Uradni list
Evropske unije

SL
Serija L

2024/1366

24.5.2024

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1366

z dne 11. marca 2024

o dopolnitvi Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta z oblikovanjem omrežnega kodeksa s sektorskimi pravili za vidike kibernetske varnosti čezmejnih pretokov električne energije

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije ([1]) ter zlasti člena 59(2), točka (e), Uredbe,

ob upoštevanju naslednjega:

(1) Obvladovanje tveganja za kibernetsko varnost je ključno za ohranjanje zanesljivosti oskrbe z električno energijo in zagotavljanje visoke ravni kibernetske varnosti v sektorju električne energije.

(2) Digitalizacija in kibernetska varnost sta odločilni za zagotavljanje bistvenih storitev in zato strateško pomembni za kritično energetsko infrastrukturo.

(3) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta ([2]) določa ukrepe za visoko skupno raven kibernetske varnosti v Uniji. Direktivo (EU) 2022/2555 dopolnjuje Uredba (EU) 2019/941 Evropskega parlamenta in Sveta ([3]), ki zagotavlja, da se kibernetski incidenti v sektorju električne energije ustrezno opredelijo kot tveganje in da so ukrepi, sprejeti za njihovo obravnavo, ustrezno obravnavani v načrtih pripravljenosti na tveganja. Uredba (EU) 2019/943 dopolnjuje Direktivo (EU) 2022/2555 in Uredbo (EU) 2019/941 z določitvijo posebnih pravil za sektor električne energije na ravni Unije. Poleg tega določbe Direktive (EU) 2022/2555 v zvezi s sektorjem električne energije dopolnjuje tudi ta delegirana uredba v vseh primerih, ki se nanašajo na čezmejne pretoke električne energije.

(4) Zaradi medsebojne povezanosti digitaliziranih elektroenergetskih sistemov preprečevanja in obvladovanja krize pri oskrbi z električno energijo, povezane s kibernetskimi napadi, ni mogoče obravnavati kot izključno nacionalno nalogo. V okviru regionalnega sodelovanja in sodelovanja na ravni Unije bi bilo treba v celoti razviti učinkovitejše in cenejše ukrepe. Zato so potrebni skupni okvir pravil in bolje usklajeni postopki, da bi zagotovili, da bodo države članice in drugi akterji lahko učinkovito čezmejno sodelovali ter da se bodo povečali preglednost, zaupanje in solidarnost med državami članicami ter pristojnimi organi, odgovornimi za električno energijo in kibernetsko varnost.

(5) Za obvladovanje tveganja za kibernetsko varnost znotraj področja uporabe te uredbe je potreben strukturiran postopek, ki med drugim vključuje opredelitev tveganj za čezmejne pretoke električne energije, ki izhajajo iz kibernetskih napadov, z njimi povezane operativne postopke in območja, ustrezne kontrole kibernetske varnosti in mehanizme za preverjanje. Čeprav časovni okvir za celotni postopek obsega več let, bi vsak korak znotraj njega moral prispevati k višji skupni ravni kibernetske varnosti v sektorju in zmanjšanju tveganja za kibernetsko varnost. Vsi udeleženci v postopku bi si morali čim bolj prizadevati za to, da bi metodologije oblikovali in se o njih dogovorili čim prej in brez nepotrebnega odlašanja ter vsekakor najpozneje v rokih, določenih v tej uredbi.

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

([2]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

([3]) Uredba (EU) 2019/941 Evropskega parlamenta in Sveta z dne 5. junija 2019 o pripravljenosti na tveganja v sektorju električne energije in razveljavitvi Direktive 2005/89/ES (UL L 158, 14.6.2019, str. 1).

(6) Ocene tveganja za kibernetsko varnost na ravni Unije in držav članic, regionalni ravni ter ravni subjektov v tej uredbi se lahko omejijo na ocene, ki nastanejo v primeru kibernetskih napadov, kot je opredeljeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta ([4]), torej bi na primer izključevale fizične napade, naravne nesreče in prekinitve zaradi izgube objektov ali človeških virov. Tveganja na ravni Unije in regionalna tveganja, povezana s fizičnimi napadi ali naravnimi nesrečami na področju električne energije so že zajeta z drugimi obstoječimi zakonodajnimi akti Unije, vključno s členom 5 Uredbe (EU) 2019/941 ali Uredbo Komisije (EU) 2017/1485 ([5]) o določitvi smernic za obratovanje sistema za prenos električne energije. Podobno je cilj Direktive (EU) 2022/2557 Evropskega parlamenta in Sveta ([6]) o odpornosti kritičnih subjektov zmanjšati ranljivosti in okrepiti fizično odpornost kritičnih subjektov, zajema pa vsa relevantna naravna tveganja in tveganja, ki jih povzroči človek, ki lahko vplivajo na izvajanje bistvenih storitev, vključno z nesrečami, naravnimi nesrečami, izrednimi razmerami v javnem zdravju, na primer pandemije, in hibridnimi grožnjami ali drugimi antagonističnimi grožnjami, vključno s terorističnimi kaznivimi dejanji, infiltracijo kriminala in sabotažo.

(7) Pojem „subjekti z velikim ali kritičnim učinkom“ v tej uredbi je temeljnega pomena za opredelitev obsega subjektov, za katere veljajo obveznosti iz te uredbe. Cilj pristopa na podlagi tveganja, ki je opisan v različnih določbah, je opredeliti postopke, ki vplivajo na čezmejne pretoke električne energije, sredstva, ki te postopke podpirajo, in subjekte, ki jih izvajajo. Glede na stopnjo učinka možnih kibernetskih napadov na njihovo izvajanje čezmejnih pretokov električne energije se lahko štejejo za subjekte z „velikim učinkom“ ali „kritičnim učinkom“. Člen 3 Direktive (EU) 2022/2555 določa pojma bistvenih in pomembnih subjektov ter merila za opredelitev subjektov na podlagi teh kategorij. Čeprav bodo številni med njimi v skladu s členom 3 Direktive (EU) 2022/2555 veljali oziroma bodo opredeljeni kot „bistveni“ subjekti, sočasno pa tudi kot subjekti z velikim ali kritičnim učinkom v skladu s členom 24 te uredbe, se merila iz te uredbe nanašajo samo na njihovo vlogo in učinek v okviru postopkov v zvezi z električno energijo, ki vplivajo na čezmejne pretoke, brez upoštevanja meril iz člena 3 Direktive (EU) 2022/2555.

(8) Subjekti, ki spadajo na področje uporabe te uredbe in se štejejo za subjekte z velikim ali kritičnim učinkom v skladu s členom 24 te uredbe, in za katere veljajo obveznosti, ki so v njej določene, so predvsem tisti, ki neposredno vplivajo na čezmejne pretoke električne energije v EU.

(9) Ta uredba uporablja obstoječe mehanizme in instrumente, ki so že določeni v drugih zakonodajnih aktih, da bi se zagotovila učinkovitost in preprečilo podvajanje pri doseganju ciljev.

(10) Države članice, ustrezni organi in operaterji sistemov bi morali pri uporabi te uredbe upoštevati dogovorjene evropske standarde in tehnične specifikacije evropskih organizacij za standardizacijo ter ravnati v skladu z zakonodajo Unije o dajanju na trg ali v uporabo izdelkov, ki jih zajema navedena zakonodaja Unije.

([4]) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).

([5]) Uredba Komisije (EU) 2017/1485 z dne 2. avgusta 2017 o določitvi smernic za obratovanje sistema za prenos električne energije (UL L 220, 25.8.2017, str. 1).

([6]) Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (UL L 333, 27.12.2022, str. 164).

(11) Da bi se zmanjšala tveganja za kibernetsko varnost, je treba določiti podrobna pravila, ki urejajo delovanje in sodelovanje ustreznih deležnikov, katerih dejavnosti so povezane z vidiki kibernetske varnosti čezmejnih pretokov električne energije, cilj tega pa je zagotoviti varnost sistema. Navedena organizacijska in tehnična pravila bi morala zagotoviti, da se večina incidentov v sektorju električne energije, katerih temeljni vzroki so povezani s kibernetsko varnostjo, učinkovito obravnava na operativni ravni. Treba je določiti, kaj bi ustrezni deležniki morali storiti, da se take krize preprečijo, in kakšne ukrepe lahko sprejmejo, če zgolj sistemska obratovalna pravila ne bi več zadoščala. Zato je treba določiti skupen okvir pravil za preprečevanje in obvladovanje sočasnih kriz pri oskrbi z električno energijo, katerih temeljni vzroki so povezani s kibernetsko varnostjo, ter za pripravo nanje. To vnaša večjo preglednost v pripravljalno fazo in med sočasno krizo pri oskrbi z električno energijo ter zagotavlja usklajeno in učinkovito sprejemanje ukrepov skupaj s pristojnimi organi za kibernetsko varnost v državah članicah. Od držav članic in ustreznih deležnikov bi bilo treba zahtevati, da sodelujejo v duhu solidarnosti na regionalni ravni in, kjer je ustrezno, dvostransko. Namen tega sodelovanja in pravil je doseči boljšo pripravljenost na tveganja za kibernetsko varnost z nižjimi stroški, kar je tudi v skladu s cilji Direktive (EU) 2022/2555. Potrebno se zdi tudi okrepiti notranji trg električne energije s krepitvijo zaupanja med državami članicami, zlasti pa zmanjšati tveganje nepotrebnega omejevanja čezmejnih pretokov električne energije, s čimer bi se zmanjšali negativni učinki prelivanja na sosednje države članice.

(12) Zanesljivost oskrbe z električno energijo zajema učinkovito sodelovanje med državami članicami, institucijami, organi, uradi in agencijami Unije ter ustreznimi deležniki. Operaterji distribucijskih sistemov in operaterji prenosnih sistemov imajo ključno vlogo pri zagotavljanju varnega, zanesljivega in učinkovitega elektroenergetskega sistema v skladu s členoma 31 in 40 Direktive (EU) 2019/944 Evropskega parlamenta in Sveta ([7]). Različni regulativni organi in drugi zadevni pristojni nacionalni organi imajo pomembno vlogo pri zagotavljanju in spremljanju kibernetske varnosti na področju oskrbe z električno energijo kot delu nalog, ki so jim dodeljene z direktivama (EU) 2019/944 in (EU) 2022/2555. Države članice bi morale imenovati obstoječ ali nov subjekt kot svoj pristojni nacionalni organ za izvajanje te uredbe, da bi zagotovile pregledno in vključujočo udeležbo vseh udeleženih akterjev, učinkovito pripravo in ustrezno izvajanje ter sodelovanje med različnimi ustreznimi deležniki in pristojnimi organi za električno energijo in kibernetsko varnost ter omogočile preprečevanje in naknadno vrednotenje kriz pri oskrbi z električno energijo, katerih temeljni vzroki so povezani s kibernetsko varnostjo, ter izmenjavo informacij v zvezi s tem.

(13) Kadar subjekt z velikim ali kritičnim učinkom zagotavlja storitve v več kot eni državi članici ali ima sedež ali drugo ustanovo ali predstavnika v eni državi članici, omrežne in informacijske sisteme pa v eni ali več drugih državah članicah, bi navedene države članice morale spodbujati svoje ustrezne pristojne organe, da si po potrebi čim bolj prizadevajo za medsebojno sodelovanje in si pomagajo.

(14) Države članice bi morale pristojnim organom v zvezi s subjekti z velikim ali kritičnim učinkom zagotoviti potrebna pooblastila za spodbujanje skladnosti s to uredbo. Ta pooblastila bi morala pristojnim organom omogočiti opravljanje inšpekcijskih pregledov na kraju samem in nadzora na daljavo. To lahko vključuje naključne preglede, opravljanje rednih revizij, ciljno usmerjene revizije varnosti na podlagi ocen tveganja ali razpoložljivih informacij o tveganju ter revizije varnosti, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja in ki vključujejo tudi zahtevanje potrebnih informacij za oceno ukrepov za kibernetsko varnost, ki jih je sprejel subjekt. Te informacije bi morale vključevati dokumentirane politike na področju kibernetske varnosti, podatke, dokumente ali kakršne koli informacije o dostopu, potrebne za opravljanje njihovih nadzornih nalog, ter dokaze o izvajanju politik na področju kibernetske varnosti, kot so rezultati revizij varnosti, ki jih izvede usposobljen revizor, in ustrezni dokazi v zvezi z njimi.

([7]) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125).

(15) V izogib vrzelim ali podvajanju obveznosti glede obvladovanja tveganj za kibernetsko varnost, ki veljajo za subjekte z velikim ali kritičnim učinkom, bi morali nacionalni organi iz Direktive (EU) 2022/2555 ter pristojni organi iz te uredbe sodelovati pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost in nadzoru spoštovanja teh ukrepov na nacionalni ravni. Pristojni organi iz Direktive (EU) 2022/2555 bi lahko šteli, da skladnost subjekta z zahtevami glede obvladovanja tveganja za kibernetsko varnost, določenimi v tej uredbi, pomeni zagotavljanje skladnosti z ustreznimi zahtevami, določenimi v navedeni direktivi, ali obratno.

(16) Za skupen pristop k preprečevanju in obvladovanju sočasnih kriz pri oskrbi z električno energijo je pomembno, da države članice enako razumejo koncept sočasne krize pri oskrbi z električno energijo in kdaj je kibernetski napad pomemben dejavnik v taki krizi. Predvsem bi bilo treba olajšati usklajevanje med državami članicami in ustreznimi subjekti, da bi se obravnavalo obstoječe ali preteče stanje, ko obstaja tveganje večjega pomanjkanja ali nezmožnosti dobave električne energije odjemalcem zaradi kibernetskega napada.

(17) V uvodni izjavi 1 Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta ([8]) je priznana ključna vloga omrežnih in informacijskih sistemov ter elektronskih komunikacijskih omrežij in storitev pri omogočanju delovanja gospodarstva v ključnih sektorjih, kot je energetika, medtem ko je v uvodni izjavi 44 pojasnjeno, da bi morala Agencija Evropske unije za kibernetsko varnost (v nadaljnjem besedilu: ENISA) sodelovati z Agencijo Evropske unije za sodelovanje energetskih regulatorjev (v nadaljnjem besedilu: ACER).

(18) Na podlagi Uredbe (EU) 2019/943 se posebna pooblastila v zvezi s kibernetsko varnostjo dodelijo operaterjem prenosnih sistemov in operaterjem distribucijskih sistemov. Njihovi evropski združenji, tj. Evropska mreža operaterjev prenosnih sistemov za električno energijo (v nadaljnjem besedilu: ENTSO za električno energijo) in Evropsko telo za operaterje distribucijskih sistemov (v nadaljnjem besedilu: telo EU ODS), v skladu s členom 30 oziroma členom 55 navedene uredbe spodbujata kibernetsko varnost v sodelovanju z ustreznimi organi in reguliranimi subjekti.

(19) Za skupen pristop k preprečevanju in obvladovanju sočasnih kriz pri oskrbi z električno energijo, katerih temeljni vzroki so povezani s kibernetsko varnostjo, je pomembno tudi, da vsi ustrezni deležniki uporabljajo usklajene metode in opredelitve za določanje tveganj, povezanih s kibernetsko varnostjo oskrbe z električno energijo. Pomembno je tudi, da lahko učinkovito primerjajo svojo uspešnost in uspešnost svojih sosed na tem področju. Zato je treba določiti postopke ter vloge in pooblastila za oblikovanje in posodobitev metodologij za obvladovanje tveganj, lestvice razvrščanja incidentov ter ukrepov za kibernetsko varnost, prilagojenih tveganjem za kibernetsko varnost, ki vplivajo na čezmejne pretoke električne energije.

(20) Države članice so odgovorne, da prek pristojnega organa, imenovanega na podlagi te uredbe, določijo subjekte, ki izpolnjujejo merila, na podlagi katerih se lahko štejejo za subjekte z velikim učinkom in subjekte s kritičnim učinkom. Za odpravo razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti sklop meril, ki bi določala, kateri subjekti spadajo na področje uporabe te uredbe. Sklop meril bi bilo treba opredeliti in redno posodabljati v okviru oblikovanja in sprejemanja pogojev in metodologij, določenih v tej uredbi.

(21) Določbe te uredbe ne bi smele posegati v pravo Unije, ki vsebuje posebne predpise o certificiranju proizvodov informacijske in komunikacijske tehnologije (IKT), storitev IKT in postopkov IKT, zlasti pa ne v Uredbo (EU) 2019/881, kar zadeva določitev okvira za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost. V okviru te uredbe bi proizvodi IKT morali vključevati tudi tehnične naprave in programsko opremo, ki omogočajo neposredno interakcijo z elektrotehničnim omrežjem, zlasti industrijske nadzorne sisteme, ki se lahko uporabljajo za prenos, distribucijo in proizvodnjo energije ter zbiranje in prenos s tem povezanih informacij. Določbe bi morale zagotoviti, da bodo proizvodi IKT, storitve IKT in postopki IKT, ki so predmet javnih naročil, izpolnjevali ustrezne varnostne cilje iz člena 51 Uredbe (EU) 2019/881.

([8]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

(22) Nedavni kibernetski napadi so pokazali, da so subjekti vse pogosteje tarča napadov na dobavne verige. Taki napadi na dobavne verige ne vplivajo zgolj na posamezne subjekte, ampak imajo lahko tudi kaskadne učinke za večje napade na subjekte, s katerimi so povezani v omrežju električne energije. Zato so bili dodani določbe in priporočila, ki pomagajo zmanjšati tveganja za kibernetsko varnost, povezana s postopki v zvezi z dobavno verigo, zlasti javnim naročanjem, ki vplivajo na čezmejne pretoke električne energije.

(23) Ker lahko izkoriščanje ranljivosti v omrežnih in informacijskih sistemih povzroči hude motnje v oskrbi z energijo in škodo za gospodarstvo in potrošnike, bi bilo treba take ranljivosti hitro odkriti in odpraviti, da bi se zmanjšala tveganja. Da bi se olajšalo učinkovito izvajanje te uredbe, bi morali ustrezni subjekti in pristojni organi sodelovati pri izvajanju in preskušanju dejavnosti, ki se štejejo kot ustrezne za ta namen, vključno z izmenjavo informacij o kibernetskih grožnja, kibernetskih napadih, ranljivostih, orodjih in metodah, taktikah, tehnikah in postopkih, pripravljenostjo za obvladovanje kibernetskih kriz in drugimi dejavnostmi. Ker se tehnologija neprekinjeno razvija, digitalizacija sektorja električne energije pa hitro napreduje, izvajanje sprejetih določb ne bi smelo povzročati škode inovacijam niti ovirati dostopa do trga električne energije in nadaljnje uporabe inovativnih rešitev, ki prispevajo k učinkovitosti in trajnostnosti elektroenergetskega sistema.

(24) Informacije, ki se zbirajo zaradi spremljanja in izvajanja te uredbe, bi morale biti razumno omejene po načelu potrebe po seznanitvi. Za deležnike bi bilo treba določiti dosegljive in učinkovite roke za predložitev takih informacij. Izogibati bi se bilo treba dvojnim priglasitvam.

(25) Zagotavljanje kibernetske varnosti se ne ustavi na mejah Unije. Za varen sistem je potrebna vključenost sosednjih tretjih držav. Unija in njene države članice bi si morale prizadevati, da sosednjim tretjim državam, katerih elektroenergetska infrastruktura je povezana z evropskim omrežjem, zagotovijo podporo pri uporabi podobnih pravil na področju kibernetske varnosti, določenih v tej uredbi.

(26) Da bi se dovolj zgodaj izboljšalo usklajevanje varnosti in preskusili prihodnji zavezujoči pogoji in metodologije, bi ENTSO za električno energijo, telo EU ODS in pristojni organi morali začeti pripravljati nezavezujoče smernice takoj po začetku veljavnosti te uredbe. Te smernice bodo izhodišče za oblikovanje prihodnjih pogojev in metodologij. Vzporedno bi morali pristojni organi subjekte opredeliti kot kandidate za subjekte z velikim ali kritičnim učinkom, da bi prostovoljno začeli izpolnjevati obveznosti.

(27) Ta uredba je bila pripravljena v tesnem sodelovanju z ACER, ENISA, ENTSO za električno energijo, telesom EU ODS in drugimi deležniki, da bi se na pregleden in participativen način sprejela učinkovita, uravnotežena in sorazmerna pravila.

(28) Ta uredba dopolnjuje in krepi ukrepe za obvladovanje tveganj, določene v okviru EU za krizno upravljanje na področju kibernetske varnosti, kot je določeno v Priporočilu Komisije (EU) 2017/1584 ([9]). Kibernetski napad bi lahko tudi povzročil krizo pri oskrbi z električno energijo, kot je opredeljena v členu 2, točka 9, Uredbe (EU) 2019/941, oziroma bi lahko k tej krizi prispeval ali z njo sovpadal, kar bi vplivalo na čezmejne pretoke električne energije. Navedena kriza bi lahko povzročila sočasno krizo pri oskrbi z električno energijo, kot je opredeljena v členu 2(10) Uredbe (EU) 2019/941. Tak incident bi lahko tudi vplival na druge sektorje, ki so odvisni od zanesljivosti oskrbe z električno energijo. Če bi tak incident prerasel v kibernetski incident velikih razsežnosti v smislu člena 16 Direktive (EU) 2022/2555, bi se morale uporabljati določbe iz navedenega člena o ustanovitvi Evropske organizacijske mreže za povezovanje v kibernetski krizi (mreža EU-CyCLONe). Za obvladovanje krize na ravni Unije bi se morale ustrezne strani zanašati na enotno ureditev EU za politično odzivanje na krize (v nadaljnjem besedilu: ureditev IPCR) iz Izvedbenega sklepa Sveta (EU) 2018/1993 ([10]).

(29) Ta uredba ne posega v zmožnost držav članic, da sprejmejo potrebne ukrepe, s katerimi zavarujejo bistvene interese svoje varnosti, zaščitijo javni red in javno varnost ter omogočijo preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. V skladu s členom 346 PDEU nobena država članica ni dolžna dajati informacij, za katere meni, da bi bilo njihovo razkritje v nasprotju z bistvenimi interesi njene varnosti.

([9]) Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

([10]) Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28).

(30) Čeprav se ta uredba načeloma uporablja za subjekte, ki opravljajo dejavnosti na področju proizvodnje električne energije v jedrskih elektrarnah, so nekatere od teh dejavnosti lahko povezane z nacionalno varnostjo.

(31) Pravo Unije o varstvu podatkov in pravo Unije o zasebnosti bi bilo treba uporabljati za vsakršno obdelavo osebnih podatkov na podlagi te uredbe. Ta uredba zlasti ne posega v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ([11]), Direktivo 2002/58/ES Evropskega parlamenta in Sveta ([12]) ter Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta ([13]). Ta uredba zato med drugim ne bi smela vplivati na naloge in pooblastila organov, pristojnih za spremljanje skladnosti z veljavnim pravom Unije o varstvu podatkov in pravom Unije o zasebnosti.

(32) Mednarodno sodelovanje na področju kibernetske varnosti je pomembno, zato bi morali pristojnim organom, ki so odgovorni za izvajanje nalog, dodeljenih na podlagi te uredbe, in ki so jih imenovale države članice, omogočiti sodelovanje v mrežah mednarodnega sodelovanja. Zato bi morali imeti pristojni organi za namene opravljanja svojih nalog možnost, da izmenjujejo informacije, vključno z osebnimi podatki, s pristojnimi organi tretjih držav, če so izpolnjeni pogoji iz prava Unije o varstvu podatkov za prenose osebnih podatkov tretjim državam, med drugim pogoji iz člena 49 Uredbe (EU) 2016/679.

(33) Obdelava osebnih podatkov v obsegu, ki je potreben in sorazmeren za zagotovitev varnosti sredstev subjektov z velikim ali kritičnim učinkom, bi lahko štela za zakonito na podlagi tega, da je taka obdelava skladna s pravno obveznostjo, ki velja za upravljavca, v skladu z zahtevami iz člena 6(1), točka (c), in člena 6(3) Uredbe (EU) 2016/679. Obdelava osebnih podatkov je lahko potrebna tudi za zakonite interese subjektov z velikim ali kritičnim učinkom ter ponudnikov varnostnih tehnologij in storitev, ki ravnajo v imenu teh subjektov, v skladu s členom 6(1), točka (f), Uredbe (EU) 2016/679, tudi kadar je taka obdelava potrebna za dogovore o izmenjavi informacij o kibernetski varnosti ali prostovoljno obveščanje o ustreznih informacijah v skladu s to direktivo. Ukrepi, povezani s preprečevanjem, odkrivanjem, prepoznavanjem, zajezitvijo in analizo kibernetskih napadov ter odzivanjem nanje, ukrepi za ozaveščanje v zvezi s posebnimi kibernetskimi grožnjami, izmenjavo informacij v okviru odpravljanja in usklajenega razkrivanja ranljivosti ter prostovoljno izmenjavo informacij o takih kibernetskih napadih, pa tudi o kibernetskih grožnjah in ranljivostih, kazalnikih ogroženosti, taktikah, tehnikah in postopkih, opozorilih glede kibernetske varnosti in orodjih za konfiguracijo, bi lahko zahtevali obdelavo nekaterih kategorij osebnih podatkov, kot so naslovi IP, enotni naslovi vira (URL), domenska imena, elektronski naslovi in, kadar ti razkrivajo osebne podatke, časovni žigi. Obdelava osebnih podatkov s strani pristojnih organov, enotnih kontaktnih točk in skupin CSIRT lahko pomeni pravno obveznost ali se lahko šteje za potrebno za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu podatkov v skladu s členom 6(1), točka (c) ali (e), in členom 6(3) Uredbe (EU) 2016/679, ali za zasledovanje pravnega interesa subjektov z velikim ali kritičnim učinkom iz člena 6(1), točka (f), navedene uredbe. Poleg tega se lahko v nacionalnem pravu določijo pravila, ki bi pristojnim organom, enotnim kontaktnim točkam in skupinam CSIRT omogočala, da v obsegu, ki je potreben in sorazmeren za zagotavljanje varnosti omrežnih in informacijskih sistemov subjektov z velikim ali kritičnim učinkom, obdelujejo posebne vrste osebnih podatkov v skladu s členom 9 Uredbe (EU) 2016/679, zlasti z določitvijo ustreznih in posebnih ukrepov za varstvo temeljnih pravic in interesov fizičnih oseb, vključno s tehničnimi omejitvami ponovne uporabe takih podatkov in uporabe najsodobnejših ukrepov za varnost in ohranjanje zasebnosti, kot so psevdonimizacija ali šifriranje, kadar lahko anonimizacija znatno vpliva na zastavljeni namen.

([11]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

([12]) Direktiva 2002/58/ES evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

([13]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

(34) V številnih primerih je zaradi kibernetskih napadov ogrožena varnost osebnih podatkov. V tem okviru bi morali pristojni organi sodelovati in si izmenjevati informacije o vseh pomembnih zadevah z organi iz Uredbe (EU) 2016/679 in Direktive 2002/58/ES.

(35) V skladu s členom 42(1) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 17. novembra 2023 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

Ta uredba vzpostavlja omrežni kodeks, ki določa sektorska pravila za vidike kibernetske varnosti čezmejnih pretokov električne energije, vključno s pravili o skupnih minimalnih zahtevah, načrtovanju, spremljanju, poročanju in obvladovanju kriz.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za vidike kibernetske varnosti čezmejnih pretokov električne energije v dejavnostih naslednjih subjektov, če so v skladu s členom 24 opredeljeni kot subjekti z velikim ali kritičnim učinkom:

(a) elektroenergetskih podjetij, kot so opredeljena v členu 2(57) Direktive (EU) 2019/944;

(b) imenovanih operaterjev trga električne energije, kot so opredeljeni v členu 2(8) Uredbe (EU) 2019/943;

(c) organiziranih mest trgovanja ali organiziranih trgov, kot so opredeljeni v členu 2(4) Izvedbene uredbe Komisije (EU) št. 1348/2014 ([14]) in ki urejajo transakcije o proizvodih, pomembnih za čezmejne pretoke električne energije;

(d) izvajalcev kritičnih IKT storitev iz člena 3(9) te uredbe;

(e) mreže ENTSO za električno energijo, vzpostavljene v skladu s členom 28 Uredbe (EU) 2019/943;

(f) telesa EU ODS, vzpostavljenega v skladu s členom 52 Uredbe (EU) 2019/943;

(g) bilančnih odgovornih akterjev, kot so opredeljeni v členu 2(14) Uredbe (EU) 2019/943;

(h) upravljavcev polnilnih mest, kot so opredeljeni v Prilogi I k Direktivi (EU) 2022/2555;

(i) regionalnih koordinacijskih centrov, vzpostavljenih v skladu s členom 35 Uredbe (EU) 2019/943;

(j) ponudnikov upravljanih varnostnih storitev, kot so opredeljeni v členu 6(40) Direktive (EU) 2022/2555;

(k) katerega koli drugega subjekta ali tretje strani, na katero so prenesena ali ki so jim dodeljena pooblastila v skladu s to uredbo.

2. Za izvajanje nalog, dodeljenih s to uredbo, so v okviru svojega sedanjega mandata odgovorni naslednji organi:

(a) Agencija Evropske unije za sodelovanje energetskih regulatorjev (v nadaljnjem besedilu: ACER), ustanovljena z Uredbo (EU) 2019/942 Evropskega parlamenta in Sveta ([15]);

(b) nacionalni pristojni organi, ki so odgovorni za izvajanje nalog, dodeljenih na podlagi te uredbe, in ki jih imenujejo države članice v skladu s členom 4, oziroma „pristojni organ“;

(c) nacionalni regulativni organi, ki jih imenuje vsaka država članica v skladu s členom 57(1) Direktive (EU) 2019/944;

([14]) Izvedbena uredba Komisije (EU) št. 1348/2014 z dne 17. decembra 2014 o sporočanju podatkov v skladu s členom 8(2) in (6) Uredbe (EU) št. 1227/2011 Evropskega parlamenta in Sveta o celovitosti in preglednosti veleprodajnega energetskega trga (UL L 363, 18.12.2014, str. 121).

([15]) Uredba (EU) 2019/942 Evropskega parlamenta in Sveta z dne 5. junija 2019 o ustanovitvi Agencije Evropske unije za sodelovanje energetskih regulatorjev (UL L 158, 14.6.2019, str. 22).

(d) pristojni organi za pripravljenost na tveganja, vzpostavljeni na podlagi člena 3 Uredbe (EU) 2019/941;

(e) skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT), določene ali vzpostavljene na podlagi člena 10 Direktive (EU) 2022/2555;

(f) pristojni organi, odgovorni za kibernetsko varnost, imenovani ali vzpostavljeni na podlagi člena 8 Direktive (EU) 2022/2555;

(g) Agencija Evropske unije za kibernetsko varnost, vzpostavljena na podlagi Uredbe (EU) 2019/881;

(h) kateri koli drug subjekt ali tretja stran, na katero so prenesena ali ki so jim dodeljena pooblastila v skladu s členom 4(3).

3. Ta uredba se uporablja tudi za vse subjekte, ki niso ustanovljeni v Uniji, vendar opravljajo storitve za subjekte v Uniji, pod pogojem, da jih pristojni organi v skladu s členom 24(2) opredelijo kot subjekte z velikim ali kritičnim učinkom.

4. Ta direktiva ne posega v pristojnosti držav članic, da zaščitijo nacionalno varnost, in v njihova pooblastila za zaščito drugih bistvenih državnih funkcij, vključno z zagotavljanjem ozemeljske celovitosti države ter vzdrževanjem javnega reda in miru.

5. Ta uredba ne posega v odgovornosti držav članic za zaščito nacionalne varnosti v zvezi z dejavnostmi na področju proizvodnje električne energije v jedrskih elektrarnah, vključno z dejavnostmi znotraj jedrske vrednostne verige, v skladu s Pogodbama.

6. Subjekti, pristojni organi, enotne kontaktne točke na ravni subjekta in skupine CSIRT obdelujejo osebne podatke v obsegu, ki je potreben za namene te uredbe, in v skladu z Uredbo (EU) 2016/679, pri čemer mora taka obdelava zlasti temeljiti na členu 6 Uredbe.

Člen 3

Opredelitev pojmov

Uporabljajo se naslednje opredelitve pojmov:

(1) „sredstvo“ pomeni vsako opredmeteno ali neopredmeteno informacijo ali programsko ali strojno opremo v omrežnih in informacijskih sistemih, ki ima vrednost za posameznika, organizacijo ali vlado;

(2) „pristojni organ za pripravljenost na tveganja“ pomeni pristojni organ, imenovan na podlagi člena 3 Uredbe (EU) 2019/941;

(3) „skupina za odzivanje na incidente na področju računalniške varnosti“ pomeni skupino, pristojno za obvladovanje tveganj in incidentov v skladu s členom 10 Direktive (EU) 2022/2555;

(4) „sredstvo s kritičnim učinkom“ pomeni sredstvo, potrebno za izvajanje postopka s kritičnim učinkom;

(5) „subjekt s kritičnim učinkom“ pomeni subjekt, ki izvaja postopek s kritičnim učinkom in ki ga pristojni organi opredelijo v skladu s členom 24;

(6) „območje s kritičnim učinkom“ pomeni območje, ki ga opredeli subjekt iz člena 2(1), ki vsebuje vsa sredstva s kritičnim učinkom in na katerih je mogoče nadzorovati dostop do teh sredstev ter ki opredeljuje področje uporabe razširjenih kontrol kibernetske varnosti;

(7) „postopek s kritičnim učinkom“ pomeni poslovni postopek, ki ga izvaja subjekt, pri katerem indeksi učinka na kibernetsko varnost elektroenergetskega sistema presegajo prag kritičnega učinka;

(8) „prag kritičnega učinka“ pomeni vrednosti indeksov učinka na kibernetsko varnost elektroenergetskega sistema iz člena 19(3), točka (b), nad katerimi kibernetski napad na poslovni postopek povzroči kritično motnjo v čezmejnih pretokih električne energije;

(9) „izvajalec kritičnih IKT storitev“ pomeni subjekt, ki zagotavlja storitev IKT, ali postopek IKT, ki je potreben za postopek s kritičnim ali velikim učinkom, ki vpliva na vidike kibernetske varnosti čezmejnih pretokov električne energije, in lahko, če je ogrožen, povzroči kibernetski napad, katerega učinek presega prag kritičnega ali velikega učinka;

(10) „čezmejni pretok električne energije“ pomeni čezmejni pretok, kot je opredeljen v členu 2, točka 3, Uredbe (EU) 2019/943;

(11) „kibernetski napad“ pomeni incident, kot je opredeljen v členu 3, točka 14, Uredbe (EU) 2022/2554;

(12) „kibernetska varnost“ pomeni kibernetsko varnost, kot je opredeljena v členu 2, točka 1, Uredbe (EU) 2019/881;

(13) „kontrola kibernetske varnosti“ pomeni ukrepe ali postopke, ki se izvajajo za preprečevanje in odkrivanje tveganj za kibernetsko varnost, boj proti takim tveganjem in njihovemu zmanjšanju;

(14) „kibernetski incident“ pomeni incident, kot je opredeljen v členu 6, točka 6, Direktive (EU) 2022/2555;

(15) „sistem upravljanja kibernetske varnosti“ pomeni politike, postopke, smernice ter povezana sredstva in dejavnosti, ki jih skupaj upravlja subjekt, da bi svoja informacijska sredstva zaščitil pred kibernetskimi grožnjami s sistematičnim vzpostavljanjem, izvajanjem, upravljanjem, spremljanjem, pregledovanjem, vzdrževanjem in izboljševanjem varnosti omrežnega in informacijskega sistema organizacije;

(16) „operativni center za kibernetsko varnost“ pomeni namenski center, v katerem tehnična skupina, ki jo sestavljajo en ali več strokovnjakov, ob podpori informacijskih sistemov za kibernetsko varnost izvaja varnostne naloge (v nadaljnjem besedilu: storitve operacijskega centra za kibernetsko varnost), kot so obvladovanje kibernetskih napadov in odpravljanje napak v varnostnih konfiguracijah, spremljanje varnosti, analiza dnevnikov in odkrivanje kibernetskih napadov;

(17) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kot je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(18) „obvladovanje ranljivosti na področju kibernetske varnosti“ pomeni prepoznavanje in obravnavanje ranljivosti;

(19) „subjekt“ pomeni subjekt, kot je opredeljen v členu 6, točka 38, Direktive (EU) 2022/2555;

(20) „zgodnje opozarjanje“ pomeni potrebne informacije za določitev, ali obstaja sum, da je pomemben incident nastal zaradi nezakonitih ali zlonamernih dejanj, in ali bi ta incident lahko imel čezmejni učinek;

(21) „indeks učinka na kibernetsko varnost elektroenergetskega sistema“ ali „ECII“ pomeni indeks ali lestvico razvrščanja možnih posledic kibernetskih napadov za poslovne postopke, ki so vključeni v čezmejne pretoke električne energije;

(22) „evropska certifikacijska shema za kibernetsko varnost“ pomeni shemo, kot je opredeljena v členu 2, točka 9, Uredbe (EU) 2019/881;

(23) „subjekt z velikim učinkom“ pomeni subjekt, ki izvaja postopek z velikim učinkom in ki ga pristojni organi opredelijo v skladu s členom 24;

(24) „postopek z velikim učinkom“ pomeni poslovni postopek, ki ga izvaja subjekt, pri katerem indeksi učinka na kibernetsko varnost elektroenergetskega sistema presegajo prag velikega učinka;

(25) „sredstvo z velikim učinkom“ pomeni sredstvo, potrebno za izvajanje postopka z velikim učinkom;

(26) „prag velikega učinka“ pomeni vrednosti indeksov učinka na kibernetsko varnost elektroenergetskega sistema iz člena 19(3), točka (b); kadar so te vrednosti presežene, uspešen kibernetski napad na postopek povzroči veliko motnjo v čezmejnih pretokih električne energije;

(27) „območje z velikim učinkom“ pomeni območje, ki ga opredeli kateri koli subjekt iz člena 2(1), ki vsebuje vsa sredstva z velikim učinkom in na katerem je mogoče nadzorovati dostop do teh sredstev ter ki opredeljuje področje uporabe minimalnih kontrol kibernetske varnosti;

(28) „proizvod IKT“ pomeni proizvod IKT, kot je opredeljen v členu 2, točka 12, Uredbe (EU) 2019/881;

(29) „storitev IKT“ pomeni storitev IKT, kot je opredeljena v členu 2, točka 13, Uredbe (EU) 2019/881;

(30) „postopek IKT“ pomeni postopek IKT, kot je opredeljen v členu 2, točka 14, Uredbe (EU) 2019/881;

(31) „obstoječi sistem“ pomeni obstoječi sistem IKT, kot je opredeljen v členu 3(3) Uredbe (EU) 2022/2554;

(32) „nacionalna enotna kontaktna točka“ pomeni enotno kontaktno točko, ki jo določi ali vzpostavi vsaka država članica v skladu s členom 8(3) Direktive (EU) 2022/2555;

(33) „organi za obvladovanje kibernetskih kriz v omrežnih in informacijskih sistemih“ pomeni organe, določene ali vzpostavljene v skladu s točko 9(1) Direktive (EU) 2022/2555;

(34) „izdajatelj“ pomeni subjekt, ki sproži dogodek za izmenjavo ali shranjevanje informacij;

(35) „specifikacije za javna naročila“ pomeni specifikacije, ki jih subjekti opredelijo pri javnem naročanju novih ali posodobljenih proizvodov IKT, postopkov IKT ali storitev IKT;

(36) „predstavnik“ pomeni fizično ali pravno osebo s sedežem v Uniji, ki je izrecno imenovana za delovanje v imenu subjekta z velikim ali kritičnim učinkom, ki nima sedeža v Uniji, vendar opravlja storitve za subjekte v Uniji, in na katerega se lahko pristojni organ ali skupina CSIRT namesto na sam subjekt z velikim ali kritičnim učinkom obrne v zvezi z obveznostmi navedenega subjekta, ki izhajajo iz te uredbe;

(37) „tveganje“ pomeni tveganje, kot je opredeljeno v členu 6(9) Direktive (EU) 2022/2555;

(38) „matrika učinka tveganja“ pomeni matriko, ki se uporabi pri oceni tveganja za določitev posledične stopnje učinka tveganja za vsako ocenjeno tveganje;

(39) „sočasna kriza pri oskrbi z električno energijo“ pomeni krizo pri oskrbi z električno energijo, kot je opredeljena v členu 2, točka 10, Uredbe (EU) 2019/941;

(40) „enotna kontaktna točka na ravni subjekta“ pomeni enotno kontaktno točko na ravni subjekta, določeno na podlagi člena 38(1), točka (c);

(41) „deležnik“ pomeni vsako stran, v katere interesu sta uspeh in tekoče delovanje organizacije ali postopka, kot so zaposleni, direktorji, delničarji, regulatorji, združenja, dobavitelji in odjemalci;

(42) „standard“ pomeni standard, kot je opredeljen v členu 2(1) Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([16]);

(43) „regija obratovanja sistema“ pomeni regije obratovanja sistema, kot so opredeljene v Prilogi I k Sklepu ACER št. 05/2022 o opredelitvi regij obratovanja sistema in vzpostavljene v skladu s členom 36 Uredbe (EU) 2019/943;

(44) „operater sistema“ pomeni operaterja distribucijskega sistema in operaterja prenosnega sistema, kot sta opredeljena v členu 2(29) in (35) Direktive (EU) 2019/944;

(45) „postopek s kritičnim učinkom na ravni Unije“ pomeni vsak postopek v sektorju električne energije, ki po možnosti vključuje več subjektov in pri katerem se morebiten učinek kibernetskega napada lahko šteje za kritičnega v okviru ocene tveganja za kibernetsko varnost na ravni Unije;

(46) „postopek z velikim učinkom na ravni Unije“ pomeni vsak postopek v sektorju električne energije, ki po možnosti vključuje več subjektov in pri katerem se morebiten učinek kibernetskega napada lahko šteje za velikega v okviru ocene tveganja za kibernetsko varnost na ravni Unije;

(47) „nepopravljena aktivno izrabljena ranljivost“ pomeni ranljivost, ki še ni bila javno razkrita in popravljena in za katero obstajajo zanesljivi dokazi, da je akter izvedel zlonamerno kodo v sistemu brez dovoljenja lastnika sistema;

(48) „ranljivost“ pomeni ranljivost, kot je opredeljena v členu 6, točka 15, Direktive (EU) 2022/2555.

Člen 4

Pristojni organ

1. Takoj ko je to mogoče, v vsakem primeru pa do 13. decembra 2024, vsaka država članica imenuje nacionalni vladni ali regulativni organ, ki je pristojen za opravljanje nalog, dodeljenih s to uredbo (v nadaljnjem besedilu: pristojni organ). Dokler se pristojnemu organu ne dodelijo naloge na podlagi te uredbe, regulativni organ, ki ga imenuje vsaka država članica v skladu s členom 57(1) Direktive (EU) 2019/944, opravlja naloge pristojnega organa v skladu s to uredbo.

2. Države članice nemudoma pošljejo uradno obvestilo Komisiji, ACER, ENISA, Skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, vzpostavljeno na podlagi člena 14 Direktive (EU) 2022/2555, in usklajevalni skupini za električno energijo, ustanovljeno na podlagi člena 1 Sklepa Komisije z dne 15. novembra 2012 ([17]), v katerem jim sporočijo ime in kontaktne podatke svojega pristojnega organa, imenovanega na podlagi odstavka 1 tega člena, ter vse naknadne spremembe teh podatkov.

([16]) Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12).

([17]) Sklep Komisije z dne 15. novembra 2012 o ustanovitvi usklajevalne skupine za električno energijo (2012/C 353/02) (UL C 353, 17.11.2012, str. 2).

3. Države članice lahko dovolijo svojemu pristojnemu organu, da naloge, ki so mu dodeljene s to uredbo, prenese na druge nacionalne organe, z izjemo nalog iz člena 5. Vsak pristojni organ spremlja, kako organi, na katere je prenesel naloge, uporabljajo to uredbo. Pristojni organ sporoči Komisiji, ACER, ENISA, usklajevalni skupini za električno energijo in Skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ime organov, na katere so bile naloge prenesene, njihove kontaktne podatke, dodeljene naloge in vse naknadne spremembe teh podatkov.

Člen 5

Sodelovanje med ustreznimi organi in telesi na nacionalni ravni

Pristojni organi usklajujejo in zagotavljajo ustrezno sodelovanje med pristojnimi organi, odgovornimi za kibernetsko varnost, organi za obvladovanje kibernetskih kriz, nacionalnimi regulativnimi organi, pristojnimi organi za pripravljenost na tveganja in skupinami CSIRT, da bi se izpolnile ustrezne obveznosti, določene v tej uredbi. Pristojni organi se tudi usklajujejo z vsemi drugimi telesi ali organi, ki jih določi vsaka država članica, da bi zagotovili učinkovite postopke in preprečili podvajanja nalog in obveznosti. Pristojni organi lahko zadevnim nacionalnim regulativnim organom naročijo, naj ACER zaprosijo za mnenje v skladu s členom 8(3).

Člen 6

Pogoji ali metodologije oziroma načrti

1. Operaterji prenosnih sistemov v sodelovanju s telesom EU ODS pripravijo predloge pogojev ali metodologij v skladu z odstavkom 2 oziroma načrtov v skladu z odstavkom 3.

2. Vsi pristojni organi odobrijo predloge naslednjih pogojev ali metodologij in vse njihove spremembe:

(a) metodologije za oceno tveganja za kibernetsko varnost na podlagi člena 18(1);

(b) celovito poročilo o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije na podlagi člena 23;

(c) minimalne in razširjene kontrole kibernetske varnosti na podlagi člena 29, kartiranje kontrol kibernetske varnosti v sektorju električne energije glede na standarde na podlagi člena 34, vključno z minimalnimi in razširjenimi kontrolami kibernetske varnosti v dobavni verigi v skladu s členom 33;

(d) priporočila za javno naročanje na področju kibernetske varnosti na podlagi člena 35;

(e) metodologijo lestvice razvrščanja kibernetskih napadov na podlagi člena 37(8).

3. Predloge regionalnih načrtov za zmanjšanje tveganja za kibernetsko varnost na podlagi člena 22 odobrijo vsi pristojni organi zadevne regije obratovanja sistema.

4. Predlogi pogojev ali metodologij iz odstavka 2 oziroma načrtov iz odstavka 3 vključujejo predlagani časovni okvir za njihovo izvajanje in opis njihovega pričakovanega učinka na cilje te uredbe.

5. Telo EU ODS lahko zadevnim operaterjem prenosnih sistemov predloži obrazloženo mnenje najpozneje tri tedne pred rokom za predložitev predloga pogojev ali metodologij oziroma načrtov pristojnim organom. Operaterji prenosnih sistemov, odgovorni za predloge pogojev ali metodologij oziroma načrtov, pred njihovo predložitvijo pristojnim organom v odobritev upoštevajo utemeljeno mnenje telesa EU ODS. Operaterji prenosnih sistemov predložijo utemeljitev, kadar se mnenje telesa EU ODS ne upošteva.

6. Sodelujoči operaterji prenosnih sistemov tesno sodelujejo pri skupnemu oblikovanju pogojev in metodologij ter načrtov. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS redno obveščajo pristojne organe in ACER o napredku pri oblikovanju pogojev ali metodologij oziroma načrtov.

Člen 7

Pravila glasovanja pri operaterjih prenosnih sistemov

1. Če operaterji prenosnih sistemov pri odločanju o predlogih pogojev ali metodologij ne morejo doseči dogovora, odločajo z glasovanjem s kvalificirano večino. Kvalificirana večina za take predloge se izračuna na naslednji način:

(a) operaterji prenosnih sistemov, ki predstavljajo vsaj 55 % držav članic, in

(b) operaterji prenosnih sistemov, ki predstavljajo države članice, ki zajemajo vsaj 65 % prebivalstva Unije.

2. Manjšina, ki lahko prepreči sprejetje sklepov o predlogih pogojev ali metodologij iz člena 6(2), mora vključevati operaterje prenosnih sistemov, ki predstavljajo najmanj štiri države članice, v nasprotnem primeru se šteje, da je kvalificirana večina dosežena.

3. Kadar operaterji prenosnih sistemov pri odločanju o predlogih pogojev ali metodologij iz člena 6(2) ne morejo doseči dogovora, regijo obratovanja sistema pa sestavlja več kot pet držav članic, odločajo z glasovanjem s kvalificirano večino. Za kvalificirano večino za predloge iz člena 6(2) je potrebna večina:

(a) sistemskih operaterjev prenosnih omrežij, ki predstavljajo najmanj 72 % zadevnih držav članic, in

(b) operaterjev prenosnih sistemov, ki predstavljajo države članice, ki zajemajo vsaj 65 % prebivalstva zadevnega območja.

4. Manjšina, ki lahko prepreči sprejetje odločitev o predlogih načrtov, vključuje vsaj najmanjše število operaterjev prenosnih sistemov, ki predstavljajo več kot 35 % prebivalstva udeleženih držav članic, ter operaterje prenosnih sistemov, ki predstavljajo vsaj eno dodatno zadevno državo članico; v nasprotnem primeru se šteje, da je kvalificirana večina dosežena.

5. Pri odločitvah operaterjev prenosnih sistemov o predlogih pogojev ali metodologij na podlagi člena 6(2) se dodeli po en glas na državo članico. Če je na ozemlju države članice več kot en operater prenosnega sistema, država članica razdeli glasovalne pravice med operaterje prenosnih sistemov.

6. Če operaterji prenosnih sistemov v sodelovanju s telesom EU ODS ne predložijo prvotnega ali spremenjenega predloga pogojev ali metodologij oziroma načrtov ustreznim pristojnim organom v rokih, ki so določeni v tej uredbi, ustreznim pristojnim organom in ACER zagotovijo ustrezne osnutke pogojev ali metodologij oziroma načrtov. Pri tem pojasnijo, kaj je preprečilo sprejetje dogovora. Pristojni organi skupaj sprejmejo ustrezne ukrepe za sprejetje zahtevanih pogojev ali metodologij oziroma zahtevanih načrtov. To se lahko na primer stori tako, da se zahtevajo spremembe osnutkov iz tega odstavka, da se ti osnutki revidirajo in dopolnijo ali, če osnutki niso bili predloženi, da se opredelijo in odobrijo zahtevani pogoji ali metodologije oziroma načrti.

Člen 8

Predložitev predlogov pristojnim organom

1. Operaterji prenosnih sistemov predložijo predloge pogojev ali metodologij oziroma načrtov v odobritev ustreznim pristojnim organom v rokih, določenih v členih 18, 23, 29, 33, 34, 35 in 37. Pristojni organi lahko v izjemnih primerih te roke skupaj podaljšajo, zlasti kadar roka ni mogoče doseči zaradi okoliščin, na katere operaterji prenosnih sistemov ali subjekt EU ODS ne morejo vplivati.

2. Predlogi pogojev ali metodologij oziroma načrtov iz odstavka 1 se hkrati s predložitvijo pristojnim organom predložijo v vednost tudi ACER.

3. ACER na podlagi skupne prošnje nacionalnih regulativnih organov izda mnenje o predlogu pogojev ali metodologij oziroma načrtov v šestih mesecih po prejemu predlogov pogojev ali metodologij oziroma načrtov in o mnenju uradno obvesti nacionalne regulativne organe ter pristojne organe. Nacionalni regulativni organi, nacionalni pristojni organi, odgovorni za kibernetsko varnost, in vsi drugi organi, ki so imenovani kot pristojni organi, se medsebojno uskladijo, preden nacionalni regulativni organi zaprosijo ACER za mnenje. ACER lahko v tako mnenje vključi priporočila. ACER se pred izdajo mnenja o predlogih iz člena 6(2) posvetuje z ENISA.

4. Pristojni organi se med seboj posvetujejo in tesno sodelujejo ter usklajujejo, da bi dosegli dogovor o predlaganih pogojih ali metodologijah oziroma načrtih. Pred odobritvijo pogojev ali metodologij oziroma načrtov po potrebi revidirajo in dopolnijo predloge na podlagi posvetovanja z ENTSO za električno energijo in telesom EU ODS, da bi zagotovili, da so predlogi skladni s to uredbo in prispevajo k visoki skupni ravni kibernetske varnosti v Uniji.

5. Pristojni organi odločijo o pogojih ali metodologijah oziroma načrtih v šestih mesecih po prejetju pogojev ali metodologij oziroma načrtov od ustreznih pristojnih organov ali, kadar je primerno, zadnjega zadevnega ustreznega pristojnega organa.

6. Kadar ACER izda mnenje, ga ustrezni pristojni organi upoštevajo in sprejmejo svoje odločitve v šestih mesecih po prejemu mnenja ACER.

7. Kadar pristojni organi skupaj zahtevajo spremembe predlaganih pogojev ali metodologij oziroma načrtov, da bi jih izboljšali, operaterji prenosnih sistemov v sodelovanju s telesom EU ODS pripravijo predlog takih sprememb pogojev ali metodologij oziroma načrtov. Operaterji prenosnih sistemov predložijo spremenjen predlog v odobritev v dveh mesecih po prejetju zahteve pristojnih organov. Pristojni organi o spremenjenih pogojih ali metodologijah oziroma načrtih odločijo v dveh mesecih po njihovi predložitvi.

8. Kadar pristojni organi ne morejo doseči dogovora v roku iz odstavka 5 ali 7, o tem obvestijo Komisijo. Komisija lahko sprejme ustrezne ukrepe, da bi omogočila sprejetje zahtevanih pogojev ali metodologij oziroma načrtov.

9. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS objavijo pogoje ali metodologije oziroma načrte na svojih spletiščih po odobritvi s strani ustreznih pristojnih organov, razen kadar se take informacije štejejo za zaupne v skladu s členom 47.

10. Pristojni organi lahko skupaj od operaterjev prenosnih sistemov in telesa EU ODS zahtevajo predloge sprememb odobrenih pogojev ali metodologij oziroma odobrenih načrtov ter določijo rok za predložitev teh predlogov. Operaterji prenosnih sistemov lahko v sodelovanju s telesom EU ODS predlagajo spremembe pristojnim organom tudi na lastno pobudo. Predlogi sprememb pogojev ali metodologij oziroma sprememb načrtov se oblikujejo in odobrijo v skladu s postopkom, določenim v tem členu.

11. Operaterji prenosnih sistemov v sodelovanju s telesom EU ODS najmanj vsaka tri leta po prvem sprejetju ustreznih pogojev ali metodologij oziroma ustreznih sprejetih načrtov pregledajo učinkovitost sprejetih pogojev ali metodologij oziroma sprejetih načrtov ter o ugotovitvah pregleda nemudoma poročajo pristojnim organom in ACER.

Člen 9

Posvetovanje

1. Operaterji prenosnih sistemov se ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS posvetujejo z deležniki, vključno z ACER, ENISA in pristojnim organom vsake države članice, o osnutku predlogov pogojev ali metodologij iz člena 6(2) in načrtov iz člena 6(3). Posvetovanje ne sme trajati manj kot en mesec.

2. Predlogi pogojev ali metodologij iz člena 6(2), ki jih predložijo operaterji prenosnih sistemov v sodelovanju s telesom EU ODS, se objavijo in predložijo v posvetovanje na ravni Unije. Predlogi načrtov iz člena 6(3), ki jih predložijo ustrezni operaterji prenosnih sistemov v sodelovanju s telesom EU ODS na regionalni ravni, se predložijo v posvetovanje vsaj na regionalni ravni.

3. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in telesa EU ODS, ki je odgovorno za pripravo predloga pogojev ali metodologij oziroma načrtov, pred predložitvijo predloga v regulativno odobritev ustrezno upoštevajo stališča deležnikov, ki izhajajo iz posvetovanj, ki so potekala v skladu z odstavkom 1. V vseh primerih se hkrati s predložitvijo predloga navede tehtna utemeljitev razlogov za vključitev ali izključitev stališč, ki izhajajo iz posvetovanja, ter se pravočasno objavi pred predlogom pogojev ali metodologij ali hkrati z njo.

Člen 10

Udeležba deležnikov

ACER v tesnem sodelovanju z ENTSO za električno energijo in telesom EU ODS organizira udeležbo deležnikov, vključno z rednimi srečanji z deležniki, da bi se opredelile težave in predlagale izboljšave v zvezi z izvajanjem te uredbe.

Člen 11

Povračilo stroškov

1. Stroške, ki jih imajo operaterji prenosnih sistemov in operaterji distribucijskih sistemov in so predmet reguliranja omrežnih tarif ter izhajajo iz obveznosti iz te uredbe, vključno s stroški, ki jih imata ENTSO za električno energijo in telo EU ODS, oceni ustrezen nacionalni regulativni organ vsake države članice.

2. Stroški, za katere se oceni, da so razumni, učinkoviti in sorazmerni, se povrnejo z omrežnimi tarifami ali drugimi ustreznimi mehanizmi, kot določi ustrezen nacionalni regulativni organ.

3. Operaterji prenosnih sistemov in operaterji distribucijskih sistemov iz odstavka 1 na zahtevo ustreznih nacionalnih regulativnih organov v razumnem obdobju, ki ga določi nacionalni regulativni organ, predložijo informacije, potrebne za olajšanje ocenjevanja nastalih stroškov.

Člen 12

Spremljanje

1. ACER spremlja izvajanje te uredbe v skladu s členom 32(1) Uredbe (EU) 2019/943 in členom 4(2) Uredbe (EU) 2019/942. Pri tem lahko sodeluje ENISA in zaprosi za podporo ENTSO za električno energijo ter telo EU ODS. ACER redno obvešča usklajevalno skupino za električno energijo in Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov o izvajanju te uredbe.

2. ACER objavi poročilo najmanj vsaka tri leta po začetku veljavnosti te uredbe, da bi:

(a) pregledal stanje izvajanja veljavnih ukrepov za obvladovanje tveganja za kibernetsko varnost ob upoštevanju subjektov z velikim ali kritičnim učinkom;

(b) opredelil, ali so morda za preprečevanje tveganj za sektor električne energije potrebna dodatna pravila o skupnih zahtevah, načrtovanju, spremljanju, poročanju in obvladovanju krize, ter

(c) opredelil področja, kjer so potrebne izboljšave za revizijo te uredbe, ali določil področja, ki niso zajeta, in nove prednostne naloge, ki se lahko pojavijo zaradi tehnološkega razvoja.

3. ACER lahko do 13. junija 2025 v sodelovanju z ENISA in po posvetovanju z ENTSO za električno energijo ter telesom EU ODS izda navodila o ustreznih informacijah, ki jih je treba sporočiti ACER za namene spremljanja, ter postopku in pogostosti zbiranja teh informacij na podlagi kazalnikov uspešnosti, opredeljenih v skladu z odstavkom 5.

4. Pristojni organi imajo lahko dostop do ustreznih informacij v lasti ACER, ki so bile zbrane v skladu s tem členom.

5. ACER v sodelovanju z ENISA in ob podpori ENTSO za električno energijo ter telesa EU ODS izda nezavezujoče kazalnike uspešnosti za oceno operativne zanesljivosti, ki so povezani z vidiki kibernetske varnosti čezmejnih pretokov električne energije.

6. Subjekti iz člena 2(1) te uredbe predložijo ACER zahtevane informacije, ki so potrebne za izvajanje nalog iz odstavka 2.

Člen 13

Primerjanje

1. ACER do 13. junija 2025 v sodelovanju z ENISA pripravi nezavezujoča navodila za primerjanje izvajanja ukrepov kibernetske varnosti. Ta vodnik vsebuje pojasnila za nacionalne regulativne organe glede načel primerjanja izvedenih kontrol kibernetske varnosti v skladu z odstavkom 2 tega člena ob upoštevanju stroškov izvajanja kontrol in učinkovitosti funkcije postopkov, proizvodov, storitev, sistemov in rešitev, ki se uporabljajo pri izvajanju takih kontrol. Pri pripravi nezavezujočih navodil za primerjanje izvajanja ukrepov kibernetske varnosti ACER upošteva obstoječa primerjalna poročila. ACER nacionalnim regulativnim organom v vednost predloži nezavezujoča navodila za primerjanje izvajanja ukrepov kibernetske varnosti.

2. Nacionalni regulativni organi v 12 mesecih po pripravi navodil za primerjanje na podlagi odstavka 1 izvedejo primerjalno analizo, da bi ocenili, ali sedanje naložbe v kibernetsko varnost:

(a) zmanjšujejo tveganja, ki vplivajo na čezmejne pretoke električne energije;

(b) zagotavljajo želene rezultate in povečujejo učinkovitost pri razvoju elektroenergetskih sistemov ter

(c) ali so učinkovite in vključene v celotno javno naročanje sredstev in storitev.

3. Nacionalni regulativni organi lahko za namene primerjalne analize upoštevajo nezavezujoča navodila za primerjanje izvajanja ukrepov kibernetske varnosti, ki ga je pripravil ACER, in zlasti ocenijo:

(a) povprečen izdatek, povezan s kibernetsko varnostjo, za zmanjšanje tveganj, ki vplivajo na čezmejne pretoke električne energije, zlasti v zvezi s subjekti z velikim ali kritičnim učinkom;

(b) v sodelovanju z ENTSO za električno energijo in telesom EU ODS povprečne cene storitev, sistemov in proizvodov na področju kibernetske varnosti, ki v veliki meri prispevajo h krepitvi in ohranjanju ukrepov za obvladovanje tveganj za kibernetsko varnost v različnih regijah obratovanja sistema;

(c) obstoj in raven primerljivosti stroškov in funkcij storitev, sistemov in rešitev na področju kibernetske varnosti, ustreznih za izvajanje te uredbe, pri čemer opredelijo morebitne ukrepe, ki so potrebni za spodbujanje učinkovitosti pri porabi, zlasti kadar so morda potrebne tehnološke naložbe v kibernetsko varnost.

4. Vse informacije v zvezi s primerjalno analizo se obravnavajo in obdelajo v skladu z zahtevami za razvrščanje podatkov iz te uredbe, minimalnimi kontrolami kibernetske varnosti in poročilom o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije. Primerjalna analiza iz odstavkov 2 in 3 se ne objavi.

5. Brez poseganja v zahteve glede zaupnosti iz člena 47 in potrebo po zaščiti varnosti subjektov, za katere veljajo določbe te uredbe, se primerjalna analiza iz odstavkov 2 in 3 tega člena posreduje vsem nacionalnim regionalnim organom, vsem pristojnim organom, ACER, ENISA in Komisiji.

Člen 14

Sporazumi z operaterji prenosnih sistemov izven Unije

1. Operaterji prenosnih sistemov v regiji obratovanja sistemov, ki je sosednja tretji državi, si v 18 mesecih po začetku veljavnosti te uredbe prizadevajo za sklenitev dogovorov z operaterji prenosnih sistemov iz sosednje tretje države, ki so skladni z ustreznim pravom Unije in v katerih je določena podlaga za sodelovanje pri zaščiti kibernetske varnosti, ter dogovorov o sodelovanju na področju kibernetske varnosti z navedenimi operaterji prenosnih sistemov.

2. Operaterji prenosnih sistemov obvestijo pristojni organ o dogovorih, sklenjenih na podlagi odstavka 1.

Člen 15

Pravni zastopniki

1. Subjekti, ki nimajo sedeža v Uniji, vendar opravljajo storitve za subjekte v Uniji in so bili z uradnim obvestilom priglašeni kot subjekti z velikim ali kritičnim učinkom v skladu s členom 24(6), v treh mesecih po uradnem obvestilu v pisni obliki določijo zastopnika v Uniji in o tem ustrezno obvestijo pristojni organ, ki pošlje uradno obvestilo.

2. Ta zastopnik je pooblaščen, da se v zvezi z obveznostmi subjekta z velikim ali kritičnim učinkom na podlagi te uredbe nanj poleg navedenega subjekta ali namesto njega obrne kateri koli pristojni organ ali skupina CSIRT v Uniji. Subjekt z velikim ali kritičnim učinkom svojemu pravnemu zastopniku da vsa potrebna pooblastila in ustrezna sredstva, s katerimi zagotovi njegovo učinkovito in pravočasno sodelovanje z ustreznimi pristojnimi organi ali skupinami CSIRT.

3. Zastopnik ima sedež v eni od držav članic, v kateri subjekt ponuja svoje storitve. Za subjekt se šteje, da spada v pristojnost države članice, v kateri ima zastopnik sedež. Subjekti z velikim ali kritičnim učinkom pristojnemu organu v državi članici, v kateri ima prebivališče ali sedež njegov pravni zastopnik, sporočijo ime, poštni naslov, elektronski naslov in telefonsko številko navedenega pravnega zastopnika.

4. Določeni pravni zastopnik je lahko odgovoren za neizpolnjevanje obveznosti na podlagi te uredbe, brez poseganja v odgovornost in sodne postopke, ki se lahko uvedejo zoper subjekta z velikim ali kritičnim učinkom.

5. Če v Uniji ni zastopnika, določenega v skladu s tem členom, lahko katera koli država članica, v kateri subjekt zagotavlja storitve, uvede sodne postopke proti subjektu zaradi neizpolnjevanja obveznosti na podlagi te uredbe.

6. Določitev pravnega zastopnika v Uniji na podlagi odstavka 1 ne pomeni ustanovitve sedeža v Uniji.

Člen 16

Sodelovanje med ENTSO za električno energijo in telesom EU ODS

1. ENTSO za električno energijo in telo EU ODS na podlagi členov 19 in 21 sodelujeta pri ocenjevanju tveganja za kibernetsko varnost ter zlasti pri naslednjih nalogah:

(a) oblikovanju metodologije za oceno tveganja za kibernetsko varnost na podlagi člena 18(1);

(b) pripravi celovitega poročila o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije na podlagi člena 23;

(c) oblikovanju skupnega okvira za kibernetsko varnost elektroenergetskega sistema na podlagi poglavja III;

(d) pripravi priporočila za javno naročanje na področju kibernetske varnosti na podlagi člena 35;

(e) oblikovanju metodologije lestvice razvrščanja kibernetskih napadov na podlagi člena 37(8).

(f) razvoju začasnega ECII na podlagi člena 48(1), točka (a);

(g) pripravi konsolidiranega začasnega seznama subjektov z velikim ali kritičnim učinkom na podlagi člena 48(3);

(h) pripravi začasnega seznama postopkov z velikim ali kritičnim učinkom na ravni Unije na podlagi člena 48(4);

(i) pripravi začasnega seznama evropskih in mednarodnih standardov in kontrol na podlagi člena 48(6);

(j) ocenjevanju tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19;

(k) regionalnem ocenjevanju tveganja za kibernetsko varnost na podlagi člena 21;

(l) opredelitvi regionalnih načrtov za zmanjšanje tveganja za kibernetsko varnost na podlagi člena 22;

(m) pripravi smernic o evropskih certifikacijskih shemah za kibernetsko varnost za proizvode IKT, storitve IKT in postopke IKT v skladu s členom 36 ter

(n) pripravi smernic za izvajanje te uredbe ob posvetovanju z ACER in ENISA.

2. ENTSO za električno energijo in telo EU ODS lahko sodelujeta v okviru delovne skupine za tveganja za kibernetsko varnost.

3. ENTSO za električno energijo in telo EU ODS redno obveščata ACER, ENISA, Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ter usklajevalno skupino za električno energijo o napredku pri ocenjevanju tveganja za kibernetsko varnost na ravni Unije in regionalnem ocenjevanju tveganja na podlagi členov 19 in 21.

Člen 17

Sodelovanje med ACER in pristojnimi organi

ACER v sodelovanju z vsakim pristojnim organom:

(1) spremlja izvajanje ukrepov za obvladovanje tveganja za kibernetsko varnost na podlagi člena 12(2), točka (a), in obveznosti poročanja na podlagi členov 27 in 39 ter

(2) spremlja postopek sprejemanja in izvajanje pogojev ali metodologij oziroma načrtov na podlagi člena 6(2) in (3). ACER, ENISA in vsak pristojni organ lahko sodelujejo v okviru organa za spremljanje tveganj za kibernetsko varnost.

POGLAVJE II

OCENA TVEGANJA IN OPREDELITEV USTREZNIH TVEGANJ ZA KIBERNETSKO VARNOST

Člen 18

Metodologije za oceno tveganja za kibernetsko varnost

1. Operaterji prenosnih sistemov do 13. marca 2025 ob pomoči ENTSO za električno energijo, v sodelovanju s telesom EU ODS in po posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov predložijo predlog metodologij za oceno tveganja za kibernetsko varnost na ravni Unije, regionalni ravni in ravni držav članic.

2. Metodologije za oceno tveganja za kibernetsko varnost na ravni Unije, regionalni ravni in ravni držav članic vključujejo:

(a) seznam kibernetskih groženj, ki jih je treba upoštevati, med drugim tudi vsaj naslednje grožnje v dobavni verigi:

(i) hudo in nepričakovano motnjo v dobavni verigi;

(ii) nerazpoložljivost proizvodov IKT, storitev IKT ali postopkov IKT iz dobavne verige;

(iii) kibernetske napade, ki se izvedejo prek akterjev v dobavni verigi;

(iv) uhajanje občutljivih informacij prek dobavne verige, vključno s spremljanjem dobavne verige;

(v) uvajanje ranljivosti ali t. i. stranskih vrat v proizvode IKT, storitve IKT ali postopke IKT prek akterjev v dobavni verigi;

(b) merila za oceno učinka tveganj za kibernetsko varnost kot velikega ali kritičnega z uporabo opredeljenih pragov za posledice in verjetnost;

(c) pristop za analizo tveganj za kibernetsko varnost, ki izhajajo iz obstoječih sistemov, kaskadnih učinkov kibernetskih napadov in narave sistemov, ki upravljajo omrežje v realnem času;

(d) pristop za analizo tveganj za kibernetsko varnost, ki izhajajo iz odvisnosti od enega samega dobavitelja proizvodov IKT, storitev IKT ali postopkov IKT.

3. Z metodologijami za oceno tveganja za kibernetsko varnost na ravni Unije, regionalni ravni in ravni držav članic se ocenjujejo tveganja za kibernetsko varnost z uporabo enake matrike učinka tveganja. Matrika učinka tveganja:

(a) meri posledice kibernetskih napadov na podlagi naslednjih meril:

(i) izpada napajanja;

(ii) zmanjšanja proizvodnje električne energije;

(iii) izgube zmogljivosti rezerve za primarno regulacijo frekvence;

(iv) izgube zmogljivosti za obnovo obratovanja omrežja električne energije brez zanašanja na zunanje prenosno omrežje za ponovno vzpostavitev po popolni ali delni zaustavitvi (t. i. zagon brez zunanjega vira napajanja);

(v) pričakovanega trajanja izpada električne energije, ki vpliva na odjemalce, skupaj z obsegom izpada glede na število odjemalcev, ter

(vi) vseh drugih kvantitativnih ali kvalitativnih meril, ki bi se lahko razumno uporabljala kot kazalnik učinka kibernetskega napada na čezmejne pretoke električne energije;

(b) meri verjetnost incidentov, kot je pogostost kibernetskih napadov na leto.

4. Z metodologijami za oceno tveganja za kibernetsko varnost na ravni Unije se opiše, kako se opredelijo vrednosti ECII za pragove velikega ali kritičnega učinka. ECII omogoča subjektom, da s pomočjo meril iz odstavka 2, točka (b), ocenijo učinek tveganj na svoje poslovne postopke v okviru ocen poslovnega učinka, ki jih izvedejo na podlagi člena 26(4), točka (c)(i).

5. ENTSO za električno energijo ob usklajevanju s telesom EU ODS obvesti usklajevalno skupino za električno energijo o predlogih metodologij za oceno tveganja za kibernetsko varnost, ki se oblikujejo v skladu z odstavkom 1.

Člen 19

Ocene tveganja za kibernetsko varnost na ravni Unije

1. ENTSO za električno energijo v sodelovanju s telesom EU ODS in ob posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov brez poseganja v člen 22 Direktive (EU) 2022/2555 v devetih mesecih po odobritvi metodologij za oceno tveganja za kibernetsko varnost na podlagi člena 8 in vsaka tri leta po tem oceni tveganje za kibernetsko varnost na ravni Unije in pripravi osnutek poročila o oceni tveganja za kibernetsko varnost na ravni Unije. Pri tem se uporabijo metodologije, oblikovane na podlagi člena 18 in odobrene na podlagi člena 8, da se opredelijo, analizirajo in ocenijo možne posledice kibernetskih napadov, ki vplivajo na obratovalno sigurnost elektroenergetskega sistema in povzročajo motnje v čezmejnih pretokih električne energije. Pri oceni tveganja za kibernetsko varnost na ravni Unije se ne upošteva pravna ali finančna škoda oziroma škoda za ugled, ki jo povzročijo kibernetski napadi.

2. Poročilo o oceni tveganja za kibernetsko varnost na ravni Unije vključuje naslednje elemente:

(a) postopke z velikim ali kritičnim učinkom na ravni Unije ter

(b) matriko učinka tveganja, ki jo subjekti in pristojni organi uporabijo za oceno tveganja za kibernetsko varnost, opredeljeno v oceni tveganja za kibernetsko varnost na ravni držav članic, izvedeno na podlagi člena 20, in oceni tveganja za kibernetsko varnost na ravni subjekta, izvedeno na podlagi člena 26(2), točka (b).

3. Poročilo o oceni tveganja za kibernetsko varnost na ravni Unije ob upoštevanju postopkov z velikim ali kritičnim učinkom na ravni Unije vključuje:

(a) oceno možnih posledic kibernetskega napada z uporabo metrike, opredeljene v metodologiji za oceno tveganja za kibernetsko varnost, oblikovani na podlagi člena 18(2), (3) in (4) ter odobreni na podlagi člena 8, in

(b) ECII ter pragove velikega in pragove kritičnega učinka, ki jih pristojni organi uporabijo na podlagi člena 24(1) in (2) za opredelitev subjektov z velikim ali kritičnim učinkom, ki so vključeni v postopke z velikim ali kritičnim učinkom na ravni Unije.

4. ENTSO za električno energijo v sodelovanju s telesom EU ODS predloži ACER v vednost osnutek poročila za oceno tveganja za kibernetsko varnost na ravni Unije z rezultati ocene tveganja za kibernetsko varnost na ravni Unije. ACER izda mnenje o osnutku poročila v treh mesecih po njegovem prejemu. ENTSO za električno energijo in telo EU ODS v največji možni meri upoštevata mnenje ACER pri dokončanju tega poročila.

5. ENTSO za električno energijo v sodelovanju s telesom EU ODS v treh mesecih po prejemu mnenja ACER uradno obvesti ACER, Komisijo, ENISA in pristojne organe o končnem poročilu o oceni tveganja za kibernetsko varnost na ravni Unije.

Člen 20

Ocena tveganja za kibernetsko varnost na ravni držav članic

1. Vsak pristojni organ v svoji državi članici oceni tveganje za kibernetsko varnost na ravni države članice v zvezi z vsemi subjekti z velikim ali kritičnim učinkom, pri čemer uporabi metodologije, oblikovane na podlagi člena 18 in odobrene na podlagi člena 8. V oceni tveganja za kibernetsko varnost na ravni držav članic se opredelijo in analizirajo tveganja kibernetskih napadov, ki vplivajo na obratovalno sigurnost elektroenergetskega sistema in povzročajo motnje v čezmejnih pretokih električne energije. Pri oceni tveganja za kibernetsko varnost na ravni držav članic se ne upoštevajo pravna ali finančna škoda oziroma škoda za ugled, ki jo povzročijo kibernetski napadi.

2. Vsak pristojni organ v 21 mesecih po priglasitvi subjektov z velikim ali kritičnim učinkom na podlagi člena 24(6) in vsaka tri leta po tem datumu ob podpori skupine CSIRT ter po posvetovanju z nacionalnim pristojnim organom, odgovornim za kibernetsko varnost, predloži ENTSO za električno energijo in telesu EU ODS poročilo o oceni tveganja za kibernetsko varnost na ravni države članice, ki vsebuje naslednje informacije za vsak poslovni postopek z velikim ali kritičnim učinkom:

(a) stanje izvajanja minimalnih in razširjenih kontrol na podlagi člena 29;

(b) seznam vseh kibernetskih napadov, prijavljenih v predhodnih treh letih na podlagi člena 38(3);

(c) povzetek informacij o kibernetski grožnji, prijavljenih v predhodnih treh letih na podlagi člena 38(6);

(d) za vsak postopek z velikim ali kritičnim učinkom na ravni Unije oceno tveganj ogroženosti zaupnosti, celovitosti in razpoložljivosti informacij ter ustreznih sredstev;

(e) po potrebi seznam dodatnih subjektov, ki so opredeljeni kot subjekti z velikim ali kritičnim učinkom na podlagi člena 24(1), (2), (3) in (5).

3. V poročilu o oceni tveganja za kibernetsko varnost na ravni držav članic se upošteva načrt pripravljenosti države članice na tveganja, pripravljen na podlagi člena 10 Uredbe (EU) 2019/941.

4. Informacije iz poročila o oceni tveganja za kibernetsko varnost na ravni držav članic iz odstavka 2, točke (a) do (d), niso povezane z nobenim določenim subjektom ali sredstvom. Poročilo o oceni tveganja za kibernetsko varnost na ravni držav članic vključuje tudi oceno tveganja začasnih odstopanj, ki jih izdajo pristojni organi v državah članicah na podlagi člena 30.

5. ENTSO za električno energijo in subjekt EU ODS lahko zaprosita pristojni organ za dodatne informacije v zvezi z nalogami iz pododstavka 2, točki (a) in (c).

6. Pristojni organi zagotovijo, da so informacije, ki jih predložijo, točne in pravilne.

Člen 21

Regionalne ocene tveganja za kibernetsko varnost

1. ENTSO za električno energijo v sodelovanju s telesom EU ODS in ob posvetovanju z ustreznim regionalnim koordinacijskim centrom izvede regionalno oceno tveganja za kibernetsko varnost za vsako regijo obratovanja sistema z uporabo metodologij, oblikovanih na podlagi člena 19 in odobrenih na podlagi člena 8, da bi opredelil, analiziral in ocenil tveganja kibernetskih napadov, ki vplivajo na obratovalno sigurnost elektroenergetskega sistema in povzročajo motnje v čezmejnih pretokih električne energije. Pri regionalni oceni tveganja za kibernetsko varnost se ne upošteva pravna ali finančna škoda oziroma škoda za ugled, ki jo povzročijo kibernetski napadi.

2. ENTSO za električno energijo v sodelovanju s telesom EU ODS in ob posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v 30 mesecih po priglasitvi subjektov z velikim ali kritičnim učinkom na podlagi člena 24(6) in vsaka tri leta po tem pripravi regionalno poročilo o oceni tveganja za kibernetsko varnost za vsako regijo obratovanja sistema.

3. V regionalnem poročilu o oceni tveganja za kibernetsko varnost se upoštevajo ustrezne informacije, vsebovane v poročilih o oceni tveganja za kibernetsko varnost na ravni Unije in na ravni držav članic.

4. V regionalni oceni tveganja za kibernetsko varnost se upoštevajo regionalni scenariji za krize pri oskrbi z električno energijo, povezani s kibernetsko varnostjo, ki so opredeljeni v členu 6 Uredbe (EU) 2019/941.

Člen 22

Regionalni načrti za zmanjšanje tveganja za kibernetsko varnost

1. ENTSO za električno energijo v sodelovanju s telesom EU ODS in ob posvetovanju z regionalnimi koordinacijskimi centri in Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v 36 mesecih po priglasitvi subjektov z velikim ali kritičnim učinkom na podlagi člena 24(6) in najpozneje do 13. junija 2031 ter vsaka tri leta po tem datumu pripravi regionalni načrt za zmanjšanje tveganja za kibernetsko varnost za vsako regijo obratovanja sistema.

2. Načrti za zmanjšanje tveganja za kibernetsko varnost vključujejo:

(a) minimalne in razširjene kontrole kibernetske varnosti, ki jih subjekti z velikim ali kritičnim učinkom uporabljajo v regijah obratovanja sistema, ter

(b) preostala tveganja za kibernetsko varnost v regijah obratovanja sistema po uporabi kontrol iz točke (a).

3. ENTSO za električno energijo predloži regionalne načrte za zmanjšanje tveganja ustreznim operaterjem prenosnih sistemov, pristojnim organom ter usklajevalni skupini za električno energijo. Usklajevalna skupina za električno energijo lahko priporoči spremembe.

4. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo, v sodelovanju s telesom EU ODS in ob posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov posodobijo regionalne načrte za zmanjšanje tveganja vsaka tri leta, razen če okoliščine zahtevajo pogostejša posodabljanja.

Člen 23

Celovito poročilo o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije

1. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo, v sodelovanju s telesom EU ODS in ob posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v 40 mesecih po priglasitvi subjektov z velikim ali kritičnim učinkom na podlagi člena 24(6) in nato vsaka tri leta predložijo usklajevalni skupini za električno energijo poročilo o rezultatih ocene tveganja za kibernetsko varnost v zvezi s čezmejnimi pretoki električne energije (v nadaljnjem besedilu: celovito poročilo o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije).

2. Celovito poročilo o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije temelji na poročilu o oceni tveganja za kibernetsko varnost na ravni Unije, poročilih o oceni tveganja za kibernetsko varnost na ravni držav članic ter regionalnih poročilih o oceni tveganja za kibernetsko varnost in vključuje naslednje informacije:

(a) seznam postopkov z velikim ali kritičnim učinkom na ravni Unije, opredeljenih v poročilu o oceni tveganja za kibernetsko varnost na ravni Unije v skladu s členom 19(2), točka (a), vključno z oceno verjetnosti in učinka tveganj za kibernetsko varnost, ocenjenih pri pripravi regionalnega poročila o oceni tveganja za kibernetsko varnost na podlagi člena 21(2) in člena 19(3), točka (a);

(b) sedanje kibernetske grožnje s posebnim poudarkom na pojavljajočih se grožnjah in tveganjih v elektroenergetskem sistemu;

(c) kibernetske grožnje v predhodnem obdobju na ravni Unije, pri čemer se zagotovi kritičen pregled morebitnega učinka takih kibernetskih napadov na čezmejne pretoke električne energije;

(d) splošno stanje izvajanja ukrepov kibernetske varnosti;

(e) stanje izvajanja tokov informacij na podlagi členov 37 in 38;

(f) seznam informacij ali posebnih meril za razvrščanje informacij na podlagi člena 46;

(g) opredeljena in poudarjena tveganja, ki lahko izhajajo iz nezanesljivega upravljanja dobavne verige;

(h) rezultate in zbrane izkušnje pri regionalnih in medregionalnih vajah na področju kibernetske varnosti, organiziranih na podlagi člena 44;

(i) analizo razvoja splošnih čezmejnih tveganj za kibernetsko varnost elektroenergetskega sistema od zadnje regionalne ocene tveganja za kibernetsko varnost;

(j) vse druge informacije, ki so lahko koristne za opredelitev možnih izboljšav te uredbe ali potrebe po reviziji te uredbe ali katerega koli od njenih orodij, ter

(k) informacije v zbirni in anonimizirani obliki o odstopanjih, odobrenih na podlagi člena 30(3).

3. Subjekti iz člena 2(1) lahko prispevajo k pripravi celovitega poročila o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije, pri čemer upoštevajo zaupnost informacij v skladu s členom 47. Operaterji prenosnih sistemov se ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS od zgodnje faze posvetujejo s temi subjekti.

4. Za celovito poročilo o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije veljajo pravila o varstvu izmenjave informacij na podlagi člena 46. ENTSO za električno energijo in telo EU ODS brez poseganja v člen 10(4) in člen 47(4) objavita javno različico navedenega poročila, ki ne vsebuje informacij, ki lahko povzročijo škodo subjektom iz člena 2(1). Javna različica tega poročila se objavi samo s soglasjem Skupine za sodelovanje na področju varnosti omrežnih in informacijskih sistemov in usklajevalne skupine za električno energijo. ENTSO za električno energijo je ob usklajevanju s telesom EU ODS odgovoren za pripravo in objavo javne različice poročila.

Člen 24

Opredelitev subjektov z velikim ali kritičnim učinkom

1. Vsak pristojni organ z uporabo ECII ter pragov velikega ali kritičnega učinka, vključenih poročilo o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(3), točka (b), v svoji državi članici opredeli subjekte z velikim ali kritičnim učinkom, ki so vključeni v postopke z velikim ali kritičnim učinkom na ravni Unije. Pristojni organi lahko subjekt v svoji državi članici zaprosijo za informacije za določitev vrednosti ECII za navedeni subjekt. Če ECII subjekta presega prag velikega ali kritičnega učinka, se opredeljeni subjekt vključi na seznam v poročilu o oceni tveganja za kibernetsko varnost na ravni države članice iz člena 20(2).

2. Vsak pristojni organ z uporabo ECII ter pragov velikega ali kritičnega učinka, vključenih poročilo o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(3), točka (b), opredeli subjekte z velikim ali kritičnim učinkom, ki nimajo sedeža v Uniji, če so dejavni znotraj Unije. Pristojni organ lahko subjekt, ki nima sedeža v Uniji, zaprosi za informacije za določitev vrednosti ECII za navedeni subjekt.

3. Vsak pristojni organ lahko v svoji državi članici opredeli dodatne subjekte kot subjekte z velikim ali kritičnim učinkom, če sta izpolnjeni naslednji merili:

(a) subjekt je del skupine subjektov, za katere obstaja znatno tveganje sočasnega kibernetskega napada;

(b) zbirni ECII za skupino subjektov presega prag velikega ali kritičnega učinka.

4. Če pristojni organ opredeli dodatne subjekte v skladu z odstavkom 3, se vsi postopki pri teh subjektih, katerih zbirni ECII za celotno skupino presega prag velikega učinka, štejejo za postopke z velikim učinkom, vsi postopki pri teh subjektih, katerih zbirni ECII za celotno skupino presega prag kritičnega učinka, pa se štejejo za postopke s kritičnim učinkom.

5. Če pristojni organ opredeli subjekte iz odstavka 3, točka (a), v več kot eni državi članici, o tem obvesti druge pristojne organe, ENTSO za električno energijo in telo EU ODS. ENTSO za električno energijo v sodelovanju s telesom EU ODS na podlagi informacij, prejetih od vseh pristojnih organov, pristojnim organom zagotovi analizo zbirne skupine subjektov iz več kot ene države članice, ki lahko ustvarijo porazdeljene motnje v čezmejnih pretokih električne energije, s čimer se lahko povzroči kibernetski napad. Kadar je skupina subjektov iz več držav članic opredeljena kot zbirna skupina, katere ECII presega prag velikega ali kritičnega učinka, vsi zadevni pristojni organi subjekte v taki skupini za svojo državo članico opredelijo kot subjekte z velikim ali kritičnim učinkom na podlagi zbirnega ECII za skupino subjektov, opredeljeni subjekti pa se vključijo na seznam v poročilu o oceni tveganja za kibernetsko varnost na ravni Unije.

6. Vsak pristojni organ v devetih mesecih po prejemu uradnega obvestila ENTSO za električno energijo in telesa EU ODS o poročilu o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(5) in vsekakor najpozneje do 13. junija 2028 subjekte s seznama uradno obvesti o tem, da so bili v svoji državi članici opredeljeni kot subjekti z velikim ali kritičnim učinkom.

7. Kadar je izvajalec storitev priglašen pristojnemu organu kot izvajalec kritičnih IKT storitev na podlagi člena 27, točka (c), pristojni organ o tem uradno obvesti pristojne organe držav članic, na ozemlju katerih je njegov sedež ali zastopnik. Ta pristojni organ uradno obvesti izvajalca storitev o tem, da je opredeljen kot izvajalec kritičnih storitev.

Člen 25

Nacionalni sistemi za preverjanje

1. Pristojni organi lahko vzpostavijo nacionalni sistem za preverjanje, da bi preverili, ali subjekti s kritičnim učinkom, opredeljeni na podlagi člena 24(1), izvajajo nacionalni zakonodajni okvir, ki je vključen v matriko za kartiranje iz člena 34. Nacionalni sistem za preverjanje lahko temelji na inšpekcijskem pregledu, ki ga opravi pristojni organ, neodvisnih varnostnih revizijah ali medsebojnih strokovnih pregledih, ki jih opravijo subjekti s kritičnim učinkom v isti državi članici pod nadzorom pristojnega organa.

2. Če se pristojni organ odloči vzpostaviti nacionalni sistem za preverjanje, zagotovi, da se preverjanje izvaja v skladu z naslednjimi zahtevami:

(a) stran, ki izvaja medsebojni strokovni pregled, revizijo ali inšpekcijski pregled, je neodvisna od subjekta s kritičnim učinkom, ki se preverja, in nima nobenih navzkrižij interesov;

(b) osebje, ki izvaja medsebojni strokovni pregled, revizijo ali inšpekcijski pregled, ima dokazano znanje na področju:

  (i) kibernetske varnosti v sektorju električne energije;

  (ii) sistemov za upravljanje kibernetske varnosti;

  (iii) revizijskih načel;

  (iv) ocen tveganja za kibernetsko varnost;

  (v) skupnega okvira za kibernetsko varnost elektroenergetskega sistema;

  (vi) nacionalne zakonodaje in regulativnega okvira ter evropskih in mednarodnih standardov v okviru preverjanja;

  (vii) postopkov s kritičnim učinkom v okviru preverjanja;

(c) strani, ki opravlja medsebojni strokovni pregled, revizijo ali inšpekcijski pregled, se omogoči dovolj časa za te dejavnosti;

(d) stran, ki opravlja medsebojni strokovni pregled, revizijo ali inšpekcijski pregled, sprejme ustrezne ukrepe za varstvo informacij, ki jih zbere med preverjanjem, v skladu s stopnjo zaupnosti;

(e) medsebojni strokovni pregledi, revizije ali inšpekcijski pregledi se opravijo najmanj enkrat na leto in zajemajo celoten okvir preverjanja najmanj vsaka tri leta.

3. Če se pristojni organ odloči vzpostaviti nacionalni sistem za preverjanje, vsako leto poroča ACER, kako pogosto je izvajal inšpekcijske preglede v okviru tega sistema.

Člen 26

Obvladovanje tveganja za kibernetsko varnost na ravni subjekta

1. Vsak subjekt z velikim ali kritičnim učinkom, kot ga opredelijo pristojni organi na podlagi člena 24(1), izvaja postopek obvladovanja tveganja za kibernetsko varnost za vsa svoja sredstva na območjih z velikim ali kritičnim učinkom. Vsak subjekt z velikim ali kritičnim učinkom vsaka tri leta izvede postopek obvladovanja tveganja za kibernetsko varnost, ki vključuje faze iz odstavka 2.

2. Vsak subjekt z velikim ali kritičnim učinkom utemelji svoj postopek obvladovanja tveganja za kibernetsko varnost na pristopu, katerega cilj je zaščititi omrežne in informacijske sisteme in ki vključuje naslednje faze:

(a) določitev okvira;

(b) oceno tveganja za kibernetsko varnost na ravni subjekta;

(c) obravnavo tveganja za kibernetsko varnost;

(d) sprejemanje tveganja za kibernetsko varnost.

3. V fazi določitve okvira vsak subjekt z velikim ali kritičnim učinkom:

(a) opredeli okvir ocene tveganja za kibernetsko varnost, vključno s postopki z velikim ali kritičnim učinkom, ki jih opredelita ENTSO za električno energijo in telo EU ODS, ter drugimi postopki, ki so lahko tarče kibernetskih napadov z velikim ali kritičnim učinkom na čezmejne pretoke električne energije, ter

(b) določi merila za oceno in sprejemanje tveganja v skladu z matriko učinka tveganja, ki jo subjekti in pristojni organi v skladu s členom 19(2) uporabijo za oceno tveganj za kibernetsko varnost v okviru metodologij za oceno tveganja za kibernetsko varnost na ravni Unije, regionalni ravni in ravni držav članic, ki jih oblikujeta ENTSO za električno energijo in telo EU ODS.

4. V fazi ocene tveganja za kibernetsko varnost vsak subjekt z velikim ali kritičnim učinkom:

(a) opredeli tveganja za kibernetsko varnost ob upoštevanju:

(i) vseh sredstev, ki podpirajo postopke z velikim ali kritičnim učinkom na ravni Unije, z oceno možnega učinka na čezmejne pretoke električne energije, če je sredstvo ogroženo;

(ii) možnih kibernetskih groženj, pri čemer se upoštevajo kibernetske grožnje, opredeljene v zadnjem celovitem poročilu o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije iz člena 23, ter groženj v dobavni verigi;

(iii) ranljivosti, vključno z ranljivostmi v obstoječih sistemih;

(iv) možnih scenarijev kibernetskih napadov, vključno s kibernetskimi napadi, ki vplivajo na obratovalno sigurnost elektroenergetskega sistema in povzročajo motnje v čezmejnih pretokih električne energije;

(v) ustreznih ocen tveganja na ravni Unije, vključno z usklajenimi ocenami tveganja za kritične dobavne verige v skladu s členom 22 Direktive (EU) 2022/2555; in

(vi) obstoječih izvedenih kontrol;

(b) analizira verjetnost in posledice tveganj za kibernetsko varnost, opredeljene v točki (a), in določi stopnjo tveganja za kibernetsko varnost z uporabo matrike učinka tveganja, ki se v skladu s členom 19(2) uporablja za oceno tveganj za kibernetsko varnost v okviru metodologij za oceno tveganja za kibernetsko varnost na ravni Unije, regionalni ravni in ravni držav članic, ki jih oblikujejo operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS;

(c) razvrsti sredstva glede na možne posledice v primeru ogroženosti kibernetske varnosti in določi območje z velikim ali kritičnim učinkom v okviru naslednjih korakov:

(i) z uporabo ECII izvede oceno poslovnega učinka za vse postopke, vključene v oceno tveganja za kibernetsko varnost;

(ii) z razvrstitvijo postopka kot postopka z velikim ali kritičnim učinkom, če njegov ECII presega prag velikega ali kritičnega učinka;

(iii) z opredelitvijo vseh sredstev z velikim ali kritičnim učinkom kot sredstev, potrebnih za postopke z velikim ali kritičnim učinkom;

(iv) z opredelitvijo območij z velikim ali kritičnim učinkom, ki vsebujejo vsa sredstva z velikim ali kritičnim učinkom, da bi se zagotovil nadzor dostopa do območij;

(d) oceni tveganja za kibernetsko varnost z njihovo prednostno razvrstitvijo ob pomoči meril za oceno tveganja in sprejemanje tveganja iz odstavka 3, točka (b).

5. V fazi obravnave tveganj za kibernetsko varnost vsak subjekt z velikim ali kritičnim učinkom pripravi načrt za zmanjšanje tveganja na ravni subjekta, tako da izbere možnosti obravnave tveganja, ki so primerne za obvladovanje tveganj, in opredeli preostala tveganja.

6. V fazi sprejemanja tveganja za kibernetsko varnost se vsak subjekt z velikim ali kritičnim učinkom odloči, ali bo sprejel preostalo tveganje na podlagi meril za sprejemanje tveganja, določenih v odstavku 3, točka (b).

7. Vsak subjekt z velikim ali kritičnim učinkom evidentira sredstva iz odstavka 1 v popisu sredstev. Ta popis sredstev ni del poročila o oceni tveganja.

8. Pristojni organ lahko med inšpekcijskimi pregledi pregleda sredstva iz popisa.

Člen 27

Poročanje o oceni tveganja na ravni subjekta

Vsak subjekt z velikim ali kritičnim učinkom v 12 mesecih po priglasitvi subjektov z velikim ali kritičnim učinkom na podlagi člena 24(6) in nato vsaka tri leta predloži pristojnemu organu poročilo, ki vsebuje naslednje informacije:

(1) seznam kontrol, izbranih za načrt za zmanjšanje tveganja na ravni subjekta na podlagi člena 26(5), z navedbo stanja izvajanja vsake kontrole;

(2) za vsak postopek z velikim ali kritičnim učinkom na ravni Unije oceno tveganja ogroženosti zaupnosti, celovitosti in razpoložljivosti informacij ter ustreznih sredstev. Ocena tega tveganja se poda v skladu z matriko učinka tveganja iz člena 19(2);

(3) seznam izvajalcev kritičnih IKT storitev za njihove postopke s kritičnim učinkom.

POGLAVJE III

SKUPNI OKVIR ZA KIBERNETSKO VARNOST ELEKTROENERGETSKEGA SISTEMA

Člen 28

Sestava, delovanje in pregled skupnega okvira za kibernetsko varnost elektroenergetskega sistema

1. Skupni okvir za kibernetsko varnost elektroenergetskega sistema vključuje naslednje kontrole in sistem upravljanja kibernetske varnosti:

(a) minimalne kontrole kibernetske varnosti, razvite v skladu s členom 29;

(b) razširjene kontrole kibernetske varnosti, razvite v skladu s členom 29;

(c) matriko za kartiranje, razvito v skladu s členom 34, v kateri so kartirane kontrole iz točk (a) in (b) glede na izbrane evropske in mednarodne standarde, nacionalno zakonodajo ali regulativne okvire;

(d) sistem upravljanja kibernetske varnosti, vzpostavljen na podlagi člena 32.

2. Vsi subjekti z velikim učinkom v svojem območju z velikim učinkom uporabijo minimalne kontrole kibernetske varnosti na podlagi odstavka 1, točka (a).

3. Vsi subjekti s kritičnim učinkom v svojem območju s kritičnim učinkom uporabijo razširjene kontrole kibernetske varnosti na podlagi odstavka 1, točka (b).

4. Skupni okvir za kibernetsko varnost elektroenergetskega sistema iz odstavka 1 se v sedmih mesecih po predložitvi prvega osnutka poročila o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(4) dopolni z minimalnimi in razširjenimi kontrolami kibernetske varnosti v dobavni verigi, razvitimi na podlagi člena 33.

Člen 29

Minimalne in razširjene kontrole kibernetske varnosti

1. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS v sedmih mesecih po predložitvi prvega osnutka poročila o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(4) pripravijo predlog minimalnih in razširjenih kontrol kibernetske varnosti.

2. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS v šestih mesecih po pripravi vsakega regionalnega poročila o oceni tveganja za kibernetsko varnost na podlagi člena 21(2) predlagajo pristojnemu organu spremembo minimalnih in razširjenih kontrol kibernetske varnosti. Predlog se opravi v skladu s členom 8(10) in upošteva tveganja, opredeljena v regionalni oceni tveganja.

3. Minimalne in razširjene kontrole kibernetske varnosti je mogoče preveriti s sodelovanjem v nacionalnem sistemu za preverjanje v skladu s postopkom iz člena 31 ali prek neodvisne varnostne revizije, ki jo opravi tretja stran in ki se izvede v skladu z zahtevami iz člena 25(2).

4. Začetne minimalne in razširjene kontrole kibernetske varnosti, razvite v skladu z odstavkom 1, temeljijo na tveganjih, ki so opredeljena v poročilu o oceni tveganja za kibernetsko varnosti na ravni Unije iz člena 19(5). Spremenjene minimalne in razširjene kontrole kibernetske varnosti, razvite v skladu z odstavkom 2, temeljijo na regionalnem poročilu o oceni tveganja za kibernetsko varnost iz člena 21(2).

5. Minimalne kontrole kibernetske varnosti vključujejo kontrole za varstvo izmenjanih informacij na podlagi člena 46.

6. Subjekti iz člena 2(1), ki so opredeljeni kot subjekti z velikim ali kritičnim učinkom na podlagi člena 24, v 12 mesecih po odobritvi minimalnih in razširjenih kontrol kibernetske varnosti na podlagi člena 8(5) ali po vsaki posodobitvi na podlagi člena 8(10) med pripravo načrta za zmanjšanje tveganja na ravni subjekta na podlagi člena 26(5) uporabijo minimalne kontrole kibernetske varnosti na območju z velikim učinkom in razširjene kontrole kibernetske varnosti na območju s kritičnim učinkom.

Člen 30

Odstopanja od minimalnih in razširjenih kontrol kibernetske varnosti

1. Subjekti iz člena 2(1) lahko zaprosijo ustrezni pristojni organ za odobritev odstopanja od obveznosti uporabe minimalnih in razširjenih kontrol kibernetske varnosti iz člena 29(6). Pristojni organ lahko odobri tako odstopanje pod naslednjimi pogoji:

(a) v izjemnih primerih kadar subjekt lahko dokaže, da stroški izvajanja ustreznih kontrol kibernetske varnosti znatno presegajo koristi. ACER, ENTSO za električno energijo in telo EU ODS lahko skupaj v okviru sodelovanja pripravijo smernice za oceno stroškov kontrol kibernetske varnosti, da bi pomagali subjektom;

(b) kadar subjekt predloži načrt za obravnavanje tveganja na ravni subjekta, ki prispeva k zmanjšanju tveganja za kibernetsko varnost z uporabo alternativnih kontrol na ravni, ki je sprejemljiva v skladu z merili za sprejemanje tveganja iz člena 26(3), točka (b).

2. Vsak pristojni organ se v treh mesecih po prejemu prošnje iz odstavka 1 odloči, ali bo odobril odstopanje od minimalnih in razširjenih kontrol kibernetske varnosti. Odstopanja od minimalnih ali razširjenih kontrol kibernetske varnosti se odobrijo za največ tri leta z možnostjo podaljšanja.

3. Informacije v zbirni in anonimizirani obliki o odobrenih odstopanjih se vključijo kot priloga k celovitemu poročilu o oceni tveganja za kibernetsko varnost čezmejnih pretokov električne energije iz člena 23. ENTSO za električno energijo in telo EU ODS skupaj po potrebi posodabljata seznam.

Člen 31

Preverjanje skupnega okvira za kibernetsko varnost elektroenergetskega sistema

1. Vsak subjekt s kritičnim učinkom, opredeljen v skladu s členom 24(1), lahko na zahtevo pristojnega organa najpozneje v 24 mesecih po sprejetju kontrol iz člena 28(1), točke (a), (b) in (c), ter vzpostavitvi sistema upravljanja kibernetske varnosti iz točke (d) navedenega člena, dokaže svojo skladnost s sistemom upravljanja kibernetske varnosti ter minimalnimi in razširjenimi kontrolami kibernetske varnosti.

2. Vsak subjekt s kritičnim učinkom izpolnjuje obveznosti iz odstavka 1 z izvedenimi neodvisnimi varnostnimi revizijami, ki jih opravi tretja stran in ki se izvedejo v skladu z zahtevami iz člena 25(2), ali s sodelovanjem v nacionalnem sistemu za preverjanje v skladu s členom 25(1).

3. Preverjanje, ali je subjekt s kritičnim učinkom skladen s sistemom upravljanja kibernetske varnosti in minimalnimi ali razširjenimi kontrolami kibernetske varnosti, zajema vsa sredstva na območju s kritičnim učinkom subjekta s kritičnim učinkom.

4. Preverjanje, ali je subjekt s kritičnim učinkom skladen s sistemom upravljanja kibernetske varnosti in minimalnimi ali razširjenimi kontrolami kibernetske varnosti, se redno ponovi najpozneje 36 mesecev po koncu prvega preverjanja in nato vsaka tri leta.

5. Vsak subjekt s kritičnim učinkom, opredeljen v skladu s členom 24, dokaže svojo skladnost s kontrolami iz člena 28(1), točke (a), (b) in (c) in vzpostavljenim sistemom upravljanja kibernetske varnosti iz točke (d) navedenega člena tako, da pristojnemu organu poroča o rezultatih preverjanja skladnosti.

Člen 32

Sistem upravljanja kibernetske varnosti

1. Vsak subjekt z velikim ali kritičnim učinkom v 24 mesecih po tem, ko ga pristojni organ uradno obvesti, da je bil opredeljen kot subjekt z velikim ali kritičnim učinkom v skladu s členom 24(6), vzpostavi sistem upravljanja kibernetske varnosti in ga nato vsaka tri leta pregleda, da:

(a) določi področje uporabe sistema upravljanja kibernetske varnosti ob upoštevanju vmesnikov in odvisnosti z drugimi subjekti;

(b) zagotovi, da je celotno višje vodstvo obveščeno o ustreznih pravnih obveznostih ter da s pravočasnimi odločitvami in hitrimi odzivi dejavno prispeva k izvajanju sistema upravljanja kibernetske varnosti;

(c) zagotovi razpoložljivost virov, potrebnih za sistem upravljanja kibernetske varnosti;

(d) vzpostavi politiko kibernetske varnosti, ki se dokumentira in o kateri so obveščeni vsi znotraj subjekta in strani, ki so izpostavljene varnostnim tveganjem;

(e) dodeli odgovornosti za naloge, ki so pomembne za kibernetsko varnost, in o njih obvešča;

(f) izvaja obvladovanje tveganja za kibernetsko varnost na ravni subjekta, kot je opredeljeno v členu 26;

(g) določi in zagotovi vire, potrebne za izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja kibernetske varnosti ob upoštevanju potrebne usposobljenosti in ozaveščenosti na področju virov za kibernetsko varnost;

(h) določi notranje in zunanje obveščanje, ki je pomembno za kibernetsko varnost;

(i) pripravlja, posodablja in nadzoruje dokumentirane informacije, povezane s sistemom upravljanja kibernetske varnosti;

(j) ocenjuje uspešnost in učinkovitost sistema upravljanja kibernetske varnosti;

(k) izvaja notranje revizije v načrtovanih časovnih presledkih, da zagotovi učinkovito izvajanje in vzdrževanje sistema upravljanja kibernetske varnosti;

(l) v načrtovanih časovnih presledkih pregleduje izvajanje sistema upravljanja kibernetske varnosti ter nadzoruje in odpravlja neskladnost virov in dejavnosti s politikami, postopki in smernicami v okviru sistema upravljanja kibernetske varnosti.

2. Področje uporabe sistema upravljanja kibernetske varnosti vključuje vsa sredstva na območju z velikim ali kritičnim učinkom subjekta z velikim ali kritičnim učinkom.

3. Pristojni organi spodbujajo uporabo evropskih ali mednarodnih standardov in specifikacij, povezanih s sistemi za upravljanje in pomembnih za varnost omrežnih in informacijskih sistemov, ne da bi predpisali uporabo določene vrste tehnologije ali ji dajale prednost.

Člen 33

Minimalne in razširjene kontrole kibernetske varnosti v dobavni verigi

1. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS v sedmih mesecih po predložitvi prvega osnutka poročila o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(4) pripravijo predlog minimalnih in razširjenih kontrol kibernetske varnosti v dobavni verigi, ki zmanjšujejo tveganja za dobavno verigo, opredeljena v ocenah tveganja za kibernetsko varnost na ravni Unije, pri čemer dopolnijo minimalne in razširjene kontrole kibernetske varnosti, razvite na podlagi člena 29. Minimalne in razširjene kontrole kibernetske varnosti v dobavni verigi se razvijejo skupaj z minimalnimi in razširjenimi kontrolami na podlagi člena 29. Minimalne in razširjene kontrole kibernetske varnosti v dobavni verigi zajemajo celoten življenjski cikel vseh proizvodov IKT, storitev IKT in postopkov IKT znotraj območja z velikim ali kritičnim učinkom subjekta z velikim ali kritičnim učinkom. Pri pripravi predloga minimalnih in razširjenih kontrol kibernetske varnosti v dobavni verigi se je treba posvetovati s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov.

2. Minimalne kontrole kibernetske varnosti v dobavni verigi vključujejo kontrole za subjekte z velikim ali kritičnim učinkom, ki:

(a) vključujejo priporočila za javno naročanje proizvodov IKT, storitev IKT in postopkov IKT, ki se nanašajo na specifikacije kibernetske varnosti in zajemajo vsaj:

(i) preverjanja preteklosti osebja dobavitelja, ki je vključen v dobavno verigo in ravna z občutljivimi informacijami ali ima dostop do sredstev z velikim ali kritičnim učinkom, ki so v lasti subjekta; Preverjanje preteklosti lahko vključuje preverjanje identitete in preteklosti osebja ali zunanjih izvajalcev subjekta v skladu z nacionalnim pravom in postopki ter ustreznim in veljavnim pravom Unije, vključno z Uredbo (EU) 2016/679 in Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta ([18]). Preverjanja preteklosti so sorazmerna in strogo omejena na to, kar je potrebno. Opravijo se izključno za namene vrednotenja morebitnega varnostnega tveganja za zadevni subjekt. Biti morajo sorazmerna s poslovnimi zahtevami, razvrstitvijo informacij, do katerih je potreben dostop, in zaznanimi tveganji, opravi pa jih sam subjekt, zunanje podjetje, ki izvaja preverjanje, ali vlada;

(ii) postopke za varno in nadzorovano načrtovanje, razvoj in proizvodnjo proizvodov IKT, storitev IKT in postopkov IKT, ki spodbujajo načrtovanje in razvoj takih proizvodov, storitev in postopkov in vključujejo ustrezne tehnične ukrepe za zagotavljanje kibernetske varnosti;

(iii) zasnovo omrežnih in informacijskih sistemov, v katerih se napravam ne zaupa, tudi če so znotraj varnega območja, ki zahtevajo preverjanje vseh prejetih zahtev in uporabljajo načelo najmanjšega privilegija;

(iv) dostop dobavitelja do sredstev subjekta;

([18]) Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

(v) pogodbene obveznosti dobavitelja glede zaščite in omejitve dostopa do občutljivih informacij subjekta;

(vi) osnovne specifikacije za javno naročanje na področju kibernetske varnosti za podizvajalce dobavitelja;

(vii) sledljivost uporabe specifikacij kibernetske varnosti od razvoja prek proizvodnje do dobave proizvodov IKT, storitev IKT ali postopkov IKT;

(viii) podporo varnostnim posodobitvam v celotni življenjski dobi proizvodov IKT, storitev IKT ali postopkov IKT;

(ix) pravico do revizije kibernetske varnosti v postopkih načrtovanja, razvoja in proizvodnje dobavitelja ter

(x) oceno profila tveganja dobavitelja;

(b) zahtevajo, da taki subjekti pri sklepanju pogodb z dobavitelji, partnerji v sodelovanju in drugimi stranmi v dobavni verigi upoštevajo priporočila za javno naročanje iz pododstavka (a), ki zajemajo običajne dobave proizvodov IKT, storitev IKT in postopkov IKT ter neželene dogodke in okoliščine, kot so prenehanje in prenos pogodb v primerih malomarnosti pogodbenega partnerja;

(c) zahtevajo, da taki subjekti upoštevajo rezultate ustreznih usklajenih ocen tveganja za varnost kritičnih dobavnih verig, ki se opravijo v skladu s členom 22(1) Direktive (EU) 2022/2555;

(d) vključujejo merila za izbiro dobaviteljev in sklepanje pogodb z dobavitelji, ki lahko izpolnjujejo specifikacije kibernetske varnosti iz točke (a) in imajo raven kibernetske varnosti, ki ustreza tveganjem za kibernetsko varnost proizvoda IKT, storitve IKT ali postopkov IKT, ki jih dobavitelj dobavlja;

(e) vključujejo merila za diverzifikacijo virov dobave proizvodov IKT, storitev IKT in postopkov IKT ter zmanjšanje tveganja vezanosti na enega prodajalca;

(f) vključujejo merila za redno spremljanje, pregledovanje ali revizijo specifikacij kibernetske varnosti za notranje operativne postopke dobavitelja v celotnem življenjskem ciklu vsakega proizvoda IKT, storitve IKT in postopka IKT.

3. Subjekti z velikim ali kritičnim učinkom za specifikacije kibernetske varnosti v priporočilu za javno naročanje na področju kibernetske varnosti iz odstavka 2, točka (a), uporabijo načela javnega naročanja iz Direktive 2014/24/EU Evropskega parlamenta in Sveta ([19]) v skladu s členom 35(4) ali opredelijo svoje specifikacije na podlagi rezultatov ocene tveganja za kibernetsko varnost na ravni subjekta.

4. Razširjene kontrole kibernetske varnosti v dobavni verigi vključujejo kontrole, ki jih izvajajo subjekti s kritičnim učinkom, da bi v okviru javnega naročanja preverili, ali proizvodi IKT, storitve IKT in postopki IKT, ki se bodo uporabljali kot sredstva s kritičnim učinkom, izpolnjujejo specifikacije kibernetske varnosti. Proizvod IKT, storitev IKT ali postopek IKT se preveri v okviru evropske certifikacijske sheme za kibernetsko varnost iz člena 31 ali dejavnosti preverjanja, ki jih izbere in organizira subjekt. Poglobljenost in obseg dejavnosti preverjanja sta zadostna za zagotovitev, da se proizvod IKT, storitev IKT ali postopek IKT lahko uporablja za zmanjševanje tveganj, opredeljenih v oceni tveganja na ravni subjekta. Subjekt s kritičnim učinkom dokumentira ukrepe, sprejete za zmanjšanje opredeljenih tveganj.

5. Minimalne in razširjene kontrole kibernetske varnosti v dobavni verigi se uporabljajo za javno naročanje ustreznih proizvodov IKT, storitev IKT in postopkov IKT Minimalne in razširjene kontrole kibernetske varnosti v dobavni verigi se uporabljajo za javno naročanje pri subjektih, opredeljenih kot subjekti s kritičnim ali velikim učinkom v skladu s členom 24, ki se začne šest mesecev po sprejetju ali posodobitvi minimalnih in razširjenih kontrol kibernetske varnosti iz člena 29.

([19]) Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

6. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS v šestih mesecih po pripravi vsakega regionalnega poročila o oceni tveganja za kibernetsko varnost na podlagi člena 21(2) predlagajo pristojnemu organu spremembo minimalnih in razširjenih kontrol kibernetske varnosti v dobavni verigi. Predlog se opravi v skladu s členom 8(10) in upošteva tveganja, opredeljena v regionalni oceni tveganja.

Člen 34

Matrika za kartiranje kontrol kibernetske varnosti v sektorju električne energije glede na standarde

1. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo, v sodelovanju s telesom EU ODS in ob posvetovanju z ENISA v sedmih mesecih po predložitvi prvega osnutka poročila o oceni tveganja za kibernetsko varnost na ravni Unije na podlagi člena 19(4) pripravijo predlog matrike za kartiranje kontrol iz člena 28(1), točki (a) in (b), glede na izbrane evropske in mednarodne standarde ter ustrezne tehnične specifikacije (v nadaljnjem besedilu: matrika za kartiranje). ENTSO za električno energijo in telo EU ODS dokumentirata enakovrednost različnih kontrol s kontrolami iz člena 28(1), točki (a) in (b).

2. Pristojni organi lahko predložijo ENTSO za električno energijo in telesu EU ODS tako kartirane kontrole iz člena 28(1), točki (a) in (b), s sklicem na ustrezne nacionalne zakonodajne ali regulativne okvire, vključno z ustreznimi nacionalnimi standardi držav članic iz člena 25 Direktive (EU) 2022/2555. Če pristojni organ države članice zagotovi tako kartiranje, ENTSO za električno energijo in telo EU ODS vključita to nacionalno kartiranje v matriko za kartiranje.

3. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo, v sodelovanju s telesom EU ODS in ob posvetovanju z ENISA v šestih mesecih po pripravi vsakega regionalnega poročila o oceni tveganja za kibernetsko varnost na podlagi člena 21(2) predlagajo pristojnemu organu spremembo matrike za kartiranje. Predlog se opravi v skladu s členom 8(10) in upošteva tveganja, opredeljena v regionalni oceni tveganja.

POGLAVJE IV

PRIPOROČILA ZA JAVNO NAROČANJE NA PODROČJU KIBERNETSKE VARNOSTI

Člen 35

Priporočila za javno naročanje na področju kibernetske varnosti

1. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS v okviru delovnega programa, ki se določi in posodablja ob vsakem sprejetju regionalnega poročila o oceni tveganja za kibernetsko varnost, pripravijo sklope nezavezujočih priporočil za javno naročanje na področju kibernetske varnosti, ki jih subjekti z velikim ali kritičnim učinkom lahko uporabijo kot podlago pri javnem naročanju proizvodov IKT, storitev IKT in postopkov IKT na območju z velikim ali kritičnim učinkom. Ta delovni program vključuje:

(a) opis in razvrstitev vrst proizvodov IKT, storitev IKT in postopkov IKT, ki ju uporabijo subjekti z velikim ali kritičnim učinkom na območju z velikim ali kritičnim učinkom;

(b) seznam vrst proizvodov IKT, storitev IKT in postopkov IKT, za katere se razvije sklop nezavezujočih priporočil v zvezi s kibernetsko varnostjo na podlagi ustreznih regionalnih poročil o oceni tveganja za kibernetsko varnost ter prednostnih nalog subjektov z velikim ali kritičnim učinkom.

2. ENTSO za električno energijo v sodelovanju s telesom EU ODS v šestih mesecih po sprejetju ali posodobitvi regionalnega poročila o oceni tveganja za kibernetsko varnost zagotovi ACER povzetek navedenega delovnega programa.

3. Operaterji prenosnih sistemov si ob pomoči ENTSO za električno energijo in v sodelovanju s subjektom EU ODS prizadevajo za zagotovitev, da so nezavezujoča priporočila za javno naročanje na področju kibernetske varnosti, pripravljena na podlagi ustreznega regionalnega poročila o oceni tveganja za kibernetsko varnost, podobna ali primerljiva v vseh regijah obratovanja sistema. Sklopi priporočil za javno naročanje na področju kibernetske varnosti vključujejo vsaj specifikacije iz člena 33(2), točka (a). Specifikacije se, kadar je mogoče, izberejo iz evropskih in mednarodnih standardov.

4. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s subjektom EU ODS zagotovijo, da so priporočila za javno naročanje na področju kibernetske varnosti:

(a) skladna z načeli javnega naročanja na podlagi Direktive 2014/24/EU in

(b) združljiva z najnovejšimi razpoložljivimi evropskimi certifikacijskimi shemami za kibernetsko varnost, ki se nanašajo na proizvod IKT, storitev IKT ali postopek IKT, ter da take sheme upoštevajo.

Člen 36

Navodila za uporabo evropskih certifikacijskih shem za kibernetsko varnost pri javnem naročanju proizvodov IKT, storitev IKT in postopkov IKT

1. Nezavezujoča priporočila za javno naročanje na področju kibernetske varnosti, pripravljena na podlagi člena 35, lahko vključujejo sektorska navodila za uporabo evropskih certifikacijskih shem za kibernetsko varnost, kadar koli je ustrezna shema na voljo za vrsto proizvoda IKT, storitve IKT ali postopka IKT, ki ga uporabljajo subjekti s kritičnim učinkom, brez poseganja v okvir vzpostavitve evropskih certifikacijskih shem za kibernetsko varnosti na podlagi člena 46 Uredbe (EU) 2019/881.

2. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS tesno sodelujejo z ENISA pri zagotavljanju sektorskih navodil, vključenih v nezavezujoča priporočila za javno naročanje na področju kibernetske varnosti iz odstavka 1.

POGLAVJE V

TOKOVI INFORMACIJ, KIBERNETSKI NAPADI IN OBVLADOVANJE KRIZ

Člen 37

Pravila o izmenjavi informacij

1. Pristojni organ ob prejemu informacij o kibernetskem napadu, o katerem se poroča:

(a) oceni stopnjo zaupnosti teh informacij in brez nepotrebnega odlašanja, najpozneje pa v 24 urah po prejemu informacij, obvesti subjekt o rezultatu svoje ocene;

(b) poskuša odkriti katere koli druge podobne kibernetske napade v Uniji, o katerih se je poročalo drugim pristojnim organom, da bi informacije, prejete v zvezi s kibernetskim napadom, o katerem se poroča, primerjal z informacijami, predloženimi v zvezi z drugimi kibernetskimi napadi, obogatil obstoječe informacije ter okrepil in uskladil odzive na področju kibernetske varnosti;

(c) je odgovoren za odstranitev poslovnih skrivnosti in anonimizacijo informacij v skladu z ustreznimi nacionalnimi pravili in pravili Unije;

(d) brez nepotrebnega odlašanja in najpozneje v 24 urah po prejemu informacij o kibernetskem napadu, o katerem se poroča, izmenja informacije z nacionalnim enotnimi kontaktnimi točkami, skupinami CSIRT in vsemi pristojnimi organi, imenovanimi v drugih državah članicah na podlagi člena 4, ter tem organom redno zagotavlja posodobljene informacije;

(e) informacije o kibernetskem napadu po anonimizaciji in odstranitvi poslovnih skrivnosti v skladu z odstavkom 1, točka (c), brez nepotrebnega odlašanja in najpozneje v 24 urah po prejemu informacij v skladu z odstavkom 1, točka (a), posreduje subjektom s kritičnim ali velikim učinkom v svoji državi članici ter jim redno zagotavlja posodobljene informacije, da lahko učinkovito organizirajo svojo obrambo;

(f) lahko od subjekta z velikim ali kritičnim učinkom, ki poroča, zahteva, da informacije o kibernetskem napadu, o katerem se poroča, na varen način nadalje posreduje drugim subjektom, ki so lahko izpostavljeni, da se v sektorju električne energije poveča ozaveščenost o razmerah in prepreči uresničitev tveganja, ki bi se lahko stopnjevalo v čezmejni kibernetski incident v sektorju električne energije;

(g) po anonimizaciji in odstranitvi poslovnih skrivnosti posreduje ENISA zbirno poročilo z informacijami o kibernetskem napadu.

2. Skupina CSIRT ob seznanitvi z nepopravljeno aktivno izrabljeno ranljivostjo:

(a) o tem prek ustreznega varnega kanala za izmenjavo informacij nemudoma obvesti ENISA, razen če je v drugi zakonodaji Unije določeno drugače;

(b) pomaga zadevnemu subjektu, da si od proizvajalca ali ponudnika zagotovi učinkovito, usklajeno in hitro odpravo nepopravljene aktivno izrabljene ranljivosti ali učinkovite in uspešne ukrepe za blažitev;

(c) izmenja razpoložljive informacije s prodajalcem in po možnosti od proizvajalca ali ponudnika zahteva, da določi seznam skupin CSIRT v državah članicah, ki jih nepopravljena aktivno izrabljena ranljivost zadeva in ki jih je treba o tem obvestiti;

(d) na podlagi potrebe po seznanitvi izmenja razpoložljive informacije s skupinami CSIRT iz prejšnje točke;

(e) izmenja strategije in ukrepe za blažitev prijavljene nepopravljene aktivno izrabljene ranljivosti, kadar obstajajo.

3. Pristojni organ ob seznanitvi z nepopravljeno aktivno izrabljeno ranljivostjo:

(a) v usklajevanju s skupinami CSIRT in svojo državo članico izmenja strategije in ukrepe za blažitev prijavljene nepopravljene aktivno izrabljene ranljivosti, kadar obstajajo;

(b) izmenja informacije s skupino CSIRT v državi članici, v kateri je bila prijavljena nepopravljena aktivno izrabljena ranljivost.

4. Pristojni organ se ob seznanitvi z nepopravljeno ranljivostjo, za katero še ni dokazov, da bi bila aktivno izrabljena, brez nepotrebnega odlašanja uskladi s skupino CSIRT za namene usklajenega razkrivanja ranljivosti, kot je določeno v členu 12(1) Direktive (EU) 2022/2555.

5. Skupina CSIRT v primeru prejema informacij v zvezi s kibernetskimi grožnjami od enega ali več subjektov z velikim ali kritičnim učinkom na podlagi člena 38(6) te informacije ali vse druge informacije, ki so pomembne za preprečevanje ali, odkrivanje zadevnega tveganja, odzivanje nanj ali njegovo zmanjšanje, brez nepotrebnega odlašanja in najpozneje v štirih urah po prejemu informacij posreduje subjektom s kritičnim ali velikim učinkom v svoji državi članici ter po potrebi vsem zadevnim skupinam CSIRT in svoji nacionalni enotni kontaktni točki.

6. Pristojni organ ob seznanitvi z informacijami v zvezi s kibernetskimi grožnjami, ki jih prejme od enega ali več subjektov z velikim ali kritičnim učinkom, te informacije posreduje skupini CSIRT za namene odstavka 5.

7. Pristojni organi lahko odgovornosti iz odstavkov 3 in 4 v zvezi z enim ali več subjekti z velikim ali kritičnim učinkom, ki delujejo v več kot eni državi članici, v celoti ali delno prenesejo na drug pristojni organ v eni od teh držav članic na podlagi dogovora med zadevnimi pristojnimi organi.

8. Operaterji prenosnih sistemov ob pomoči ENTSO za električno energijo in v sodelovanju s telesom EU ODS do 13. junija 2025 oblikujejo metodologijo lestvice razvrščanja kibernetskih napadov. Operaterji prenosnih sistemov lahko ob pomoči ENTSO za električno energijo in telesa EU ODS od pristojnih organov zahtevajo, da se posvetujejo z ENISA in svojimi pristojnimi organi, odgovornimi za kibernetsko varnost, da bi si zagotovili pomoč pri oblikovanju take lestvice razvrščanja. Metodologija zagotavlja razvrstitev resnosti kibernetskega napada v skladu s petimi stopnjami, pri čemer sta dve najvišji stopnji „velika“ in „kritična“. Razvrstitev temelji na oceni naslednjih parametrov:

(a) potencialnega učinka ob upoštevanju izpostavljenih sredstev in območij, določenih v skladu s členom 26(4), točka (c), ter

(b) resnosti kibernetskega napada.

9. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 13. junija 2026 izvede študijo izvedljivosti za oceno možnosti in finančnih stroškov, potrebnih za razvoj skupnega orodja, ki vsem subjektom omogoča izmenjavo informacij z ustreznimi nacionalnimi organi.

10. Študija izvedljivosti obravnava možnost, da tako skupno orodje:

(a) zagotovi podporo subjektom s kritičnim ali velikim učinkom z ustreznimi varnostnimi informacijami za delovanje čezmejnih pretokov električne energije, kot so poročanje o kibernetskih napadih v skoraj realnem času, zgodnja opozorila v zvezi z zadevami kibernetske varnosti in nerazkrite ranljivosti opreme, ki se uporablja v elektroenergetskem sistemu;

(b) ostane v primernem in zelo zanesljivem okolju;

(c) omogoča zbiranje podatkov od subjektov s kritičnim ali velikim učinkom ter olajša odstranitev zaupnih informacij in anonimizacijo podatkov ter njihovo takojšnje posredovanje razširjanje subjektom s kritičnim ali velikim učinkom.

11. ENTSO za električno energijo v sodelovanju s telesom EU ODS:

(a) se pri ocenjevanju izvedljivosti posvetuje z ENISA in Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, nacionalnimi enotnimi kontaktnimi točkami in predstavniki glavnih deležnikov;

(b) rezultate študije izvedljivosti predstavi ACER in Skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov.

12. ENTSO za električno energijo lahko v sodelovanju s telesom EU ODS analizira in spodbuja pobude, ki jih predlagajo subjekti s kritičnim ali velikim učinkom, da bi se ocenila in preskusila taka orodja za izmenjavo informacij.

Člen 38

Vloga subjektov z velikim ali kritičnim učinkom pri izmenjavi informacij

1. Vsak subjekt z velikim ali kritičnim učinkom:

(a) za vsa sredstva v svojem območju kibernetske varnosti, določenem na podlagi člena 26(4), točka (c), vzpostavi vsaj zmogljivosti centra za operacije na področju kibernetske varnosti, da bi:

  (i) zagotovil, da se v ustreznih omrežnih in informacijskih sistemih ter aplikacijah ustvarjajo varnostni dnevniki za spremljanje varnosti, kar omogoča odkrivanje anomalij in zbiranje informacij o kibernetskih napadih;

  (ii) izvedel spremljanje varnosti, vključno z odkrivanjem vdorov in ocenjevanjem ranljivosti omrežnih in informacijskih sistemov;

  (iii) analiziral in po potrebi sprejel vse potrebne ukrepe v okviru svoje odgovornosti in zmogljivosti za zaščito subjekta;

  (iv) sodeloval pri zbiranju in izmenjavi informacij iz tega člena;

(b) ima pravico, da vse ali del teh zmogljivosti na podlagi točke (a) priskrbi prek ponudnikov upravljanih varnostnih storitev. Subjekti s kritičnim ali velikim učinkom so še naprej odgovorni za ponudnike upravljanih varnostnih storitev in nadzirajo njihovo delo;

(c) določi enotno kontaktno točko na ravni subjekta za izmenjavo informacij.

2. ENISA lahko v okviru naloge iz člena 6(2) Uredbe (EU) 2019/881 izda nezavezujoče smernice o vzpostavitvi takih zmogljivosti ali oddaji storitve v podizvajanje ponudnikom upravljanih varnostnih storitev.

3. Vsak subjekt s kritičnim ali velikim učinkom brez nepotrebnega odlašanja in najpozneje v štirih urah po seznanitvi, da se o incidentu poroča, izmenja s svojimi skupinami CSIRT in pristojnim organom ustrezne informacije v zvezi s kibernetskim napadom, o katerem se poroča.

4. Šteje se, da se o informacijah, povezanih s kibernetskim napadom, poroča, če izpostavljeni subjekt oceni, da ta napad v skladu z metodologijo lestvice razvrščanja kibernetskih napadov na podlagi člena 37(8) z vidika kritičnosti sega od stopnje „velika“ do stopnje „kritična“. Enotna kontaktna točka na ravni subjekta, določena v skladu z odstavkom 1, točka (c), sporoči razvrstitev incidenta.

5. Kadar subjekti s kritičnim ali velikim učinkom skupini CSIRT priglasijo ustrezne informacije v zvezi z nepopravljenimi aktivno izrabljenimi ranljivostmi, lahko skupina CSIRT te informacije posreduje svojemu pristojnemu organu. Skupina CSIRT lahko glede na stopnjo občutljivosti priglašenih informacij na podlagi utemeljenih razlogov, povezanih s kibernetsko varnostjo, zadrži informacije ali odloži njihovo posredovanje.

6. Vsak subjekt s kritičnim ali velikim učinkom svojim skupinam CSIRT brez nepotrebnega odlašanja posreduje vse informacije v zvezi s kibernetsko grožnjo, o kateri se poroča in ki ima lahko čezmejni učinek. Šteje se, da se o informacijah, povezanih s kibernetsko grožnjo, poroča, če je izpolnjen vsaj eden od naslednjih pogojev:

(a) drugim subjektom s kritičnim ali velikim učinkom se s tem zagotovijo pomembne informacije za preprečevanje ali odkrivanje učinka tveganja, odzivanje nanj ali njegovo zmanjšanje;

(b) opredeljene tehnike, taktike in postopki, uporabljeni v okviru napada, vodijo do informacij, kot so ogroženi naslovi URL ali IP, zgoščene vrednosti ali kateri koli drug atribut, uporaben za kontekstualizacijo in korelacijo napada;

(c) kibernetska grožnja se lahko nadalje oceni in kontekstualizira z dodatnimi informacijami, ki jih zagotovijo izvajalci storitev ali tretje strani, za katere ta uredba ne velja.

7. Vsak subjekt s kritičnim ali velikim učinkom pri izmenjavi informacij v skladu s tem členom navede:

(a) da so informacije predložene v skladu s to uredbo;

(b) ali se informacije nanašajo na:

(i) kibernetski napad iz odstavka 3, o katerem se poroča;

(ii) nepopravljene aktivno izrabljene ranljivosti iz odstavka 4, ki niso znane v javnosti;

(iii) kibernetsko grožnjo iz odstavka 5, o kateri se poroča;

(c) v primeru kibernetskega napada, o katerem se poroča, stopnjo kibernetskega napada v skladu z metodologijo lestvice razvrščanja kibernetskih napadov iz člena 37(8) in informacijami, na podlagi katerih je bila ta razvrstitev opravljena, vključno vsaj s kritičnostjo kibernetskega napada.

8. Kadar subjekt s kritičnim ali velikim učinkom priglasi pomemben incident v skladu s členom 23 Direktive (EU) 2022/2555 in kadar poročanje o incidentu v skladu z navedenim členom vključuje ustrezne informacije, kot se zahtevajo v skladu z odstavkom 3 tega člena, poročanje, ki ga opravi subjekt v skladu s členom 23(1) navedene direktive, pomeni poročanje o informacijah v skladu z odstavkom 3 tega člena.

9. Vsak subjekt s kritičnim ali velikim učinkom poroča svojemu pristojnemu organu ali skupini CSIRT tako, da jasno opredeli posebne informacije, ki se izmenjujejo s pristojnim organom ali skupino CSIRT samo v primerih, ko bi bila izmenjava informacij lahko vir kibernetskega napada. Vsak subjekt s kritičnim ali velikim učinkom ima pravico, da pristojnemu organu ali skupini CSIRT zagotovi nezaupno različico informacij.

Člen 39

Odkrivanje kibernetskih napadov in ravnanje s povezanimi informacijami

1. Subjekti s kritičnim ali velikim učinkom razvijejo potrebne zmogljivosti za obvladovanje odkritih kibernetskih napadov ob potrebni podpori ustreznega pristojnega organa, ENTSO za električno energijo in telesa EU ODS. Subjekte s kritičnim ali velikim učinkom lahko podpira skupina CSIRT, imenovana v zadevni državi članici, v okviru naloge, ki je skupinam CSIRT dodeljena na podlagi člena 11(5), točka (a), Direktive (EU) 2022/2555. Subjekti s kritičnim ali velikim učinkom izvajajo učinkovite postopke za opredelitev in razvrščanje kibernetskih napadov ter odzivanje na kibernetske napade, ki bodo ali bi lahko vplivali na čezmejne pretoke električne energije, da se čim bolj zmanjša njihov učinek.

2. Če ima kibernetski napad učinek na čezmejne pretoke električne energije, enotne kontaktne točke izpostavljenih subjektov s kritičnim ali velikim učinkom na ravni subjekta sodelujejo pri izmenjavi informacij med njimi, ki jo usklajuje pristojni organ države članice, v kateri se je prvič poročalo o kibernetskem napadu.

3. Subjekti s kritičnim ali velikim učinkom:

(a) zagotovijo, da ima njihova enotna kontaktna točka na ravni subjekta dostop do informacij, ki jih je prejela od nacionalne enotne kontaktne točke prek svojega pristojnega organa na podlagi potrebe po seznanitvi;

(b) če tega niso storili že v skladu s členom 3(4) Direktive (EU) 2022/2555, obvestijo pristojni organ države članice, v kateri imajo sedež, in nacionalno enotno kontaktno točko o seznamu svojih enotnih kontaktnih točk za kibernetsko varnost na ravni subjekta:

   (i) od katerih lahko pristojni organ in nacionalna enotna kontaktna točka pričakujeta, da bosta prejela informacije o kibernetskih napadih, o katerih se poroča;

   (ii) ki jim bodo morali pristojni organi in nacionalne enotne kontaktne točke posredovati informacije;

(c) vzpostavijo postopke za obvladovanje kibernetskih napadov, vključno z vlogami in odgovornostmi, nalogami ter odzivi, ki temeljijo na opazovanem razvoju kibernetskega napada znotraj območij s kritičnim ali velikim učinkom;

(d) vsaj vsako leto preskusijo celovite postopke za obvladovanje kibernetskih napadov, tako da preskusijo vsaj en scenarij, ki neposredno ali posredno vpliva na čezmejne pretoke električne energije. Subjekti s kritičnim ali velikim učinkom lahko ta letni preskus izvedejo med rednimi vajami iz člena 43. Kakršna koli dejavnost odziva na kibernetski napad v živo, pri čemer se posledice tega napada v skladu z metodologijo lestvice razvrščanja kibernetskih napadov iz člena 37(8) razvrstijo vsaj v stopnjo 2 in katerega temeljni vzroki so povezani s kibernetsko varnostjo, se lahko uporabi kot letni preskus načrta odziva na kibernetski napad.

4. Države članice lahko naloge iz odstavka 1 prenesejo tudi na regionalne koordinacijske centre v skladu s členom 37(2) Uredbe (EU) 2019/943.

Člen 40

Obvladovanje kriz

1. Kadar pristojni organ ugotovi, da je kriza pri oskrbi z električno energijo povezana s kibernetskim napadom, ki ima učinek na več kot eno državo članico, pristojni organi iz izpostavljenih držav članic, nacionalni pristojni organi, odgovorni za kibernetsko varnost, nacionalni pristojni organi za pripravljenost na tveganja in organi za obvladovanje kibernetskih kriz v omrežnih in informacijskih sistemih iz izpostavljenih držav članic skupaj ustanovijo *ad hoc* skupino za čezmejno krizno usklajevanje.

2. *Ad hoc* skupina za čezmejno krizno usklajevanje:

(a) usklajuje učinkovito pridobivanje in nadaljnje razširjanje vseh ustreznih informacij o kibernetski varnosti subjektom, vključenim v postopek obvladovanja kriz;

(b) organizira komunikacijo med vsemi subjekti, na katere je vplivala kriza, in pristojnimi organi, da bi se zmanjšala prekrivanja ter povečala učinkovitost analiz in tehničnih odzivov za odpravo sočasnih kriz pri oskrbi z električno energijo, katerih temeljni vzroki so povezani s kibernetsko varnostjo;

(c) v sodelovanju s pristojnimi skupinami CSIRT subjektom, na katere je incident vplival, zagotovi potrebno strokovno znanje, vključno z operativnim svetovanjem o izvajanju morebitnih blažilnih ukrepov;

(d) Komisijo in usklajevalno skupino za električno energijo obvešča ter jima zagotavlja redne posodobljene informacije o stanju incidenta v skladu z načeli o varstvu iz člena 46;

(e) pridobiva nasvete od ustreznih organov, agencij ali subjektov, ki bi lahko pomagali zmanjšati krizo pri oskrbi z električno energijo.

3. Kadar kibernetski napad izpolnjuje pogoje za kibernetski incident velikih razsežnosti ali se pričakuje, da jih bo izpolnjeval, *ad hoc* skupina za čezmejno krizno usklajevanje o tem nemudoma obvesti nacionalne organe za obvladovanje kibernetskih kriz v skladu s členom 9(1) Direktive (EU) 2022/2555 v državah članicah, na katere je incident vplival, ter Komisijo in mrežo EU-CyCLONe. V takem primeru *ad hoc* skupina za čezmejno krizno usklajevanje podpira mrežo EU-CyCLONe v zvezi s sektorskimi posebnostmi.

4. Subjekti s kritičnim ali velikim učinkom razvijejo in imajo na voljo zmogljivosti, notranje smernice, načrte pripravljenosti in osebje za sodelovanje pri odkrivanju in zmanjševanju čezmejnih kriz. Subjekt s kritičnim ali velikim učinkom, na katerega vpliva sočasna kriza pri oskrbi z električno energijo, v sodelovanju s svojim pristojnim organom razišče temeljni vzrok take krize, da ugotovi, v kolikšni meri je ta povezana s kibernetskim napadom.

5. Države članice lahko naloge iz odstavka 4 prenesejo tudi na regionalne koordinacijske centre v skladu s členom 37(2) Uredbe (EU) 2019/943.

Člen 41

Načrti za obvladovanje kibernetskih kriz in odzivanje nanje

1. ACER v 24 mesecih po prejetem uradnem obvestilu o poročilu o oceni tveganja za celotno Unijo v tesnem sodelovanju z ENISA, ENTSO za električno energijo, telesom EU ODS, nacionalnimi pristojnimi organi, odgovornimi za kibernetsko varnost, pristojnimi organi, nacionalnimi pristojnimi organi za pripravljenost na tveganja, nacionalnimi regulativnimi organi in nacionalnimi organi za obvladovanje kibernetskih kriz v omrežnih in informacijskih sistemih pripravi za sektor električne energije načrt za obvladovanje kibernetskih kriz na ravni Unije in odzivanje nanje.

2. Vsak pristojni organ v 12 mesecih po tem, ko ACER v skladu z odstavkom 1 pripravi za sektor električne energije načrt za obvladovanje kibernetskih kriz na ravni Unije in odzivanje nanje, pripravi nacionalni načrt za obvladovanje kibernetskih kriz in odzivanje nanje za čezmejne pretoke električne energije, pri čemer upošteva načrt za obvladovanje kibernetskih kriz na ravni Unije in nacionalni načrt pripravljenosti na tveganja, pripravljen v skladu s členom 10 Uredbe (EU) 2019/941. Ta načrt je skladen z načrtom odzivanja na kibernetske incidente velikih razsežnosti in krize na podlagi člena 9(4) Direktive (EU) 2022/2555. Pristojni organ se usklajuje s subjekti s kritičnim ali velikim učinkom ter nacionalnimi pristojnimi organi za pripravljenost na tveganja v svoji državi članici.

3. Nacionalni načrt odzivanja na kibernetske incidente velikih razsežnosti in krize, ki se zahteva na podlagi člena 9(4) Direktive (EU) 2022/2555, se šteje za nacionalni načrt za obvladovanje kibernetske krize iz tega člena, če vključuje določbe o obvladovanju kriz in odzivanju nanje, ki se nanašajo na čezmejne pretoke električne energije.

4. Države članice lahko naloge iz odstavkov 1 in 2 prenesejo tudi na regionalne koordinacijske centre v skladu s členom 37(2) Uredbe (EU) 2019/943.

5. Subjekti s kritičnim ali velikim učinkom zagotovijo, da njihovi postopki obvladovanja kriz, povezani s kibernetsko varnostjo:

(a) uradno vključujejo združljive postopke obravnavanja čezmejnih kibernetskih incidentov, kot so opredeljeni v členu 6(8) Direktive (EU) 2022/2555, v njihove načrte za obvladovanje kriz;

(b) so del splošnih dejavnosti obvladovanja kriz.

6. Subjekti s kritičnim ali velikim učinkom v 12 mesecih po njihovi priglasitvi na podlagi člena 24(6) in nato vsaka tri leta pripravijo načrt za obvladovanje kriz na ravni subjekta, ki se nanaša na kibernetsko krizo in se vključi v njihove splošne načrte za obvladovanje kriz. Ta načrt vključuje vsaj naslednje:

(a) pravila o razglasitvi krize, določena v členu 14(2) in (3) Uredbe (EU) 2019/941;

(b) jasne vloge in odgovornosti za obvladovanje kriz, vključno z vlogo drugih ustreznih subjektov s kritičnim in velikim učinkom;

(c) posodobljene kontaktne informacije ter pravila za obveščanje in izmenjavo informacij v kriznih razmerah, vključno s povezavo s skupinami CSIRT.

7. Ukrepi za obvladovanje kriz v skladu s členom 21(2), točka (c), Direktive (EU) 2022/2555 se v skladu s tem členom štejejo za načrt za obvladovanje kriz na ravni subjekta za sektor električne energije, če ta vključuje vse zahteve iz odstavka 6.

8. Načrti za obvladovanje kriz se preskusijo med vajami na področju kibernetske varnosti iz členov 43, 44 in 45.

9. Subjekti s kritičnim ali velikim učinkom vključijo svoje načrte za obvladovanje kriz na ravni subjekta v svoje načrte za neprekinjeno poslovanje za postopke s kritičnim ali velikim učinkom. Načrti za obvladovanje kriz na ravni subjekta vključujejo:

(a) postopke, ki so odvisni od razpoložljivosti, celovitosti in zanesljivosti storitev IT;

(b) vse lokacije neprekinjenega poslovanja, vključno z lokacijami za strojno in programsko opremo;

(c) vse notranje vloge in odgovornosti, povezane s postopki neprekinjenega poslovanja.

10. Subjekti s kritičnim ali velikim učinkom posodobijo svoje načrte za obvladovanje kriz na ravni subjekta vsaj vsaka tri leta in kadar koli je to potrebno.

11. ACER posodobi načrt za obvladovanje kibernetskih kriz in odzivanje nanje na ravni Unije za sektor električne energije, ki ga pripravi v skladu z odstavkom 1, vsaj vsaka tri leta in kadar koli je to potrebno.

12. Vsak pristojni organ posodobi nacionalni načrt za obvladovanje kibernetskih kriz in odzivanje na krize na področju čezmejnih pretokov električne energije, pripravljen v skladu z odstavkom 2, vsaj vsaka tri leta in kadar koli je to potrebno.

13. Subjekti s kritičnim ali velikim učinkom preskusijo svoje načrte neprekinjenega poslovanja vsaj enkrat na tri leta ali po večjih spremembah v postopku s kritičnim učinkom. Rezultati preskusov načrtov neprekinjenega poslovanja se dokumentirajo. Subjekti s kritičnim ali velikim učinkom lahko preskus načrta neprekinjenega poslovanja vključijo v vaje na področju kibernetske varnosti.

14. Subjekti s kritičnim ali velikim učinkom po potrebi in vsaj enkrat na tri leta posodobijo svoj načrt neprekinjenega poslovanja, pri čemer upoštevajo rezultate preskusa.

15. Če se pri preskusu ugotovijo pomanjkljivosti v načrtu neprekinjenega poslovanja, subjekt s kritičnim ali velikim učinkom te pomanjkljivosti odpravi v 180 koledarskih dneh po preskusu in opravi nov preskus, da dokaže učinkovitost popravnih ukrepov.

16. Če subjekt s kritičnim ali velikim učinkom ne more odpraviti pomanjkljivosti v 180 koledarskih dneh, razloge za to navede v poročilu, ki ga predloži svojemu pristojnemu organu v skladu s členom 27.

Člen 42

Zmogljivosti zgodnjega opozarjanja glede kibernetske varnosti v sektorju električne energije

1. Pristojni organi sodelujejo z ENISA pri razvoju zmogljivosti zgodnjega opozarjanja glede kibernetske varnosti v sektorju električne energije v okviru pomoči državam članicam na podlagi člena 6(2) in člena 7 Uredbe (EU) 2019/881.

2. Zmogljivosti zgodnjega opozarjanja glede kibernetske varnosti v sektorju električne energije ENISA pri izvajanju nalog iz člena 7(7) Uredbe (EU) 2019/881 omogočajo, da:

(a) zbira informacije, ki jih prostovoljno izmenjujejo:

  (i) skupine CSIRT, pristojni organi;

  (ii) subjekti iz člena 2 te uredbe;

  (iii) vsi drugi subjekti, ki želijo prostovoljno izmenjati ustrezne informacije;

(b) oceni in razvrsti zbrane informacije;

(c) oceni informacije, do katerih ima dostop, za opredelitev pogojev kibernetskega tveganja in ustreznih kazalnikov za vidike čezmejnih pretokov električne energije;

(d) opredeli pogoje in kazalnike, ki so pogosto povezani s kibernetskimi napadi v sektorju električne energije;

(e) opredeli, ali je treba z oceno in opredelitvijo dejavnikov tveganja opraviti nadaljnjo analizo in sprejeti preventivne ukrepe;

(f) obvesti pristojne organe o ugotovljenih tveganjih in priporočenih preventivnih ukrepih, specifičnih za zadevne subjekte;

(g) obvesti vse zadevne subjekte iz člena 2 o rezultatih informacij, ocenjenih v skladu s točkami (b), (c) in (d) tega odstavka;

(h) redno vključuje ustrezne informacije v poročilo o stanju, izdanem v skladu s členom 7(6) Uredbe (EU) 2019/881;

(i) iz zbranih informacij po možnosti izpelje ustrezne podatke, ki kažejo na morebitno kršitev varnosti ali kibernetski napad (t. i. kazalniki ogroženosti).

3. Skupine CSIRT informacije, ki jih prejmejo od ENISA, nemudoma razširijo zadevnim subjektom v okviru svojih nalog, opredeljenih v členu 11(3), točka (b), Direktive (EU) 2022/2555.

4. ACER spremlja učinkovitost zmogljivosti zgodnjega opozarjanja glede kibernetske varnosti v sektorju električne energije. ENISA pomaga ACER z zagotavljanjem vseh potrebnih informacij v skladu s členom 6(2) in členom 7(1) Uredbe (EU) 2019/881. Analiza te dejavnosti spremljanja je del spremljanja na podlagi člena 12 te uredbe.

POGLAVJE VI

OKVIR VAJ NA PODROČJU KIBERNETSKE VARNOSTI V SEKTORJU ELEKTRIČNE ENERGIJE

Člen 43

Vaje na področju kibernetske varnosti na ravni subjekta in države članice

1. Vsak subjekt s kritičnim učinkom do 31. decembra v letu po svoji priglasitvi in nato vsaka tri leta izvede vajo na področju kibernetske varnosti, ki vključuje enega ali več scenarijev kibernetskih napadov, ki neposredno ali posredno vplivajo na čezmejne pretoke električne energije in so povezani s tveganji, ugotovljenimi med ocenami tveganja za kibernetsko varnost na ravni držav članic in subjektov v skladu s členoma 20 in 27.

2. Z odstopanjem od odstavka 1 se lahko nacionalni pristojni organi za pripravljenost na tveganja po posvetovanju s pristojnim organom in ustreznim organom za obvladovanje kibernetskih kriz, kot je imenovan ali ustanovljen v skladu s členom 9 Direktive (EU) 2022/2555, odloči, da namesto izvedbe vaje na področju kibernetske varnosti na ravni subjekta organizira vajo na ravni države članice, kot je opisano v odstavku 1. Pristojni organ o tem obvesti:

(a) vse subjekte s kritičnim učinkom v svoji državi članici, nacionalni regulativni organ, skupine CSIRT in nacionalni pristojni organ, odgovoren za kibernetsko varnost, najpozneje do 30. junija v letu pred izvedbo vaje na področju kibernetske varnosti na ravni subjekta;

(b) vsak subjekt, ki bo sodeloval pri vaji na področju kibernetske varnosti na ravni države članice, najpozneje šest mesecev pred izvedbo vaje.

3. Nacionalni pristojni organi za pripravljenost na tveganja ob tehnični podpori svojih skupin CSIRT organizira vajo na področju kibernetske varnosti iz odstavka 2 na ravni države članice samostojno ali v okviru druge vaje na področju kibernetske varnosti v tej državi članici. Da bi se lahko te vaje združile, lahko nacionalni pristojni organi za pripravljenost na tveganja izvedbo vaje kibernetske varnosti na ravni države članice iz odstavka 1 preloži za eno leto.

4. Vaje na področju kibernetske varnosti na ravni subjekta in na ravni države članice so skladne z nacionalnimi okviri obvladovanja kibernetskih kriz v skladu s členom 9(4), točka (d), Direktive (EU) 2022/2555.

5. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 31. decembra 2026 in nato vsaka tri leta zagotovi predlogo scenarija vaj za izvajanje vaj na področju kibernetske varnosti na ravni subjektov in držav članic iz odstavka 1. V tej predlogi se upoštevajo rezultati zadnje izvedene ocene tveganja za kibernetsko varnost na ravni subjekta in države članice, vključena pa so tudi ključna merila uspeha. ENTSO za električno energijo in telo EU ODS v pripravo take predloge vključita ACER in ENISA.

Člen 44

Regionalne ali medregionalne vaje na področju kibernetske varnosti

1. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 31. decembra 2029 in nato vsaka tri leta v vsaki regiji obratovanja sistema organizira regionalno vajo na področju kibernetske varnosti. Subjekti s kritičnim učinkom v regiji obratovanja sistema sodelujejo v regionalni vaji na področju kibernetske varnosti. ENTSO za električno energijo lahko v sodelovanju s telesom EU ODS namesto regionalne vaje na področju kibernetske varnosti v istem časovnem okviru organizira medregionalno vajo v več kot eni regiji obratovanja sistema. Pri vaji bi bilo treba upoštevati druge obstoječe ocene tveganja za kibernetsko varnost in scenarije, pripravljene na ravni Unije.

2. ENISA podpira ENTSO za električno energijo in telo EU ODS pri pripravi in organizaciji vaje na področju kibernetske varnosti na regionalni ali medregionalni ravni.

3. ENTSO za električno energijo v sodelovanju s telesom EU ODS šest mesecev pred izvedbo vaje o tem obvesti subjekte s kritičnim učinkom, ki bodo sodelovali v regionalni ali medregionalni vaji na področju kibernetske varnosti.

4. Organizator redne vaje na področju kibernetske varnosti na ravni Unije v skladu s členom 7(5) Uredbe (EU) 2019/881 ali katere koli obvezne vaje na področju kibernetske varnosti, povezane s sektorjem električne energije na istem geografskem območju, lahko k sodelovanju povabi ENTSO za električno energijo in telo EU ODS. V takih primerih se obveznost iz odstavka 1 ne uporablja, če vsi subjekti s kritičnim učinkom v regiji obratovanja sistema sodelujejo pri isti vaji.

5. Če ENTSO za električno energijo in telo EU ODS sodelujeta pri vaji na področju kibernetske varnosti iz odstavka 4, lahko regionalno ali medregionalno vajo na področju kibernetske varnosti iz odstavka 1 odložita za eno leto.

6. ENTSO za električno energijo v usklajevanju s telesom EU ODS do 31. decembra 2027 in vsaka tri leta po tem datumu zagotovi predlogo vaje za izvajanje regionalnih in medregionalnih vaj na področju kibernetske varnosti. V tej predlogi se upoštevajo rezultati zadnje izvedene ocene tveganja za kibernetsko varnost na regionalni ravni, vključena pa so tudi ključna merila uspeha. ENTSO za električno energijo se o organizaciji in izvedbi regionalnih in medregionalnih vaj na področju kibernetske varnosti posvetuje s Komisijo ter lahko zaprosi za nasvet ACER, ENISA in Skupno raziskovalno središče.

Člen 45

Rezultat vaj na področju kibernetske varnosti na ravni subjekta ali države članice ali na regionalni oziroma medregionalni ravni

1. Izvajalci kritičnih storitev na zahtevo subjekta s kritičnim učinkom sodelujejo pri vajah na področju kibernetske varnosti iz člena 43(1) in (2) ter člena 44(1), kadar za subjekt s kritičnim učinkom zagotavljajo storitve na področju, ki ustreza obsegu zadevne vaje na področju kibernetske varnosti.

2. Organizatorji vaj na področju kibernetske varnosti iz člena 43(1) in (2) ter člena 44(1) po nasvetu ENISA, če zanj zaprosijo, in v skladu s členom 7(5) Uredbe (EU) 2019/881 ustrezno vajo na področju kibernetske varnosti analizirajo in zaključijo s poročilom, v katerem povzamejo izkušnje in ki ga naslovijo na vse udeležence. Poročilo vključuje:

(a) scenarije vaj, poročila o srečanjih, glavna stališča, uspehe in pridobljene izkušnje na vseh ravneh vrednostne verige električne energije;

(b) navedbo o tem, ali so bila izpolnjena ključna merila uspeha;

(c) seznam priporočil za subjekte, ki so sodelovali v zadevni vaji na področju kibernetske varnosti, da popravijo, prilagodijo ali spremenijo postopke, povezane modele upravljanja in vse obstoječe pogodbene obveznosti, sklenjene z izvajalci kritičnih storitev, ki se nanašajo na kibernetske krize.

3. Organizatorji vaj na področju kibernetske varnosti iz člena 43(1) in (2) ter člena 44(1) na zahtevo mreže skupin CSIRT, Skupine za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ali mreže EU-CyCLONe izmenjajo rezultate zadevne vaje na področju kibernetske varnosti. Organizatorji z vsakim subjektom, ki sodeluje pri vajah, izmenjajo informacije iz odstavka 2, točki (a) in (b), tega člena. Organizatorji posredujejo seznam priporočil iz točke (c) navedenega odstavka izključno s subjekti, na katere se priporočila nanašajo.

4. Organizatorji vaj na področju kibernetske varnosti iz člena 43(1) in (2) ter člena 44(1) redno spremljajo izvajanje priporočil v skladu z odstavkom 2, točka (c), tega člena pri subjektih, ki sodelujejo pri vajah.

POGLAVJE VII

VARSTVO INFORMACIJ

Člen 46

Načela za varstvo izmenjanih informacij

1. Subjekti iz člena 2(1) zagotovijo, da so informacije, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, dostopne le na podlagi potrebe po seznanitvi in v skladu z ustreznimi predpisi Unije in nacionalnimi predpisi o varnosti informacij.

2. Subjekti iz člena 2(1) zagotovijo, da se informacije, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, obdelujejo in spremljajo v celotnem življenjskem ciklu teh informacij ter da se lahko ob koncu življenjskega cikla objavijo šele po anonimizaciji.

3. Subjekti iz člena 2(1) zagotovijo, da so sprejeti vsi potrebni organizacijski in tehnični varnostni ukrepi za varovanje in zaščito zaupnosti, celovitosti, razpoložljivosti in nezatajljivosti informacij, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, ne glede na uporabljena sredstva. Varnostni ukrepi:

(a) so sorazmerni;

(b) upoštevajo tveganja za kibernetsko varnost, povezana z znanimi preteklimi in nastajajočimi grožnjami, ki so jim te informacije lahko izpostavljene v okviru te uredbe;

(c) čim bolj temeljijo na nacionalnih, evropskih ali mednarodnih standardih in najboljših praksah;

(d) so dokumentirani.

4. Subjekti iz člena 2(1) zagotovijo, da je vsak posameznik, ki mu je odobren dostop do informacij, zagotovljenih, prejetih, izmenjanih ali posredovanih v skladu s to uredbo, seznanjen z varnostnimi pravili, ki se uporabljajo na ravni subjekta, ter z ukrepi in postopki, pomembnimi za varstvo informacij. Ti subjekti zagotovijo, da zadevni posameznik potrdi odgovornost za varovanje informacij v skladu z navodili med seznanitvijo.

5. Subjekti iz člena 2(1) zagotovijo, da je dostop do informacij, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, omejen na posameznike:

(a) ki so pooblaščeni za dostop do teh informacij na podlagi svojih funkcij, in na izvajanje dodeljenih nalog;

(b) za katere je subjekt lahko ocenil etična načela in načela integritete ter za katere ni dokazov o negativnih rezultatih preverjanja preteklosti, da bi ocenil zanesljivost posameznika v skladu z najboljšimi praksami in standardnimi varnostnimi zahtevami subjekta ter po potrebi z nacionalnimi zakoni in predpisi.

6. Subjekti iz člena 2(1) morajo imeti pisno soglasje fizične ali pravne osebe, ki je prvotno ustvarila ali zagotovila informacije, preden te informacije posredujejo tretji strani, ki ne spada na področje uporabe te uredbe.

7. Subjekt iz člena 2(1) lahko meni, da se te informacije izmenjujejo brez upoštevanja odstavkov 1 in 4 tega člena, da se prepreči sočasna kriza pri oskrbi z električno energijo, katere temeljni vzrok je povezan s kibernetsko varnostjo, ali čezmejna kriza v Uniji v drugem sektorju. V tem primeru:

(a) se posvetuje s pristojnim organom, ki ga pooblasti za izmenjavo takih informacij;

(b) anonimizira take informacije, ne da bi izgubil elemente, potrebne za obveščanje javnosti o neposrednem in resnem tveganju za čezmejne pretoke električne energije ter o možnih ukrepih za zmanjšanje tveganja;

(c) zaščiti identiteto izdajatelja in subjektov, ki so take informacije obdelovali v skladu s to uredbo.

8. Pristojni organi lahko z odstopanjem od odstavka 6 tega člena informacije, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, posredujejo tretji strani, ki ni navedena v členu 2(1), brez predhodnega pisnega soglasja izdajatelja informacij, vendar slednjega o tem obvestijo v najkrajšem možnem času. Pred razkritjem kakršnih koli informacij, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, tretji strani, ki ni navedena v členu 2(1), zadevni pristojni organ razumno zagotovi, da je zadevna tretja stran seznanjena z veljavnimi varnostnimi pravili, in pridobi razumno zagotovilo, da lahko zadevna tretja stran zagotovi varnost prejetih informacij v skladu z odstavki 1 do 5 tega člena. Pristojni organ take informacije anonimizira, ne da bi izgubil elemente, potrebne za obveščanje javnosti o neposrednem in resnem tveganju za čezmejne pretoke električne energije in možnih ukrepih za zmanjšanje tveganja, ter zaščiti identiteto izdajatelja informacij. V tem primeru tretja oseba, ki ni navedena v členu 2(1), prejete informacije zavaruje v skladu z določbami, ki že veljajo na ravni subjekta, če pa to ni mogoče, v skladu z določbami in navodili ustreznega pristojnega organa.

9. Ta člen se ne uporablja za subjekte, ki niso navedeni v členu 2(1) in ki so prejeli informacije v skladu z odstavkom 6 tega člena. V tem primeru se uporabi odstavek 7 tega člena ali pa lahko pristojni organ temu subjektu zagotovi pisne določbe, ki se uporabljajo v primerih, ko se informacije prejmejo v skladu s to uredbo.

Člen 47

Zaupnost informacij

1. Za vse informacije, ki se zagotovijo, prejmejo, izmenjajo ali posredujejo v skladu s to uredbo, veljajo pogoji varovanja poslovne skrivnosti iz odstavkov 2 do 5 tega člena te uredbe in zahteve iz člena 65 Uredbe (EU) 2019/943. Vse informacije, ki jih za namene izvajanja te uredbe zagotovijo, prejmejo, izmenjajo ali posredujejo subjekti iz člena 2 te uredbe, se zavarujejo ob upoštevanju stopnje zaupnosti informacij, ki jo je uporabil izdajatelj.

2. Obveznost varovanja poklicne skrivnosti velja za subjekte iz člena 2.

3. Nacionalni pristojni organi, odgovorni za kibernetsko varnost, nacionalni regulativni organi, nacionalni pristojni organi za pripravljenost na tveganja in skupine CSIRT si izmenjujejo vse potrebne informacije za izvajanje svojih nalog.

4. Vse informacije, ki jih subjekti iz člena 2(1) prejmejo, izmenjajo ali posredujejo za namene izvajanja člena 23, se anonimizirajo in združijo.

5. Brez poseganja v primere, ki jih ureja nacionalna zakonodaja, druge določbe te uredbe ali druga ustrezna zakonodaja Unije, se informacije, ki jih pri opravljanju svojih nalog prejme kateri koli subjekt ali organ, za katerega velja ta uredba, ne smejo razkriti nobenemu drugemu subjektu ali organu.

6. Brez poseganja v nacionalno zakonodajo ali zakonodajo Unije organ, subjekt ali fizična oseba, ki prejme informacije v skladu s to uredbo, teh informacij ne sme uporabiti za noben drug namen razen za opravljanje svojih dolžnosti v skladu s to uredbo.

7. ACER po posvetovanju z ENISA, vsemi pristojnimi organi, ENTSO za električno energijo in telesom EU ODS do 13. junija 2025 izda smernice o mehanizmih za izmenjavo informacij med vsemi subjekti iz člena 2(1), zlasti o predvidenih komunikacijskih tokovih in metodah za anonimizacijo in združevanje informacij za namene izvajanja tega člena.

8. Informacije, ki so v skladu s pravili Unije in nacionalnimi pravili zaupne, se s Komisijo in drugimi ustreznimi organi izmenjajo le, če je izmenjava potrebna za uporabo te uredbe. Izmenjujejo se le tiste informacije, ki so potrebne in sorazmerne z namenom te izmenjave. Pri izmenjavi informacij se ohrani zaupnost teh informacij ter zaščitijo varnostni in poslovni interesi subjektov s kritičnim ali velikim učinkom.

POGLAVJE VIII

KONČNE DOLOČBE

Člen 48

Začasne določbe

1. ENTSO za električno energijo v sodelovanju s telesom EU ODS do odobritve pogojev ali metodologij iz člena 6(2) oziroma načrtov iz člena 6(3) pripravi nezavezujoče smernice o naslednjih vprašanjih:

(a) začasnem ECII v skladu z odstavkom 2 tega člena;

(b) začasnem seznamu postopkov z velikim ali kritičnim učinkom na ravni Unije v skladu z odstavkom 4 tega člena in

(c) začasnem seznamu evropskih in mednarodnih standardov ter kontrol, ki jih zahteva nacionalna zakonodaja in so pomembni za vidike kibernetske varnosti čezmejnih pretokov električne energije v skladu z odstavkom 6 tega člena.

2. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 13. oktobra 2024 pripravi priporočilo o začasnem ECII. ENTSO za električno energijo v sodelovanju s telesom EU ODS o priporočenem začasnem ECII uradno obvesti pristojne organe.

3. Pristojni organi štiri mesece po prejemu priporočenega začasnega ECII ali najpozneje do 13. februarja 2025 na podlagi priporočenega ECII opredelijo kandidate za subjekte z velikim ali kritičnim učinkom v svoji državi članici ter pripravijo začasni seznam subjektov z velikim ali kritičnim učinkom. Subjekti z velikim ali kritičnim učinkom, ki so navedeni na začasnem seznamu, lahko na podlagi previdnostnega načela prostovoljno izpolnijo svoje obveznosti iz te uredbe. Pristojni organi do 13. marca 2025 uradno obvestijo subjekte z začasnega seznama, da so bili opredeljeni kot subjekti z velikim ali kritičnim učinkom.

4. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 13. decembra 2024 pripravi začasni seznam postopkov z velikim ali kritičnim učinkom na ravni Unije. Subjekti, priglašeni v skladu z odstavkom 3, ki se na podlagi previdnostnega načela prostovoljno odločijo, da bodo izpolnili svoje obveznosti iz te uredbe, uporabijo začasni seznam postopkov z velikim ali kritičnim učinkom, da določijo začasna območja z velikim ali kritičnim učinkom ter opredelijo, katera sredstva je treba vključiti v prvo oceno tveganja za kibernetsko varnost na ravni subjekta.

5. Vsak pristojni organ v skladu s členom 4(1) do 13. septembra 2024 ENTSO za električno energijo in telesu EU ODS predloži seznam svojih nacionalnih predpisov, ki so pomembni za vidike kibernetske varnosti čezmejnih pretokov električne energije.

6. ENTSO za električno energijo v sodelovanju s telesom EU ODS do 13. junija 2025 pripravi začasni seznam evropskih in mednarodnih standardov in kontrol, ki jih zahteva nacionalna zakonodaja in so pomembni za vidike kibernetske varnosti čezmejnih pretokov električne energije, pri čemer upošteva informacije, ki jih zagotovijo pristojni organi.

7. Začasni seznam evropskih in mednarodnih standardov in kontrol vključuje:

(a) evropske in mednarodne standarde ter nacionalne predpise, ki zagotavljajo smernice o metodologijah za obvladovanje tveganja za kibernetsko varnost na ravni subjekta, in

(b) kontrole kibernetske varnosti, enakovredne kontrolam, ki naj bi bile del minimalnih in razširjenih kontrol kibernetske varnosti.

8. ENTSO za električno energijo in telo EU ODS pri dokončnem oblikovanju začasnega seznama standardov upoštevata stališča, ki jih predložita ENISA in ACER. ENTSO za električno energijo in telo EU ODS objavita začasni seznam evropskih in mednarodnih standardov in kontrol na svojih spletiščih.

9. ENTSO za električno energijo in telo EU ODS se posvetujeta z ENISA in ACER o predlogih nezavezujočih smernic, pripravljenih v skladu z odstavkom 1.

10. Dokler se minimalne in razširjene kontrole kibernetske varnosti ne oblikujejo v skladu s členom 29 in ne sprejmejo v skladu s členom 8, si vsi subjekti iz člena 2(1) prizadevajo za postopno uporabo nezavezujočih smernic, pripravljenih v skladu z odstavkom 1.

Člen 49

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 11. marca 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN