pruža, u suradnji s nadležnim CSIRT-ovima, potrebno stručno znanje, uključujući operativne savjete o provedbi mogućih mjera ublažavanja, za subjekte pogođene incidentom;

(d) obavješćuje Komisiju i Koordinacijsku skupinu za električnu energiju te ih redovito obavješćuje o stanju incidenta u skladu s načelima zaštite utvrđenima u članku 46.;

(e) traži savjet od relevantnih tijela, agencija ili subjekata koji bi mogli pomoći u ublažavanju elektroenergetske krize.

3. Ako se kibernetički napad može smatrati kibernetičkosigurnosnim incidentom velikih razmjera ili se očekuje da će ga se smatrati kibernetičkosigurnosnim incidentom velikih razmjera, *ad hoc* skupina za koordinaciju prekograničnih kriznih situacija odmah obavješćuje nacionalna tijela za upravljanje kibernetičkim krizama u skladu s člankom 9. stavkom 1. Direktive (EU) 2022/2555 u državama članicama pogođenima incidentom, kao i Komisiju i mrežu EU CyCLONe. U takvoj situaciji *ad hoc* skupina za koordinaciju prekograničnih kriznih situacija dostavlja mreži EU CyCLONe informacije o sektorskim posebnostima.

4. Subjekti s kritičnim utjecajem i velikim utjecajem razvijaju i imaju na raspolaganju kapacitete, interne smjernice, planove pripravnosti i osoblje za sudjelovanje u otkrivanju i ublažavanju prekograničnih kriza. Subjekt s kritičnim utjecajem ili velikim utjecajem na koji je utjecala istodobna elektroenergetska kriza istražuje temeljni uzrok takve krize u suradnji sa svojim nadležnim tijelom kako bi se utvrdilo u kojoj je mjeri kriza povezana s kibernetičkim napadom.

5. Države članice mogu delegirati zadaće iz stavka 4. i regionalnim koordinacijskim centrima u skladu s člankom 37. stavkom 2. Uredbe (EU) 2019/943.

Članak 41.

Planovi za upravljanje krizama u području kibernetičke sigurnosti i odgovor na njih

1. U roku od 24 mjeseca nakon dostavljanja ACER-u izvješća o procjeni rizika na razini Unije, ACER u bliskoj suradnji s ENISA-om, ENTSO-om za električnu energiju, tijelom EU-a za ODS-ove, nadležnim tijelima odgovornima za kibernetičku sigurnost, nadležnim tijelima, nadležnim tijelima za pripravnost za rizike, nacionalnim regulatornim tijelima i nacionalnim tijelima za upravljanje kibernetičkosigurnosnim krizama u području mrežne i informacijske sigurnosti izrađuje plan za upravljanje kibernetičkosigurnosnim krizama i odgovor na njih na razini Unije.

2. U roku od 12 mjeseci nakon što ACER izradi plan upravljanja kibernetičkosigurnosnim krizama i odgovor na njih na razini Unije za elektroenergetski sektor u skladu sa stavkom 1., svako nadležno tijelo izrađuje nacionalni plan za upravljanje kibernetičkosigurnosnim krizama i odgovor na njih za prekogranične protoke električne energije, uzimajući u obzir plan upravljanja kibernetičkosigurnosnim krizama na razini Unije i nacionalni plan pripravnosti na rizike uspostavljen u skladu s člankom 10. Uredbe (EU) 2019/941. Taj plan mora biti u skladu s planom za odgovor na kibernetičkosigurnosne incidente velikih razmjera i kibernetičkosigurnosne krize u skladu s člankom 9. stavkom 4. Direktive (EU) 2022/2555. Nadležno tijelo djeluje koordinirano sa subjektima s kritičnim i velikim utjecajem te s nadležnim tijelima za pripravnost za rizike u svojoj državi članici.

3. Nacionalni plan za odgovor na kibernetičkosigurnosne incidente velikih razmjera i kibernetičkosigurnosne krize koji se zahtijeva na temelju članka 9. stavka 4. Direktive (EU) 2022/2555 smatra se nacionalnim planom za upravljanje kibernetičkosigurnosnim krizama na temelju ovog članka ako uključuje odredbe o upravljanju krizama i odgovoru na njih za prekogranične protoke električne energije.

4. Zadaće navedene u stavcima 1. i 2. države članice mogu delegirati i regionalnim koordinacijskim centrima u skladu s člankom 37. stavkom 2. Uredbe (EU) 2019/943.

5. Subjekti s kritičnim i velikim utjecajem osiguravaju da njihovi procesi upravljanja kibernetičkosigurnosnim krizama ispunjavaju sljedeće uvjete:

(a) sadržavaju kompatibilne postupke rješavanja prekograničnih kibernetičkosigurnosnih incidenata kako su definirani u članku 6. stavku 8. Direktive (EU) 2022/2555 koji su formalno uključeni u njihove planove za upravljanje krizama;

(b) dio su općih aktivnosti upravljanja kriznim situacijama.

6. U roku od 12 mjeseci nakon što prime obavijest o tome da su utvrđeni kao subjekti s velikim i kritičnim utjecajem u skladu s člankom 24. stavkom 6. i svake tri godine nakon toga ti subjekti izrađuju plan upravljanja krizama na razini subjekta za kibernetičkosigurnosnu krizu koji se uključuje u njihove opće planove upravljanja krizama. Taj plan obuhvaća barem sljedeće:

(a) pravila o proglašenju krize kako su utvrđena u članku 14. stavcima 2. i 3. Uredbe (EU) 2019/941;

(b) jasne uloge i odgovornosti za upravljanje krizama, uključujući ulogu drugih relevantnih subjekata s kritičnim i velikim utjecajem;

(c) ažurirane informacije za kontakt, kao i pravila za komunikaciju i razmjenu informacija tijekom krizne situacije, uključujući vezu s CSIRT-ovima.

7. Mjere za upravljanje krizama u skladu s člankom 21. stavkom 2. točkom (c) Direktive (EU) 2022/2555 smatraju se planom upravljanja krizama na razini subjekta za elektroenergetski sektor u skladu s ovim člankom ako uključuje sve zahtjeve navedene u stavku 6.

8. Planovi upravljanja krizama testiraju se tijekom vježbi u području kibernetičke sigurnosti iz članaka 43., 44. i 45.

9. Subjekti s kritičnim utjecajem i velikim utjecajem uključuju svoje planove upravljanja krizama na razini subjekta u svoje planove kontinuiteta poslovanja za procese s kritičnim ili velikim utjecajem. Planovi upravljanja kriznim situacijama na razini subjekta uključuju:

(a) postupke koji ovise o dostupnosti, cjelovitosti i pouzdanosti IT usluga;

(b) sve lokacije za kontinuitet poslovanja, uključujući lokacije za hardver i softver;

(c) sve unutarnje uloge i odgovornosti povezane s procesima kontinuiteta poslovanja.

10. Subjekti s kritičnim i velikim utjecajem ažuriraju svoje planove upravljanja krizama na razini subjekta najmanje svake tri godine i kad god je to potrebno.

11. ACER ažurira plan upravljanja krizama u području kibernetičke sigurnosti i odgovora na njih na razini Unije za elektroenergetski sektor izrađen u skladu sa stavkom 1. najmanje svake tri godine i kad god je to potrebno.

12. Svako nadležno tijelo ažurira nacionalni plan za upravljanje krizama u području kibernetičke sigurnosti i odgovora na njih za prekogranične protoke električne energije izrađen u skladu sa stavkom 2. najmanje svake tri godine i kad god je to potrebno.

13. Subjekti s kritičnim utjecajem i velikim utjecajem testiraju svoje planove kontinuiteta poslovanja najmanje jednom svake tri godine ili nakon velikih promjena u procesu s kritičnim utjecajem. Rezultati testiranja plana kontinuiteta poslovanja dokumentiraju se. Subjekti s kritičnim utjecajem i velikim utjecajem mogu uključiti ispitivanje svojeg plana kontinuiteta poslovanja u vježbe u području kibernetičke sigurnosti.

14. Subjekti s kritičnim utjecajem ili velikim utjecajem ažuriraju svoj plan kontinuiteta poslovanja kad god je to potrebno, a najmanje jednom svake tri godine, uzimajući u obzir ishod ispitivanja.

15. Ako se testiranjem utvrde nedostaci u planu kontinuiteta poslovanja, subjekt s kritičnim ili velikim utjecajem te nedostatke ispravlja u roku od 180 kalendarskih dana nakon ispitivanja i provodi novo ispitivanje kako bi dokazao da su korektivne mjere djelotvorne.

16. Ako subjekt s kritičnim ili velikim utjecajem ne može ispraviti nedostatke u roku od 180 kalendarskih dana, on o tome dostavlja izvješće svojem nadležnom tijelu u skladu s člankom 27., u kojem navodi razloge za to.

Članak 42.

Kapaciteti za rano uzbunjivanje u području kibernetičke sigurnosti za elektroenergetski sektor

1. Nadležna tijela surađuju s ENISA-om na razvoju kapaciteta ranog upozoravanja u području kibernetičke sigurnosti za elektroenergetski sektor (ECEAC) u okviru pomoći državama članicama u skladu s člankom 6. stavkom 2. i člankom 7. Uredbe (EU) 2019/881.

2. ECEAC omogućuje ENISA-i da pri obavljanju zadaća navedenih u članku 7. stavku 7. Uredbe (EU) 2019/881:

(a) prikuplja dobrovoljno razmijenjene informacije od:

i. CSIRT-ova, nadležnih tijela;

ii. subjekata iz članka 2. ove Uredbe;

iii. svakog drugog subjekta koji želi dijeliti relevantne informacije na dobrovoljnoj osnovi;

(b) procijeni i klasificira prikupljene informacije;

(c) procijeni informacije kojima ENISA ima pristup za utvrđivanje uvjeta kibernetičkosigurnosnih rizika i relevantnih pokazatelja za aspekte prekograničnih protoka električne energije;

(d) utvrdi uvjete i pokazatelje koji su često povezani s kibernetičkim napadima u elektroenergetskom sektoru;

(e) utvrdi hoće li se provesti daljnja analiza i preventivne mjere procjenom i utvrđivanjem čimbenika rizika;

(f) obavješćuje nadležna tijela o utvrđenim rizicima i konkretnim preporučenim preventivnim mjerama za predmetne subjekte;

(g) obavješćuje sve relevantne subjekte iz članka 2. o rezultatima informacija procijenjenih u skladu s točkama (b), (c) i (d) ovog stavka;

(h) periodično uključuje relevantne informacije u izvješće o informiranosti o stanju, koje se izdaje u skladu s člankom 7. stavkom 6. Uredbe (EU) 2019/881;

i. ako je to moguće, izvodi primjenjive podatke koji upućuju na moguću povredu sigurnosti ili kibernetički napad („pokazatelji ugroženosti”) iz prikupljenih informacija.

3. CSIRT-ovi bez odgode prosljeđuju informacije primljene od ENISA-e predmetnim subjektima u okviru svojih zadaća utvrđenih u članku 11. stavku 3. točki (b) Direktive (EU) 2022/2555.

4. ACER prati djelotvornost ECEAC-a. ENISA pomaže ACER-u tako što mu dostavlja sve potrebne informacije u skladu s člankom 6. stavkom 2. i člankom 7. stavkom 1. Uredbe (EU) 2019/881. Analiza te aktivnosti praćenja dio je praćenja u skladu s člankom 12. ove Uredbe.

POGLAVLJE VI.

OKVIR ZA VJEŽBE U PODRUČJU KIBERNETIČKE SIGURNOSTI U ELEKTROENERGETSKOM SEKTORU

Članak 43.

Vježbe u području kibernetičke sigurnosti na razini subjekta i država članica

1. Do 31. prosinca godine nakon primanja obavijesti o tome da je utvrđen kao subjekt s kritičnim utjecajem i svake tri godine nakon toga svaki takav subjekt dužan je izvesti vježbu u području kibernetičke sigurnosti u koja je obuhvaćen najmanje jedan scenarij s kibernetičkim napadom koji izravno ili neizravno utječu na prekogranične protoke električne energije i koji je povezan s rizicima utvrđenima tijekom procjena kibernetičkosigurnosnih rizika na razini države članice i subjekta u skladu s člancima 20. i 27.

2. Odstupajući od stavka 1., nadležno tijelo za pripravnost za rizike može nakon savjetovanja s nadležnim tijelom i relevantnim tijelom za upravljanje kibernetičkosigurnosnim krizama kako je imenovano ili uspostavljeno u skladu s člankom 9. Direktive (EU) 2022/2555 odlučiti organizirati vježbu u području kibernetičke sigurnosti na razini države članice kako je opisano u stavku 1. umjesto da provodi takvu vježbu na razini subjekta. U tu svrhu nadležno tijelo obavješćuje:

(a) sve subjekte svoje države članice s kritičnim utjecajem, nacionalna regulatorna tijela, CSIRT-ove i nadležna tijela odgovorna za kibernetičku sigurnost najkasnije do 30. lipnja godine koja prethodi vježbi u području kibernetičke sigurnosti na razini subjekta;

(b) svakog subjekta koji sudjeluje u vježbi u području kibernetičke sigurnosti na razini država članica najkasnije šest mjeseci prije početka vježbe.

3. Nadležno tijelo za pripravnost za rizike uz tehničku potporu svojih CSIRT-ova organizira vježbu u području kibernetičke sigurnosti opisanu u stavku 2. na razini države članice neovisno ili u kontekstu druge vježbe u području kibernetičke sigurnosti u toj državi članici. Kako bi se te vježbe mogle grupirati, nadležno tijelo za pripravnost za rizike može odgoditi vježbu u području kibernetičke sigurnosti na razini države članice iz stavka 1. za godinu dana.

4. Vježbe u području kibernetičke sigurnosti na razini subjekta i na razini država članica moraju biti u skladu s nacionalnim okvirima za upravljanje krizama u području kibernetičke sigurnosti u skladu s člankom 9. stavkom 4. točkom (d) Direktive (EU) 2022/2555.

5. Do 31. prosinca 2026. i svake tri godine nakon toga ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove stavlja na raspolaganje predložak scenarija za izvođenje vježbi u području kibernetičke sigurnosti na razini subjekta i država članica iz stavka 1. U tom predlošku uzimaju se u obzir najnovije procjene kibernetičkosigurnosnih rizika na razini subjekta i država članica te su u njemu definirani glavni kriteriji uspješnosti. ENTSO za električnu energiju i tijelo EU-a za ODS-ove uključuju ACER i ENISA-u u izradu takvog predloška.

Članak 44.

Regionalne ili međuregionalne vježbe u području kibernetičke sigurnosti

1. Do 31. prosinca 2029. i svake tri godine nakon toga u svakoj regiji pogona sustava ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove organizira regionalnu vježbu u području kibernetičke sigurnosti. Subjekti s kritičnim utjecajem u regiji pogona sustava sudjeluju u regionalnoj vježbi u području kibernetičke sigurnosti. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, može umjesto regionalne vježbe u području kibernetičke sigurnosti organizirati međuregionalnu vježbu u više regija pogona sustava u istom razdoblju. U vježbi bi trebalo uzeti u obzir druge postojeće procjene i scenarije kibernetičkosigurnosnih rizika izrađene na razini Unije.

2. ENISA podupire ENTSO za električnu energiju i tijelo EU-a za ODS-ove u pripremi i organizaciji vježbe za kibernetičku sigurnost na regionalnoj ili međuregionalnoj razini.

3. ENTSO za električnu energiju, u koordinaciji s tijelom EU-a za ODS-ove, obavješćuje subjekte s kritičnim utjecajem koji sudjeluju u regionalnoj ili međuregionalnoj vježbi u području kibernetičke sigurnosti šest mjeseci prije početka vježbe.

4. Organizator redovite vježbe u području kibernetičke sigurnosti na razini Unije u skladu s člankom 7. stavkom 5. Uredbe (EU) 2019/881 ili bilo koje obvezne vježbe u području kibernetičke sigurnosti povezane s elektroenergetskim sektorom unutar istog geografskog područja može pozvati ENTSO za električnu energiju i tijelo EU-a za ODS-ove da sudjeluju u takvim vježbama. U takvim se slučajevima ne primjenjuje obveza iz stavka 1. ako svi subjekti s kritičnim utjecajem u regiji pogona sustava sudjeluju u istoj vježbi.

5. Ako u vježbi u području kibernetičke sigurnosti iz stavka 4. sudjeluju ENTSO za električnu energiju i tijelo EU-a za ODS-ove, onu mogu godinu dana odgoditi regionalnu ili međuregionalnu vježbu za kibernetičku sigurnost iz stavka 1.

6. Do 31. prosinca 2027. i svake tri godine nakon tog datuma ENTSO za električnu energiju dužan je u suradnji s tijelom EU-a za ODS-ove staviti na raspolaganje predložak vježbe za provedbu regionalnih i međuregionalnih vježbi u području kibernetičke sigurnosti. U tom predlošku uzimaju se u obzir najnovije procjene kibernetičkosigurnosnih rizika na regionalnoj razini te su u njemu definirani glavni kriteriji uspješnosti. ENTSO za električnu energiju savjetuje se s Komisijom i može zatražiti savjet ACER-a, ENISA-e i Zajedničkog istraživačkog centra o organizaciji i provedbi regionalnih i međuregionalnih vježbi u području kibernetičke sigurnosti.

Članak 45.

Ishod vježbi u području kibernetičke sigurnosti na razini subjekta, razini države članice, regionalnoj razini ili međuregionalnoj razini

1. Na zahtjev subjekta s kritičnim utjecajem pružatelji ključnih usluga sudjeluju u vježbama u području kibernetičke sigurnosti iz članka 43. stavaka 1. i 2. i iz članka 44. stavka 1. kad pružaju usluge subjektu s kritičnim utjecajem u području koje odgovara opsegu relevantne vježbe u području kibernetičke sigurnosti.

2. Organizatori vježbi u području kibernetičke sigurnosti iz članka 43. stavaka 1. i 2. i iz članka 44. stavka 1. uz savjetovanje s ENISA-om na njihov zahtjev i u skladu s člankom 7. stavkom 5. Uredbe (EU) 2019/881 analiziraju i dovršavaju relevantnu vježbu u području kibernetičke sigurnosti u obliku izvješća u kojem su sažeta stečena iskustva i koje je upućeno svim sudionicima. Izvješće mora sadržavati:

(a) scenarije vježbi, izvješća sa sastanaka, glavna stajališta, uspjehe i stečena iskustva na bilo kojoj razini lanca vrijednosti elektroenergetskog sektora;

(b) zaključak jesu li ispunjeni ključni kriteriji uspješnosti;

(c) popis preporuka za subjekte koji sudjeluju u relevantnoj vježbi u području kibernetičke sigurnosti radi ispravljanja, prilagođavanja ili mijenjanja procesa, postupaka, povezanih modela upravljanja u krizama u području kibernetičke sigurnosti i svih postojećih ugovornih odnosa s pružateljima ključnih usluga.

3. Ako to zatraži mreža CSIRT-ova, skupina za suradnju u području mrežne i informacijske sigurnosti ili mreža EU CyCLONe, organizatori vježbi u području kibernetičke sigurnosti iz članka 43. stavaka 1. i 2. te iz članka 44. stavka 1. razmjenjuju informacije o ishodu relevantne vježbe u području kibernetičke sigurnosti. Organizatori sa svakim subjektom koji sudjeluje u vježbama razmjenjuju informacije iz stavka 2. točaka (a) i (b) ovog članka. Organizatori dijele popis preporuka iz tog stavka točke (c) isključivo sa subjektima navedenima u preporukama.

4. Organizatori vježbi u području kibernetičke sigurnosti iz članka 43. stavaka 1. i 2. te iz članka 44. stavka 1. redovito prate provedbu preporuka u skladu sa stavkom 2. točkom (c) ovog članka sa subjektima koji sudjeluju u vježbama.

POGLAVLJE VII.

ZAŠTITA INFORMACIJA

Članak 46.

Načela zaštite razmijenjenih informacija

1. Subjekti iz članka 2. stavka 1. osiguravaju da su informacije koje se pružaju, primaju, razmjenjuju ili prenose u skladu s ovom Uredbom dostupne samo na temelju nužnosti pristupa informacijama i u skladu s relevantnim pravilima Unije i nacionalnim pravilima o sigurnosti informacija.

2. Subjekti iz članka 2. stavka 1. osiguravaju da se informacije koje se pružaju, primaju, razmjenjuju ili prenose u skladu s ovom Uredbom obrađuju i prate tijekom cijelog svojeg životnog ciklusa te da se mogu objaviti na kraju svojeg životnog ciklusa tek nakon što su anonimizirane.

3. Subjekti iz članka 2. stavka 1. osiguravaju da su uspostavljene sve potrebne zaštitne mjere organizacijske i tehničke prirode za zaštitu povjerljivosti, cjelovitosti, dostupnosti i neosporivosti informacija dostavljenih, primljenih, razmijenjenih ili prenesenih u skladu s ovom Uredbom, neovisno o korištenim sredstvima. Zaštitne mjere ispunjavaju sljedeće uvjete:

(a) razmjerne su;

(b) njima se uzimaju u obzir kibernetičkosigurnosni rizici povezani s poznatim prošlim i novim prijetnjama kojima takve informacije mogu podlijegati u kontekstu ove Uredbe;

(c) u mjeri u kojoj je to moguće, temelje se na nacionalnim, europskim ili međunarodnim normama i najboljim praksama;

(d) dokumentiraju se.

4. Subjekti iz članka 2. stavka 1. osiguravaju da svaka osoba kojoj je odobren pristup informacijama koje se pružaju, primaju, razmjenjuju ili prenose u skladu s ovom Uredbom bude obaviještena o sigurnosnim pravilima koja se primjenjuju na razini subjekta te o mjerama i postupcima relevantnima za zaštitu informacija. Ti subjekti osiguravaju da predmetni pojedinac preuzme odgovornost za zaštitu informacija kako je naloženo tijekom informativnog sastanka.

5. Subjekti iz članka 2. stavka 1. osiguravaju da pristup informacijama koje se pružaju, primaju, razmjenjuju ili prenose u skladu s ovom Uredbom imaju samo pojedinci:

(a) koji su ovlašteni pristupiti tim informacijama na temelju svojih funkcija pri čemu je taj pristup ograničen na izvršavanje dodijeljenih zadaća;

(b) za koje je subjekt mogao procijeniti etička načela i načela integriteta te za koje nema dokaza o negativnom ishodu provjere podobnosti kako bi se ocijenila pouzdanost pojedinca u skladu s najboljim praksama i standardnim sigurnosnim zahtjevima subjekta te, prema potrebi, nacionalnim zakonima i propisima.

6. Subjekti iz članka 2. stavka 1. imaju pisanu suglasnost fizičke ili pravne osobe koja je izvorno stvorila ili dostavila informacije prije nego što te informacije dostave trećoj strani koja nije obuhvaćena područjem primjene ove Uredbe.

7. Subjekt iz članka 2. stavka 1. može smatrati da se te informacije razmjenjuju bez usklađivanja sa stavcima 1. i 4. ovog članka kako bi se spriječila istodobna elektroenergetska kriza čiji je temeljni uzrok povezan s kibernetičkom sigurnošću ili bilo koja prekogranična kriza u Uniji u drugom sektoru. U tom slučaju taj subjekt:

(a) savjetuje se s nadležnim tijelom i dobiva odobrenje nadležnog tijela za razmjenu takvih informacija;

(b) anonimizira takve informacije bez gubitka elemenata potrebnih za obavješćivanje javnosti o neposrednom i ozbiljnom riziku za prekogranične protoke električne energije i mogućim mjerama ublažavanja;

(c) štiti identitet autora i subjekata koji su obradili takve informacije u skladu s ovom Uredbom.

8. Odstupajući od stavka 6. ovog članka, nadležna tijela mogu dostaviti informacije dostavljene, primljene, razmijenjene ili prenesene na temelju ove Uredbe trećoj strani koja nije navedena u članku 2. stavku 1. bez prethodne pisane suglasnosti autora informacija, ali o tome što prije obavješćuju treću stranu. Prije otkrivanja bilo kakvih informacija dostavljenih, primljenih, razmijenjenih ili prenesenih na temelju ove Uredbe trećoj strani koja nije navedena u članku 2. stavku 1., predmetno nadležno tijelo razumno osigurava da je predmetna treća strana upoznata sa sigurnosnim pravilima koja su na snazi i dobiva razumno jamstvo da predmetna treća strana može zaštititi primljene informacije u skladu sa stavcima od 1. do 5. ovog članka. Nadležno tijelo anonimizira takve informacije bez gubitka elemenata potrebnih za obavješćivanje javnosti o neposrednom i ozbiljnom riziku za prekogranične protoke električne energije i mogućim mjerama ublažavanja te za zaštitu identiteta autora informacija. U tom slučaju treća strana koja nije navedena u članku 2. stavku 1. štiti primljene informacije u skladu s odredbama koje su već na snazi na razini subjekta ili, ako to nije moguće, odredbama i uputama relevantnog nadležnog tijela.

9. Ovaj se članak ne primjenjuje na subjekte koji nisu navedeni u članku 2. stavku 1., a kojima se pružaju informacije u skladu sa stavkom 6. ovog članka. U tom slučaju primjenjuje se stavak 7. ovog članka ili nadležno tijelo tom subjektu može osigurati pisane odredbe koje se primjenjuju onda kad su informacije primljene u skladu s ovom Uredbom.

Članak 47.

Povjerljivost informacija

1. Sve informacije dostavljene, primljene, razmijenjene ili prenesene u skladu s ovom Uredbom podliježu uvjetima čuvanja poslovne tajne utvrđenima u stavcima od 2. do 5. ovog članka ove Uredbe i zahtjevima utvrđenima u članku 65. Uredbe (EU) 2019/943. Sve informacije koje se dostavljaju, primaju, razmjenjuju ili prenose među subjektima iz članka 2. ove Uredbe za potrebe provedbe ove Uredbe štite se uzimajući u obzir razinu povjerljivosti informacija koju primjenjuje autor podataka.

2. Obveza čuvanja poslovne tajne primjenjuje se na subjekte iz članka 2.

3. Nadležna tijela odgovorna za kibernetičku sigurnost, nacionalna regulatorna tijela, nadležna tijela za pripravnost za rizike i CSIRT-ovi razmjenjuju sve informacije potrebne za obavljanje svojih zadaća.

4. Sve informacije primljene, razmijenjene ili prenesene među subjektima iz članka 2. stavka 1. za potrebe provedbe članka 23. anonimiziraju se i agregiraju.

5. Informacije koje bilo koji subjekt ili tijelo koje podliježe ovoj Uredbi primi tijekom obavljanja svojih dužnosti ne smiju se otkrivati nijednom drugom subjektu ili tijelu, ne dovodeći u pitanje slučajeve obuhvaćene nacionalnim pravom, drugim odredbama ove Uredbe ili drugim relevantnim zakonodavstvom Unije.

6. Ne dovodeći u pitanje nacionalno zakonodavstvo ili zakonodavstvo Unije, tijelo, subjekt ili fizička osoba koja prima informacije u skladu s ovom Uredbom ne smije ih upotrebljavati ni u koju drugu svrhu osim obavljanja svojih dužnosti na temelju ove Uredbe.

7. ACER, nakon savjetovanja s ENISA-om, svim nadležnim tijelima, ENTSO-om za električnu energiju i tijelom EU-a za ODS-ove, do 13. lipnja 2025. izdaje smjernice za sve subjekte iz članka 2. stavka 1. za razmjenu informacija, a posebno predviđenih komunikacijskih tokova, te metode anonimizacije i agregiranja informacija za potrebe provedbe ovog članka.

8. Informacije koje su povjerljive u skladu s pravilima Unije i nacionalnim pravilima razmjenjuju se s Komisijom i drugim relevantnim tijelima samo ako je ta razmjena potrebna za primjenu ove Uredbe. Razmijenjene informacije ograničene su na ono što je nužno i razmjerno svrsi te razmjene. Pri razmjeni informacija čuva se njihova povjerljivost te štite sigurnost i komercijalni interesi subjekata s kritičnim ili velikim utjecajem.

POGLAVLJE VIII.

ZAVRŠNE ODREDBE

Članak 48.

Privremene odredbe

1. Do odobrenja odredaba i uvjeta ili metodologija iz članka 6. stavka 2. ili planova iz članka 6. stavka 3., ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove izrađuje neobvezujuće smjernice o sljedećim pitanjima:

(a) privremeni indeks utjecaja na kibernetičku sigurnost elektroenergetskog sektora („ECII") u skladu sa stavkom 2. ovog članka;

(b) privremeni popis procesa s velikim i kritičnim utjecajem na razini Unije u skladu sa stavkom 4. ovog članka; i

(c) privremeni popis europskih i međunarodnih normi i kontrola koje se zahtijevaju nacionalnim zakonodavstvom i koje su relevantne za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije u skladu sa stavkom 6. ovog članka.

2. Do 13. listopada 2024. ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove izrađuje preporuku za privremeni ECII. ENTSO za električnu energiju u suradnji s tijelom EU-a za ODS-ove obavješćuje nadležna tijela o preporučenom privremenom indeksu ECII.

3. Četiri mjeseca od primitka preporučenog privremenog indeksa ECII, ili najkasnije do 13. veljače 2025., nadležna tijela utvrđuju subjekte koji su kandidati za subjekte s velikim i kritičnim utjecajem u svojoj državi članici na temelju preporučenog indeksa ECII te izrađuju privremeni popis subjekata s velikim i kritičnim utjecajem. Subjekti s velikim i kritičnim utjecajem navedeni na privremenom popisu mogu dobrovoljno ispuniti svoje obveze utvrđene u ovoj Uredbi na temelju načela predostrožnosti. Do 13. ožujka 2025., nadležna tijela obavješćuju subjekte s privremenog popisa da su utvrđeni kao subjekti s velikim ili kritičnim utjecajem.

4. Do 13. prosinca 2024., ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, izrađuje privremeni popis postupaka s velikim i kritičnim utjecajem na razini Unije. Subjekti obaviješteni u skladu sa stavkom 3. koji dobrovoljno odluče ispuniti svoje obveze kako je utvrđeno u ovoj Uredbi na temelju načela predostrožnosti upotrebljavaju privremeni popis procesa s velikim i kritičnim utjecajem kako bi utvrdili privremena područja od velikog i kritičnog utjecaja te koja se imovina treba uključiti u prvu procjenu kibernetičkosigurnosnih rizika na razini subjekta.

5. Do 13. rujna 2024., svako nadležno tijelo u skladu s člankom 4. stavkom 1. dostavlja ENTSO-u za električnu energiju i tijelu EU-a za ODS-ove popis svojeg nacionalnog zakonodavstva koji se odnosi na kibernetičkosigurnosne aspekte prekograničnih protoka električne energije.

6. Do 13. lipnja 2025. ENTSO za električnu energiju, u suradnji s tijelom EU-a za ODS-ove, priprema privremeni popis europskih i međunarodnih normi i kontrola koje se zahtijevaju nacionalnim zakonodavstvom i koje su relevantne za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije, uzimajući u obzir informacije koje su dostavila nadležna tijela.

7. Privremeni popis europskih i međunarodnih normi i kontrola uključuje:

(a) europske i međunarodne norme i nacionalno zakonodavstvo kojim se pružaju smjernice o metodologijama za upravljanje kibernetičkosigurnosnim rizicima na razini subjekta; i

(b) kibernetičkosigurnosne kontrole jednakovrijedne kontrolama za koje se očekuje da će biti dio minimalnih i naprednih kibernetičkosigurnosnih kontrola.

8. Pri finalizaciji privremenog popisa normi ENTSO za električnu energiju i tijelo EU-a za ODS-ove uzimaju u obzir stajališta ENISA-e i ACER-a. ENTSO za električnu energiju i tijelo EU-a za ODS-ove objavljuju prijelazni popis europskih i međunarodnih normi i kontrola na svojim internetskim stranicama.

9. ENTSO za električnu energiju i tijelo EU-a za ODS-ove savjetuju se s ENISA-om i ACER-om o prijedlozima neobvezujućih smjernica izrađenih u skladu sa stavkom 1.

10. Dok se minimalne i napredne kibernetičkosigurnosne kontrole ne budu razvijale u skladu s člankom 29. i donosile na temelju članka 8., svi subjekti iz članka 2. stavka 1. nastoje postupno primjenjivati neobvezujuće smjernice izrađene u skladu sa stavkom 1.

Članak 49.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 11. ožujka 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN