Úradný vestník
Európskej únie

SK
Séria L

2024/1366

24.5.2024

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2024/1366

z 11. marca 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 stanovením sieťového predpisu pre odvetvové pravidlá týkajúce sa aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 z 5. júna 2019 o vnútornom trhu s elektrinou ([1]), a najmä na jeho článok 59 ods. 2 písm. e),

keďže:

(1) Riadenie kybernetickobezpečnostných rizík je zásadné v záujme zachovania bezpečnosti dodávok elektriny a zaistenia vysokej úrovne kybernetickej bezpečnosti v odvetví elektrickej energie.

(2) Digitalizácia a kybernetická bezpečnosť sú rozhodujúce pri poskytovaní základných služieb, v dôsledku čoho majú strategický význam pre kritickú energetickú infraštruktúru.

(3) V smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 ([2]) sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii. Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 ([3]) dopĺňa smernicu (EÚ) 2022/2555 tým, že sa ním zabezpečuje riadne určenie kybernetických incidentov v odvetví elektrickej energie ako rizika a riadne zohľadnenie opatrení prijatých na ich riešenie v plánoch pripravenosti na riziká. Nariadenie (EÚ) 2019/943 dopĺňa smernicu (EÚ) 2022/2555 a nariadenie (EÚ) 2019/941 stanovením osobitných pravidiel pre odvetvie elektrickej energie na úrovni Únie. Týmto delegovaným nariadením sa ďalej dopĺňajú ustanovenia smernice (EÚ) 2022/2555 týkajúce sa odvetvia elektrickej energie vo všetkých prípadoch, keď ide o cezhraničné toky elektriny.

(4) V kontexte prepojených digitalizovaných elektrizačných sústav nemožno považovať prevenciu a riadenie krízy dodávok elektriny súvisiacej s kybernetickými útokmi za výlučne vnútroštátnu úlohu. Mal by sa plne rozvinúť potenciál efektívnejších a menej nákladných opatrení prostredníctvom regionálnej spolupráce a spolupráce na úrovni Únie. Preto je potrebný spoločný rámec pravidiel a lepšie koordinované postupy, aby sa zabezpečilo, že členské štáty a iní aktéri budú môcť účinne spolupracovať naprieč hranicami v duchu zvýšenej transparentnosti, dôvery a solidarity medzi členskými štátmi a príslušnými orgánmi zodpovednými za elektrinu a kybernetickú bezpečnosť.

(5) Riadenie kybernetickobezpečnostných rizík v rozsahu pôsobnosti tohto nariadenia si vyžaduje štruktúrovaný proces, ktorý okrem iného zahŕňa identifikáciu rizík pre cezhraničné toky elektriny vyplývajúcich z kybernetických útokov, súvisiace prevádzkové procesy a obvody, zodpovedajúce kontroly kybernetickej bezpečnosti a overovacie mechanizmy. Hoci je časový rámec celého procesu rozložený na roky, každý jeho krok by mal prispieť k vysokej spoločnej úrovni kybernetickej bezpečnosti v tomto odvetví a k zmierneniu kybernetickobezpečnostných rizík. Všetky subjekty zúčastnené na tomto procese by mali vynaložiť maximálne úsilie na vypracovanie a odsúhlasenie metodík čo najskôr bez zbytočného odkladu a v každom prípade najneskôr v lehotách stanovených v tomto nariadení.

([1]) Ú. v. EÚ L 158, 14.6.2019, s. 54.

([2]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 z 5. júna 2019 o pripravenosti na riziká v sektore elektrickej energie a o zrušení smernice 2005/89/ES (Ú. v. EÚ L 158, 14.6.2019, s. 1).

(6) Posúdenia kybernetickobezpečnostných rizík na úrovni Únie, členských štátov, regiónov a subjektov v tomto nariadení možno obmedziť na riziká vyplývajúce z kybernetických útokov v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 ([4]), čím sa vylúčia napríklad fyzické útoky, prírodné katastrofy a výpadky v dôsledku straty zariadení alebo ľudských zdrojov. Na celoúnijné a regionálne riziká súvisiace s fyzickými útokmi alebo prírodnými katastrofami v oblasti elektrickej energie sa už vzťahujú iné existujúce právne predpisy Únie vrátane článku 5 nariadenia (EÚ) 2019/941 alebo nariadenie Komisie (EÚ) 2017/1485 ([5]), ktorým sa stanovuje usmernenie pre prevádzkovanie elektrizačnej prenosovej sústavy. Podobne cieľom smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 ([6]) o odolnosti kritických subjektov je obmedziť zraniteľnosti a posilniť fyzickú odolnosť kritických subjektov, pričom sa vzťahuje na všetky relevantné prírodné a ľudskou činnosťou spôsobené riziká, ktoré môžu ovplyvniť poskytovanie základných služieb, vrátane nehôd, prírodných katastrof, ohrozenia verejného zdravia, ako sú pandémie, a hybridných hrozieb alebo iných antagonistických hrozieb vrátane trestných činov terorizmu, prenikania trestnej činnosti a sabotáže.

(7) Pojem „subjekty s veľkým a kritickým vplyvom“ v tomto nariadení je základom na vymedzenie rozsahu subjektov, na ktoré sa budú vzťahovať povinnosti opísané v tomto nariadení. Cieľom prístupu založeného na rizikách, ktorý je uvedený v rôznych ustanoveniach, je identifikovať procesy, podporné aktíva a prevádzkujúce subjekty, ktoré majú vplyv na cezhraničné toky elektriny. V závislosti od stupňa vplyvu možných kybernetických útokov na ich prevádzku cezhraničných tokov elektriny ich možno považovať za subjekty „s veľkým vplyvom“ alebo „s kritickým vplyvom“. V článku 3 smernice (EÚ) 2022/2555 sa stanovujú pojmy kľúčové a dôležité subjekty a kritériá na označenie subjektov takýmito kategóriami. Hoci sa mnohé z nich budú považovať a budú súčasne označené za „kľúčové“ subjekty v zmysle článku 3 smernice (EÚ) 2022/2555 a za subjekty s veľkým alebo kritickým vplyvom podľa článku 24 tohto nariadenia, kritériá stanovené v tomto nariadení sa vzťahujú výlučne na ich úlohu a vplyv v rámci procesov súvisiacich s elektrinou, ktoré majú dosah na cezhraničné toky bez toho, aby sa akokoľvek zohľadňovali kritériá vymedzené v článku 3 smernice (EÚ) 2022/2555.

(8) Subjekty v rozsahu pôsobnosti tohto nariadenia, ktoré sa považujú za subjekty s veľkým alebo kritickým vplyvom podľa článku 24 tohto nariadenia a na ktoré sa vzťahujú povinnosti v ňom stanovené, sú predovšetkým subjekty, ktoré majú priamy vplyv na cezhraničné toky elektriny v EÚ.

(9) Toto nariadenie s cieľom zabezpečiť efektívnosť a zabrániť duplicite pri dosahovaní cieľov využíva existujúce mechanizmy a nástroje, ktoré už boli zavedené v iných právnych predpisoch.

(10) Pri uplatňovaní tohto nariadenia by členské štáty, príslušné orgány a prevádzkovatelia sústav mali zohľadniť dohodnuté európske normy a technické špecifikácie európskych normalizačných organizácií a konať v súlade s právnymi predpismi Únie týkajúcimi sa uvádzania výrobkov, na ktoré sa vzťahujú dané právne predpisy Únie, na trh alebo do prevádzky.

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022, s. 1).

([5]) Nariadenie Komisie (EÚ) 2017/1485 z 2. augusta 2017, ktorým sa stanovuje usmernenie pre prevádzkovanie elektrizačnej prenosovej sústavy (Ú. v. EÚ L 220, 25.8.2017, s. 1).

([6]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (Ú. v. EÚ L 333, 27.12.2022, s. 164).

(11) S cieľom zmierniť kybernetickobezpečnostné riziká je nutné stanoviť podrobný súbor pravidiel upravujúcich kroky príslušných zainteresovaných strán, ktorých činnosti sa týkajú aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny, a spoluprácu medzi nimi v snahe zaistiť bezpečnosť systému. Týmito organizačnými a technickými pravidlami by sa malo zaistiť, aby sa väčšina incidentov v odvetví elektrickej energie s hlavnými príčinami týkajúcimi sa kybernetickej bezpečnosti účinne riešila na prevádzkovej úrovni. Treba stanoviť, čo by tieto príslušné zainteresované strany mali urobiť v záujme prevencie takýchto kríz a aké opatrenia môžu prijať, ak by už samotné pravidlá na úrovni prevádzky sústavy nestačili. Je preto nutné vytvoriť spoločný rámec pravidiel spôsobu prevencie súbežných kríz dodávok elektriny s hlavnou príčinou týkajúcou sa kybernetickej bezpečnosti, ako aj prípravy na takéto krízy a ich riadenia. Prináša to viac transparentnosti do prípravnej fázy a počas súbežnej krízy dodávok elektriny a zabezpečí sa tak koordinované a účinné prijímanie opatrení spolu s príslušnými orgánmi pre kybernetickú bezpečnosť v členských štátoch. Od členských štátov a príslušných subjektov by sa malo vyžadovať, aby v duchu solidarity spolupracovali na regionálnej úrovni a v relevantných prípadoch dvojstranne. Účelom tejto spolupráce a pravidiel je dosiahnuť lepšiu pripravenosť na kybernetickobezpečnostné riziká pri nižších nákladoch, a to aj v súlade s cieľmi smernice (EÚ) 2022/2555. Zároveň sa zdá, že je nutné posilniť vnútorný trh s elektrinou posilnením dôvery a istoty medzi členskými štátmi, a to najmä zmiernením rizika neprimeraného obmedzenia cezhraničných tokov elektriny, čím sa zníži riziko negatívnych účinkov presahovania na susedné členské štáty.

(12) Bezpečnosť dodávok elektriny predpokladá efektívnu spoluprácu medzi členskými štátmi, inštitúciami, orgánmi, úradmi a agentúrami Únie a príslušnými zainteresovanými stranami. Prevádzkovatelia distribučných sústav a prevádzkovatelia prenosových sústav zohrávajú kľúčovú úlohu pri zaisťovaní bezpečnej, spoľahlivej a efektívnej elektrizačnej sústavy v súlade s článkami 31 a 40 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([7]). Pri zabezpečovaní a monitorovaní kybernetickej bezpečnosti pri dodávkach elektriny zohrávajú dôležitú úlohu aj rôzne regulačné orgány a iné relevantné príslušné vnútroštátne orgány v rámci úloh, ktoré im vyplývajú zo smerníc (EÚ) 2019/944 a (EÚ) 2022/2555. Členské štáty by mali určiť existujúci alebo nový subjekt za svoj príslušný vnútroštátny orgán na vykonávanie tohto nariadenia s cieľom zabezpečiť transparentnú a inkluzívnu účasť všetkých zúčastnených aktérov, efektívnu prípravu a jeho riadne vykonávanie, spoluprácu medzi rôznymi príslušnými zainteresovanými stranami a príslušnými orgánmi pôsobiacimi v odvetví elektrickej energie a v oblasti kybernetickej bezpečnosti, ako aj uľahčiť prevenciu a *ex post* hodnotenie kríz dodávok elektriny s hlavnými príčinami týkajúcimi sa kybernetickej bezpečnosti a výmenu informácií v tejto súvislosti.

(13) Keď subjekt s veľkým alebo kritickým vplyvom poskytuje služby vo viac ako jednom členskom štáte, prípadne má svoje sídlo alebo inú prevádzkareň či zástupcu v niektorom členskom štáte, ale jeho siete a informačné systémy sa nachádzajú v jednom alebo vo viacerých iných členských štátoch, tieto členské štáty by mali nabádať svoje príslušné orgány, aby podľa potreby vynaložili maximálne úsilie na spoluprácu a vzájomnú pomoc.

(14) Členské štáty by mali zabezpečiť, aby príslušné orgány mali vo vzťahu k subjektom s veľkým a kritickým vplyvom potrebné právomoci na podporu súladu s týmto nariadením. Tieto právomoci by mali príslušným orgánom umožňovať vykonávanie kontrol na mieste a dohľad na diaľku. To môže zahŕňať náhodné kontroly, vykonávanie pravidelných auditov, cielené bezpečnostné audity založené na posúdeniach rizík alebo dostupných informáciách súvisiacich s rizikami, ako aj bezpečnostné previerky založené na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posudzovania rizík, ktoré zahŕňajú požadovanie informácií potrebných na posúdenie opatrení v oblasti kybernetickej bezpečnosti prijatých subjektom. Tieto informácie by mali zahŕňať zdokumentované politiky kybernetickej bezpečnosti, údaje o prístupe, dokumenty alebo akékoľvek informácie potrebné na plnenie ich úloh dohľadu a dôkazy o vykonávaní politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov vykonaných kvalifikovaným audítorom a príslušné podkladové dôkazy.

([7]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/944 z 5. júna 2019 o spoločných pravidlách pre vnútorný trh s elektrinou a o zmene smernice 2012/27/EÚ (prepracované znenie) (Ú. v. EÚ L 158, 14.6.2019, s. 125).

(15) S cieľom zabrániť medzerám medzi povinnosťami v oblasti riadenia kybernetickobezpečnostných rizík uloženými subjektom s veľkým a kritickým vplyvom alebo ich duplicite by vnútroštátne orgány podľa smernice (EÚ) 2022/2555 a príslušné orgány podľa tohto nariadenia mali spolupracovať v súvislosti s vykonávaním opatrení na riadenie kybernetickobezpečnostných rizík a dohľadom nad dodržiavaním týchto opatrení na vnútroštátnej úrovni. Súlad subjektu s požiadavkami na riadenie kybernetickobezpečnostných rizík stanovenými v tomto nariadení by príslušné orgány podľa smernice (EÚ) 2022/2555 mohli považovať za zabezpečovanie dodržiavania zodpovedajúcich požiadaviek stanovených v uvedenej smernici, resp. naopak.

(16) Spoločný prístup k predchádzaniu súbežným krízam dodávok elektriny a ich riadeniu si vyžaduje, aby členské štáty rovnako chápali to, čo predstavuje súbežnú krízu dodávok elektriny a kedy pri nej zohráva dôležitú úlohu kybernetický útok. Predovšetkým by sa mala uľahčiť koordinácia medzi členskými štátmi a príslušnými subjektmi na účely riešenia situácie, v ktorej existuje alebo bezprostredne hrozí potenciálne riziko výrazného nedostatku elektriny alebo nemožnosti dodávať elektrinu odberateľom, a to v dôsledku kybernetického útoku.

(17) V odôvodnení 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([8]) sa uznáva kľúčová úloha sietí a informačných systémov a elektronických komunikačných sietí a služieb pri udržiavaní chodu kľúčových odvetví hospodárstva, ako je energetika, kým v odôvodnení 44 sa vysvetľuje, že Agentúra Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) by mala udržiavať kontakty s Agentúrou Európskej únie pre spoluprácu regulačných orgánov v oblasti energetiky (ďalej len „ACER“).

(18) V nariadení (EÚ) 2019/943 sa prevádzkovateľom prenosových sústav (ďalej len „PPS“) a prevádzkovateľom distribučných sústav (ďalej len „PDS“) prideľujú osobitné povinnosti v oblasti kybernetickej bezpečnosti. Ich európske združenia, konkrétne Európska sieť PPS pre elektrinu (ďalej len „ENTSO pre elektrinu“) a Európsky subjekt PDS (ďalej len „subjekt PDS EÚ“), podľa článku 30, resp. článku 55 uvedeného nariadenia podporujú kybernetickú bezpečnosť v spolupráci s príslušnými orgánmi a regulovanými subjektmi.

(19) Spoločný prístup k predchádzaniu súbežným krízam dodávok elektriny s hlavnými príčinami týkajúcimi sa kybernetickej bezpečnosti a k ich riadeniu si takisto vyžaduje, aby všetky príslušné zainteresované strany používali harmonizované metódy a definície na identifikáciu rizík súvisiacich s kybernetickou bezpečnosťou dodávok elektriny. Vyžaduje si aj schopnosť účinne porovnávať svoju výkonnosť a výkonnosť svojich susedov v tejto oblasti. Treba preto stanoviť procesy, úlohy a povinnosti s cieľom vypracovať a aktualizovať metodiky riadenia rizík, stupnice klasifikácie incidentov a opatrenia kybernetickej bezpečnosti prispôsobené kybernetickobezpečnostným rizikám, ktoré majú vplyv na cezhraničné toky elektriny.

(20) Členské štáty sú prostredníctvom príslušného orgánu určeného na účely tohto nariadenia zodpovedné za identifikáciu subjektov, ktoré spĺňajú kritériá na to, aby sa považovali za subjekty s veľkým a kritickým vplyvom. S cieľom odstrániť rozdiely medzi členskými štátmi v tejto súvislosti a zabezpečiť právnu istotu, pokiaľ ide o opatrenia na riadenie kybernetickobezpečnostných rizík a oznamovacie povinnosti pre všetky príslušné subjekty, by sa mal stanoviť súbor kritérií, ktorými sa určia subjekty, ktoré patria do rozsahu pôsobnosti tohto nariadenia. Tento súbor kritérií by sa mal vymedziť a pravidelne aktualizovať prostredníctvom procesu vypracúvania a prijímania podmienok a metodík, ako sa stanovuje v tomto nariadení.

(21) Ustanoveniami tohto nariadenia by nemali byť dotknuté právne predpisy Únie, v ktorých sa stanovujú osobitné pravidlá certifikácie produktov informačných a komunikačných technológií (ďalej len „IKT“), služieb IKT a procesov IKT, a to najmä nariadenie (EÚ) 2019/881, pokiaľ ide o rámec pre zavádzanie európskych schém certifikácie kybernetickej bezpečnosti. V kontexte tohto nariadenia by produkty IKT mali zahŕňať aj technické zariadenia a softvér, ktoré umožňujú priamu interakciu s elektrotechnickou sústavou, najmä priemyselnými kontrolnými systémami, ktoré možno použiť na prenos energie, distribúciu energie a výrobu energie, ako aj na zber a zasielanie súvisiacich informácií. Ustanoveniami by sa malo zabezpečiť, aby produkty IKT, služby IKT a procesy IKT, ktoré sa majú obstarať, spĺňali príslušné bezpečnostné ciele uvedené v článku 51 nariadenia (EÚ) 2019/881.

([8]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

(22) Nedávne kybernetické útoky svedčia o tom, že subjekty sa čoraz viac stávajú terčom útokov na dodávateľské reťazce. Takéto útoky na dodávateľské reťazce majú vplyv nielen na jednotlivé subjekty zahrnuté v rozsahu pôsobnosti, ale môžu mať aj kaskádový účinok na väčšie útoky na subjekty, ku ktorým sú pripojené v elektrizačnej sústave. Z tohto dôvodu boli doplnené ustanovenia a odporúčania na pomoc pri zmierňovaní kybernetickobezpečnostných rizík spojených s procesmi, ktoré súvisia s dodávateľským reťazcom, najmä s obstarávaním, ktoré majú vplyv na cezhraničné toky elektriny.

(23) Keďže využitie zraniteľností v sieťach a informačných systémoch môže zapríčiniť značné narušenia dodávok energie a škody pre hospodárstvo a spotrebiteľov, tieto zraniteľnosti by sa mali rýchlo identifikovať a napraviť v snahe znížiť riziká. S cieľom uľahčiť účinné vykonávanie tohto nariadenia by príslušné subjekty a príslušné orgány mali spolupracovať pri realizovaní a testovaní činností, ktoré sa považujú za vhodné na tento účel, vrátane výmeny informácií o kybernetických hrozbách, kybernetických útokoch, zraniteľnostiach, nástrojoch a metódach, taktikách, technikách a postupoch, pripravenosti na riadenie kríz kybernetickej bezpečnosti a iných aktivít. Vzhľadom na to, že technológie sa neustále vyvíjajú a digitalizácia odvetvia elektrickej energie rýchlo napreduje, vykonávanie prijatých ustanovení by nemalo mať škodlivý vplyv na inovácie a nemalo by predstavovať prekážku prístupu na trh s elektrinou a následného využívania inovatívnych riešení, ktoré prispievajú k efektívnosti a udržateľnosti elektrizačnej sústavy.

(24) Informácie zozbierané s cieľom monitorovať vykonávanie tohto nariadenia by sa mali primerane obmedziť podľa potreby poznať. Zainteresovaným stranám by sa mali poskytnúť splniteľné a účinné lehoty na predkladanie takýchto informácií. Malo by sa zabrániť dvojitému oznamovaniu.

(25) Kybernetickobezpečnostná ochrana sa nekončí na hraniciach Únie. Zabezpečený systém si vyžaduje zapojenie susedných tretích krajín. Únia a jej členské štáty by sa mali usilovať o podporu susedných tretích krajín, ktorých elektrická infraštruktúra je pripojená k európskej sústave, pri uplatňovaní podobných pravidiel kybernetickej bezpečnosti, aké sú stanovené v tomto nariadení.

(26) Na zlepšenie včasnej koordinácie bezpečnosti a na odskúšanie budúcich záväzných podmienok a metodík by ENTSO pre elektrinu, subjekt PDS EÚ a príslušné orgány mali začať vypracúvať nezáväzné usmernenie ihneď po nadobudnutí účinnosti tohto nariadenia. Toto usmernenie bude slúžiť ako základ na vypracovanie budúcich podmienok a metodík. Príslušné orgány by súbežne s tým mali určiť subjekty ako kandidátov na subjekty s veľkým a kritickým vplyvom, aby mohli dobrovoľne začať plniť povinnosti.

(27) Toto nariadenie bolo vypracované v úzkej spolupráci s organizáciami ACER, ENISA, ENTSO pre elektrinu, so subjektom PDS EÚ a s inými zainteresovanými subjektmi s cieľom transparentným a participatívnym spôsobom prijať účinné, vyvážené a primerané pravidlá.

(28) Týmto nariadením sa dopĺňajú a posilňujú opatrenia krízového riadenia zavedené v rámci EÚ pre reakciu na kybernetické krízy, ako sa stanovuje v odporúčaní Komisie (EÚ) 2017/1584 ([9]). Kybernetický útok by mohol takisto spôsobiť krízu dodávok elektriny v zmysle článku 2 bodu 9 nariadenia (EÚ) 2019/941, prispieť k nej alebo s ňou spolupôsobiť, čo by malo vplyv na cezhraničné toky elektriny. Takáto kríza dodávok elektriny by mohla viesť k súbežnej kríze dodávok elektriny v zmysle článku 2 bodu 10 nariadenia (EÚ) 2019/941. Takýto incident by mohol mať dosah aj na iné odvetvia závislé od bezpečnosti dodávok elektriny. Ak by sa takýto incident vystupňoval na rozsiahly kybernetický incident v zmysle článku 16 smernice (EÚ) 2022/2555, uplatňovať by sa mali ustanovenia uvedeného článku, ktorým sa zriaďuje Európska sieť styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“). Pokiaľ ide o krízové riadenie na úrovni Únie, príslušné strany by sa mali opierať o integrované dojednania EÚ o politickej reakcii na krízu (ďalej len „dojednania IPCR“) podľa vykonávacieho rozhodnutia Rady (EÚ) 2018/1993 ([10]).

(29) Týmto nariadením nie je dotknutá právomoc členských štátov prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov, a to v súlade s právom Únie. V súlade s článkom 346 ZFEÚ nemá byť žiaden členský štát povinný poskytovať informácie, ktorých sprístupnenie podľa jeho názoru odporuje základným záujmom jeho bezpečnosti.

([9]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

([10]) Vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu (Ú. v. EÚ L 320, 17.12.2018, s. 28).

(30) Hoci sa toto nariadenie vzťahuje v zásade na subjekty vykonávajúce činnosti v oblasti výroby elektrickej energie v jadrových elektrárňach, niektoré z uvedených činností môžu súvisieť s národnou bezpečnosťou.

(31) Na každé spracúvanie osobných údajov podľa tohto nariadenia by sa malo uplatňovať právo Únie v oblasti ochrany údajov a právo Únie v oblasti ochrany súkromia. Týmto nariadením konkrétne nie je dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([11]), smernica Európskeho parlamentu a Rady 2002/58/ES ([12]) a nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 ([13]). Týmto nariadením by preto nemali byť dotknuté okrem iného úlohy a právomoci orgánov príslušných na monitorovanie dodržiavania platného práva Únie v oblasti ochrany údajov a práva Únie v oblasti ochrany súkromia.

(32) Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by príslušné orgány zodpovedné za plnenie úloh, ktoré im boli pridelené podľa tohto nariadenia, a určené členskými štátmi mali mať možnosť zúčastňovať sa na sieťach medzinárodnej spolupráce. Príslušné orgány by preto na účely plnenia svojich úloh mali mať možnosť vymieňať si informácie vrátane osobných údajov s príslušnými orgánmi tretích krajín za predpokladu, že sú splnené podmienky podľa práva Únie v oblasti ochrany údajov pre prenosy osobných údajov do tretích krajín, okrem iného podmienky stanovené v článku 49 nariadenia (EÚ) 2016/679.

(33) Spracovanie osobných údajov v nevyhnutnom a primeranom rozsahu na účely zaistenia bezpečnosti aktív subjektmi s veľkým alebo kritickým vplyvom by sa mohlo považovať za zákonné na základe toho, že takéto spracovanie je v súlade so zákonnou povinnosťou, ktorej podlieha prevádzkovateľ v súlade s požiadavkami článku 6 ods. 1 písm. c) a článku 6 ods. 3 nariadenia (EÚ) 2016/679. Spracovanie osobných údajov môže byť potrebné aj pre oprávnené záujmy subjektov s veľkým alebo kritickým vplyvom, ako aj pre poskytovateľov bezpečnostných technológií a služieb, ktorí konajú v mene uvedených subjektov podľa článku 6 ods. 1 písm. f) nariadenia (EÚ) 2016/679, a to aj vtedy, keď je takéto spracovanie nevyhnutné na účely dohôd o výmene informácií o kybernetickej bezpečnosti alebo dobrovoľného zasielania relevantných informácií v súlade s týmto nariadením. Opatrenia súvisiace s prevenciou, odhaľovaním, identifikáciou, obmedzovaním následkov, analýzou kybernetických útokov a reakciami na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmena informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania zraniteľností, dobrovoľná výmena informácií o týchto kybernetických útokoch a o kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetickobezpečnostné výstrahy a konfiguračné nástroje môžu vyžadovať spracovanie určitých kategórií osobných údajov, ako sú IP adresy, jednotné vyhľadávače prostriedkov (URL), názvy domén, e-mailové adresy a časové pečiatky, ak prezrádzajú osobné údaje. Spracovanie osobných údajov príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT môže predstavovať právnu povinnosť alebo by sa mohlo považovať za nevyhnutné na vykonanie úlohy vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi podľa článku 6 ods. 1 písm. c) alebo e) a článku 6 ods. 3 nariadenia (EÚ) 2016/679 alebo na sledovanie oprávneného záujmu subjektov s veľkým alebo kritickým vplyvom podľa článku 6 ods. 1 písm. f) uvedeného nariadenia. Okrem toho sa vo vnútroštátnom práve môžu stanoviť pravidlá umožňujúce príslušným orgánom, jednotným kontaktným miestam a jednotkám CSIRT v rozsahu, ktorý je potrebný a primeraný na účely zaistenia bezpečnosti sietí a informačných systémov subjektov s veľkým alebo kritickým vplyvom, spracovávať osobitné kategórie osobných údajov podľa článku 9 nariadenia (EÚ) 2016/679, najmä stanovením vhodných a konkrétnych opatrení na ochranu základných práv a záujmov fyzických osôb vrátane technických obmedzení opakovaného použitia takýchto údajov a použitia najmodernejších bezpečnostných opatrení a opatrení na ochranu súkromia, ako je pseudonymizácia alebo šifrovanie, ak anonymizácia môže výrazne ovplyvniť sledovaný účel.

([11]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([12]) Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

([13]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

(34) V dôsledku kybernetických útokov je v mnohých prípadoch porušená ochrana osobných údajov. V uvedenej súvislosti by príslušné orgány mali spolupracovať a vymieňať si informácie o všetkých relevantných záležitostiach s orgánmi uvedenými v nariadení (EÚ) 2016/679 a smernici 2002/58/ES.

(35) V súlade s článkom 42 ods. 1 nariadenia (EÚ) 2018/1725 sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 17. novembra 2023 svoje stanovisko,

PRIJALA TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

Týmto nariadením sa zavádza sieťový predpis, v ktorom sa stanovujú odvetvové pravidlá týkajúce sa aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny vrátane pravidiel týkajúcich sa spoločných minimálnych požiadaviek, plánovania, monitorovania, podávania správ a krízového riadenia.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na aspekty kybernetickej bezpečnosti cezhraničných tokov elektriny v rámci činností týchto subjektov, ak sú identifikované ako subjekty s veľkým vplyvom alebo subjekty s kritickým vplyvom v súlade s článkom 24:

a) elektroenergetické podniky v zmysle článku 2 bodu 57 smernice (EÚ) 2019/944;

b) nominovaní organizátori trhu s elektrinou v zmysle článku 2 bodu 8 nariadenia (EÚ) 2019/943;

c) organizované miesta obchodovania alebo „organizované trhy“ v zmysle článku 2 bodu 4 vykonávacieho nariadenia Komisie (EÚ) č. 1348/2014 ([14]), ktoré zariaďujú transakcie s produktmi relevantnými pre cezhraničné toky elektriny;

d) poskytovatelia kritických služieb IKT v zmysle článku 3 bodu 9 tohto nariadenia;

e) ENTSO pre elektrinu zriadená podľa článku 28 nariadenia (EÚ) 2019/943;

f) subjekt PDS EÚ zriadený podľa článku 52 nariadenia (EÚ) 2019/943;

g) samostatné subjekty zúčtovania v zmysle článku 2 bodu 14 nariadenia (EÚ) 2019/943;

h) prevádzkovatelia nabíjacích bodov v zmysle prílohy I k smernici (EÚ) 2022/2555;

i) regionálne koordinačné centrá zriadené podľa článku 35 nariadenia (EÚ) 2019/943;

j) poskytovatelia riadených bezpečnostných služieb v zmysle článku 6 bodu 40 smernice (EÚ) 2022/2555;

k) akýkoľvek iný subjekt alebo tretia strana, na ktorú boli delegované alebo ktorej boli pridelené povinnosti podľa tohto nariadenia.

2. Za plnenie úloh pridelených v tomto nariadení sú v rámci svojich súčasných mandátov zodpovedné tieto orgány:

a) Agentúra Európskej únie pre spoluprácu regulačných orgánov v oblasti energetiky (ďalej len „ACER“) zriadená nariadením Európskeho parlamentu a Rady (EÚ) 2019/942 ([15]);

b) príslušné vnútroštátne orgány zodpovedné za plnenie úloh, ktoré im boli pridelené podľa tohto nariadenia, a určené členskými štátmi podľa článku 4 alebo „príslušný orgán“;

c) národné regulačné orgány určené každým členským štátom podľa článku 57 ods. 1 smernice (EÚ) 2019/944;

([14]) Vykonávacie nariadenie Komisie (EÚ) č. 1348/2014 zo 17. decembra 2014 o oznamovaní údajov, ktorým sa vykonáva článok 8 ods. 2 a 6 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1227/2011 o integrite a transparentnosti veľkoobchodného trhu s energiou (Ú. v. EÚ L 363, 18.12.2014, s. 121).

([15]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/942 z 5. júna 2019, ktorým sa zriaďuje Agentúra Európskej únie pre spoluprácu regulačných orgánov v oblasti energetiky (Ú. v. EÚ L 158, 14.6.2019, s. 22).

d) príslušné orgány pre pripravenosť na riziká zriadené podľa článku 3 nariadenia (EÚ) 2019/941;

e) jednotky pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“) určené alebo zriadené podľa článku 10 smernice (EÚ) 2022/2555;

f) príslušné orgány zodpovedné za kybernetickú bezpečnosť určené alebo zriadené podľa článku 8 smernice (EÚ) 2022/2555;

g) Agentúra Európskej únie pre kybernetickú bezpečnosť zriadená podľa nariadenia (EÚ) 2019/881;

h) akékoľvek iné orgány alebo tretia strana, na ktorú boli delegované alebo ktorej boli pridelené povinnosti podľa článku 4 ods. 3

3. Toto nariadenie sa vzťahuje aj na všetky subjekty, ktoré nie sú usadené v Únii, ale ktoré poskytujú služby subjektom v Únii, a to za predpokladu, že ich príslušné orgány určili za subjekty s veľkým alebo kritickým vplyvom v súlade s článkom 24 ods. 2

4. Týmto nariadením nie je dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti ani ich právomoc chrániť iné základné funkcie štátu vrátane zabezpečenia územnej celistvosti štátu a udržiavania verejného poriadku.

5. Týmto nariadením nie je dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti, pokiaľ ide o činnosti v oblasti výroby elektrickej energie v jadrových elektrárňach vrátane činností v rámci jadrového hodnotového reťazca, a to v súlade so zmluvami.

6. Subjekty, príslušné orgány, jednotné kontaktné miesta na úrovni subjektov a jednotky CSIRT spracúvajú osobné údaje v rozsahu potrebnom na účely tohto nariadenia a v súlade s nariadením (EÚ) 2016/679, pričom takéto spracovanie sa opiera najmä o jeho článok 6

Článok 3

Vymedzenie pojmov

Uplatňuje sa toto vymedzenie pojmov:

1. „aktívum“ sú akékoľvek hmotné alebo nehmotné informácie, softvér alebo hardvér v sieti a informačných systémoch, ktoré majú hodnotu pre jednotlivca, organizáciu alebo vládu;

2. „príslušný orgán pre pripravenosť na riziká“ je príslušný orgán určený podľa článku 3 nariadenia (EÚ) 2019/941;

3. „jednotka pre riešenie počítačových bezpečnostných incidentov“ je tím zodpovedný za riešenie rizík a incidentov v súlade s článkom 10 smernice (EÚ) 2022/2555;

4. „aktívum s kritickým vplyvom“ je aktívum, ktoré je nevyhnutné na vykonanie procesu s kritickým vplyvom;

5. „subjekt s kritickým vplyvom“ je subjekt, ktorý vykonáva proces s kritickým vplyvom a ktorý určili príslušné orgány v súlade s článkom 24;

6. „zóna kritického vplyvu“ je zóna vymedzená subjektom uvedeným v článku 2 ods. 1, ktorá zahŕňa všetky aktíva s kritickým vplyvom a v ktorej možno kontrolovať prístup k týmto aktívam a ktorá vymedzuje priestor, v ktorom sa uplatňujú pokročilé kontroly kybernetickej bezpečnosti;

7. „proces s kritickým vplyvom“ je obchodný proces vykonávaný subjektom, v prípade ktorého indexy vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy prekračujú prahovú hodnotu kritického vplyvu;

8. „prahová hodnota kritického vplyvu“ sú hodnoty indexov vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy uvedených v článku 19 ods. 3 písm. b), pri prekročení ktorých kybernetický útok na obchodný proces spôsobí kritické narušenie cezhraničných tokov elektriny;

9. „poskytovateľ kritických služieb IKT“ je subjekt, ktorý poskytuje službu alebo proces IKT, ktoré sú potrebné pre proces s kritickým vplyvom alebo proces s veľkým vplyvom ovplyvňujúci aspekty kybernetickej bezpečnosti cezhraničných tokov elektriny a ktorý v prípade kompromitácie môže spôsobiť kybernetický útok s vplyvom prekračujúcim prahovú hodnotu kritického vplyvu alebo veľkého vplyvu;

10. „cezhraničný tok elektriny“ je cezhraničný tok vymedzený v článku 2 bode 3 nariadenia (EÚ) 2019/943;

11. „kybernetický útok“ je incident v zmysle článku 3 bodu 14 nariadenia (EÚ) 2022/2554;

12. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle článku 2 bodu 1 nariadenia (EÚ) 2019/881;

13. „kontrola kybernetickej bezpečnosti“ sú činnosti alebo postupy vykonávané na účely predchádzania kybernetickobezpečnostným rizikám, ich odhaľovania, boja proti nim alebo ich minimalizácie;

14. „kybernetický incident“ je incident v zmysle článku 6 bodu 6 smernice (EÚ) 2022/2555;

15. „systém riadenia kybernetickej bezpečnosti“ sú politiky, postupy, usmernenia a súvisiace zdroje a činnosti, spoločne spravované subjektom v snahe o ochranu svojich informačných aktív pred kybernetickými hrozbami, systematické vytváranie, zavádzanie, prevádzkovanie, monitorovanie, preskúmavanie, udržiavanie a zlepšovanie bezpečnosti sietí a informačných systémov organizácie;

16. „operačné centrum kybernetickej bezpečnosti“ je špecializované centrum, v ktorom technický tím zložený z jedného alebo viacerých odborníkov s podporou informačných systémov kybernetickej bezpečnosti vykonáva úlohy súvisiace s bezpečnosťou [služby operačného centra kybernetickej bezpečnosti (ďalej len „CSOC“)], ako je riešenie kybernetických útokov a chýb bezpečnostnej konfigurácie, monitorovanie bezpečnosti, analýza logov a odhaľovanie kybernetických útokov;

17. „kybernetická hrozba“ je kybernetická hrozba v zmysle článku 2 bodu 8 nariadenia (EÚ) 2019/881;

18. „riadenie zraniteľnosti v oblasti kybernetickej bezpečnosti“ je postup identifikácie a riešenia zraniteľností;

19. „subjekt“ je subjekt v zmysle článku 6 bodu 38 smernice (EÚ) 2022/2555;

20. „včasné varovanie“ sú informácie potrebné na indikáciu toho, či existuje podozrenie, že významný incident je spôsobený nezákonným alebo zlomyseľným konaním, alebo či by mohol mať cezhraničný vplyv;

21. „index vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy“ (ďalej len „ECII“) je index alebo klasifikačná stupnica, ktorá zoraďuje možné dôsledky kybernetických útokov na obchodné procesy v rámci cezhraničných tokov elektriny;

22. „európsky systém certifikácie kybernetickej bezpečnosti“ je systém v zmysle článku 2 bodu 9 nariadenia (EÚ) 2019/881;

23. „subjekt s veľkým vplyvom“ je subjekt, ktorý vykonáva proces s veľkým vplyvom a ktorý určili príslušné orgány v súlade s článkom 24;

24. „proces s veľkým vplyvom“ je akýkoľvek obchodný proces vykonávaný subjektom, v prípade ktorého indexy vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy prekračujú prahovú hodnotu veľkého vplyvu;

25. „aktívum s veľkým vplyvom“ je aktívum, ktoré je nevyhnutné na vykonanie procesu s veľkým vplyvom;

26. „prahová hodnota veľkého vplyvu“ sú hodnoty indexov vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy uvedených v článku 19 ods. 3 písm. b), pri prekročení ktorých úspešný kybernetický útok na proces spôsobí veľké narušenie cezhraničných tokov elektriny;

27. „zóna veľkého vplyvu“ je zóna vymedzená subjektom uvedeným v článku 2 ods. 1, ktorá zahŕňa všetky aktíva s veľkým vplyvom a v ktorej možno kontrolovať prístup k týmto aktívam a ktorá vymedzuje rozsah, v ktorom sa uplatňujú minimálne kontroly kybernetickej bezpečnosti;

28. „produkt IKT“ je produkt IKT v zmysle článku 2 bodu 12 nariadenia (EÚ) 2019/881;

29. „služba IKT“ je služba IKT v zmysle článku 2 bodu 13 nariadenia (EÚ) 2019/881;

30. „proces IKT“ je proces IKT v zmysle článku 2 bodu 14 nariadenia (EÚ) 2019/881;

31. „pôvodný systém“ je pôvodný systém IKT v zmysle článku 3 bodu 3 nariadenia (EÚ) 2022/2554;

32. „vnútroštátne jednotné kontaktné miesto“ je jednotné kontaktné miesto určené alebo zriadené každým členským štátom podľa článku 8 ods. 3 smernice (EÚ) 2022/2555;

33. „orgány pre riadenie kybernetických kríz NIS“ sú orgány určené alebo zriadené podľa článku 9 bodu 1 smernice (EÚ) 2022/2555;

34. „pôvodca“ je subjekt, ktorý iniciuje udalosť výmeny informácií, zdieľania informácií alebo uloženia informácií;

35. „špecifikácie obstarávania“ sú špecifikácie, ktoré si subjekty určujú na účely obstarávania nových alebo aktualizovaných produktov IKT, procesov IKT alebo služieb IKT;

36. „zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene subjektu s veľkým alebo kritickým vplyvom, ktorý nie je usadený v Únii, ale poskytuje služby subjektom v Únii, a ktorú môže kontaktovať príslušný orgán alebo jednotka CSIRT namiesto samotného subjektu s veľkým alebo kritickým vplyvom v súvislosti s povinnosťami uvedeného subjektu podľa tohto nariadenia;

37. „riziko“ je riziko v zmysle článku 6 bodu 9 smernice (EÚ) 2022/2555;

38. „matica vplyvu rizika“ je matica používaná počas posudzovania rizika na určenie výslednej úrovne vplyvu rizika pre každé posudzované riziko;

39. „súbežná kríza dodávok elektriny“ je kríza dodávok elektriny v zmysle článku 2 bodu 10 nariadenia (EÚ) 2019/941;

40. „jednotné kontaktné miesto na úrovni subjektu“ je jednotné kontaktné miesto na úrovni subjektu určené podľa článku 38 ods. 1 písm. c);

41. „zainteresovaná strana“ je akákoľvek strana, ktorá má záujem na úspešnom a neustálom fungovaní organizácie alebo procesu, ako sú zamestnanci, riaditelia, akcionári, regulačné orgány, združenia, dodávatelia a zákazníci;

42. „norma“ je norma v zmysle článku 2 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([16]);

43. „región prevádzky sústavy“ je región prevádzky sústavy v zmysle prílohy I k rozhodnutiu ACER 05/2022 o určení regiónov prevádzky sústavy, zriadený v súlade s článkom 36 nariadenia (EÚ) 2019/943;

44. „prevádzkovatelia sústavy“ sú „prevádzkovateľ distribučnej sústavy“ (PDS) a „prevádzkovateľ prenosovej sústavy“ (PPS) v zmysle článku 2 bodov 29 a 35 smernice (EÚ) 2019/944;

45. „proces s kritickým vplyvom na celú Úniu“ je akýkoľvek proces v odvetví elektroenergetiky, ktorý môže zahŕňať viacero subjektov, v prípade ktorého sa možný vplyv kybernetického útoku môže počas vykonávania posúdenia kybernetickobezpečnostných rizík v celej Únii považovať za kritický;

46. „proces s veľkým vplyvom na celú Úniu“ je akýkoľvek proces v odvetví elektroenergetiky, ktorý môže zahŕňať viacero subjektov, v prípade ktorého sa možný vplyv kybernetického útoku môže počas vykonávania posúdenia kybernetickobezpečnostných rizík v celej Únii považovať za veľký;

47. „neopravená aktívne zneužívaná zraniteľnosť“ je zraniteľnosť, ktorá ešte nebola zverejnená a opravená a v prípade ktorej existujú spoľahlivé dôkazy o tom, že niekto spustil zlomyseľný kód v systéme bez povolenia vlastníka systému;

48. „zraniteľnosť“ je zraniteľnosť v zmysle článku 6 bodu 15 smernice (EÚ) 2022/2555.

Článok 4

Príslušný orgán

1. Každý členský štát čo najskôr a v každom prípade do 13. decembra 2024 určí národný vládny alebo regulačný orgán zodpovedný za plnenie úloh, ktoré sú mu pridelené v tomto nariadení (ďalej len „príslušný orgán“). Kým príslušnému orgánu nebude pridelené plnenie úloh podľa tohto nariadenia, úlohy príslušného orgánu v súlade s týmto nariadením plní regulačný orgán určený každým členským štátom podľa článku 57 ods. 1 smernice (EÚ) 2019/944.

2. Členské štáty bezodkladne upovedomia Komisiu, agentúru ACER, agentúru ENISA, skupinu pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenú podľa článku 14 smernice (EÚ) 2022/2555 a skupinu pre koordináciu v oblasti elektrickej energie zriadenú podľa článku 1 rozhodnutia Komisie z 15. novembra 2012 ([17]) a oznámia im názov a kontaktné údaje svojho príslušného orgánu určeného podľa odseku 1 tohto článku a všetky ich následné zmeny.

([16]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

([17]) Rozhodnutie Komisie z 15. novembra 2012, ktorým sa zriaďuje skupina pre koordináciu v oblasti elektrickej energie (2012/C 353/02) (Ú. v. EÚ C 353, 17.11.2012, s. 2).

3. Členské štáty môžu svojmu príslušnému orgánu povoliť, aby delegoval úlohy, ktoré mu boli pridelené v tomto nariadení, na iné vnútroštátne orgány s výnimkou úloh uvedených v článku 5. Každý príslušný orgán monitoruje uplatňovanie tohto nariadenia orgánmi, na ktoré delegoval úlohy. Príslušný orgán oznámi názvy orgánov, na ktoré bola delegovaná úloha, ich kontaktné údaje, pridelené úlohy a všetky ich následné zmeny Komisii, agentúre ACER, skupine pre koordináciu v oblasti elektrickej energie, agentúre ENISA a skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

Článok 5

Spolupráca medzi relevantnými orgánmi a subjektmi na vnútroštátnej úrovni

Príslušné orgány na účely plnenia príslušných povinností stanovených v tomto nariadení koordinujú a zabezpečujú náležitú spoluprácu medzi príslušnými orgánmi zodpovednými za kybernetickú bezpečnosť, orgánmi pre riadenie kybernetických kríz, národnými regulačnými orgánmi, príslušnými orgánmi pre pripravenosť na riziká a jednotkami CSIRT. Príslušné orgány takisto koordinujú činnosti s akýmikoľvek inými subjektmi alebo orgánmi určenými každým členským štátom s cieľom zaistiť efektívne postupy a zabrániť duplicite úloh a povinností. Príslušné orgány musia mať možnosť dať príslušným národným regulačným orgánom pokyn, aby agentúru ACER požiadali o stanovisko podľa článku 8 ods. 3

Článok 6

Podmienky alebo metodiky, alebo plány

1. PPS vypracujú v spolupráci so subjektom PDS EÚ návrhy podmienok alebo metodík podľa odseku 2, alebo plánov podľa odseku 3.

2. Schváleniu všetkými príslušnými orgánmi podliehajú tieto podmienky alebo metodiky a akékoľvek ich zmeny:

a) metodiky posudzovania kybernetickobezpečnostných rizík podľa článku 18 ods. 1;

b) komplexná správa o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny podľa článku 23;

c) minimálne a pokročilé kontroly kybernetickej bezpečnosti podľa článku 29, mapovanie kontrol kybernetickej bezpečnosti v odvetví elektrickej energie z hľadiska noriem podľa článku 34 vrátane minimálnych a pokročilých kontrol kybernetickej bezpečnosti v dodávateľskom reťazci v súlade s článkom 33;

d) odporúčania týkajúce sa obstarávania kybernetickej bezpečnosti podľa článku 35;

e) metodika určenia klasifikačnej stupnice kybernetických útokov podľa článku 37 ods. 8

3. Návrhy regionálnych plánov na zmiernenie kybernetickobezpečnostných rizík podľa článku 22 podliehajú schváleniu všetkými príslušnými orgánmi dotknutého regiónu prevádzky sústavy.

4. Návrhy podmienok, metodík uvedených v odseku 2 alebo plánov uvedených v odseku 3 zahŕňajú navrhovaný harmonogram ich vykonávania a opis ich očakávaného vplyvu na ciele tohto nariadenia.

5. Subjekt PDS EÚ môže dotknutým PPS poskytnúť odôvodnené stanovisko do troch týždňov pred uplynutím lehoty na predloženie návrhu podmienok alebo metodík, alebo plánov príslušným orgánom. PPS zodpovední za návrh podmienok alebo metodík, alebo plánov zohľadnia odôvodnené stanovisko subjektu PDS EÚ pred predložením návrhu na schválenie príslušným orgánom. PPS poskytnú odôvodnenie, ak stanovisko subjektu PDS EÚ nie je zohľadnené.

6. Pri spoločnom vypracúvaní podmienok, metodík a plánov zúčastnení PPS úzko spolupracujú. PPS s pomocou siete ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ pravidelne informujú príslušné orgány a agentúru ACER o pokroku pri vypracúvaní podmienok alebo metodík, alebo plánov.

Článok 7

Pravidlá hlasovania v prípade PPS

1. Ak PPS, ktorí rozhodujú o návrhoch podmienok alebo metodík, nedokážu dospieť k dohode, rozhodnú hlasovaním kvalifikovanou väčšinou. Kvalifikovaná väčšina sa v prípade takýchto návrhov vypočíta takto:

a) PPS zastupujúci najmenej 55 % členských štátov a

b) PPS zastupujúci členské štáty, ktorých počet obyvateľov tvorí spolu najmenej 65 % obyvateľstva Únie.

2. Blokujúca menšina v prípade rozhodnutí o návrhoch podmienok alebo metodík uvedených v článku 6 ods. 2 musí zahŕňať PPS zastupujúcich najmenej štyri členské štáty; v opačnom prípade sa kvalifikovaná väčšina považuje za dosiahnutú.

3. Ak PPS v regióne prevádzky sústavy, ktorí rozhodujú o návrhoch plánov uvedených v článku 6 ods. 2, nedokážu dospieť k dohode a ak dotknutý región prevádzky sústavy pozostáva z viac ako piatich členských štátov, PPS rozhodnú hlasovaním kvalifikovanou väčšinou. Na kvalifikovanú väčšinu v prípade návrhov uvedených v článku 6 ods. 2 sa vyžaduje väčšina:

a) PPS zastupujúcich najmenej 72 % dotknutých členských štátov a

b) PPS zastupujúcich členské štáty, ktorých počet obyvateľov tvorí spolu najmenej 65 % obyvateľstva dotknutej oblasti.

4. Blokujúca menšina v prípade rozhodnutí o návrhoch plánov musí zahŕňať prinajmenšom minimálny počet PPS zastupujúcich viac ako 35 % obyvateľstva zúčastnených členských štátov plus PPS zastupujúcich najmenej jeden ďalší dotknutý členský štát; v opačnom prípade sa kvalifikovaná väčšina považuje za dosiahnutú.

5. V prípade rozhodnutí PPS o návrhoch podmienok alebo metodík podľa článku 6 ods. 2 sa za každý členský štát pridelí jeden hlas. Ak na území členského štátu existuje viac ako jeden PPS, členský štát rozdelí hlasovacie práva medzi týchto PPS.

6. Ak PPS v spolupráci so subjektom PDS EÚ nepredložia relevantným príslušným orgánom pôvodný alebo zmenený návrh podmienok alebo metodík, alebo plánov v lehotách stanovených v tomto nariadení, relevantným príslušným orgánom a agentúre ACER poskytnú príslušné návrhy podmienok alebo metodík, alebo plánov. Vysvetlia, čo bránilo dosiahnutiu dohody. Príslušné orgány spoločne prijmú vhodné opatrenia na prijatie požadovaných podmienok alebo metodík, alebo požadovaných plánov. Môžu tak urobiť napríklad požiadaním o zmeny návrhov podľa tohto odseku, revíziou a skompletizovaním týchto návrhov alebo v prípade, že neboli poskytnuté žiadne návrhy, stanovením a schválením požadovaných podmienok alebo metodík, alebo plánov.

Článok 8

Predkladanie návrhov príslušným orgánom

1. PPS predložia návrhy podmienok alebo metodík, alebo plánov na schválenie relevantným príslušným orgánom v príslušných lehotách stanovených v článkoch 18, 23, 29, 33, 34, 35 a 37. Príslušné orgány môžu spoločne predĺžiť tieto lehoty za výnimočných okolností, najmä v prípadoch, keď lehotu nemožno dodržať z dôvodu okolností mimo kontroly PPS alebo subjektu PDS EÚ.

2. Návrhy podmienok, metodík alebo plánov podľa odseku 1 sa predkladajú agentúre ACER na informačné účely v rovnakom čase, ako sa predkladajú príslušným orgánom.

3. ACER na základe spoločnej žiadosti národných regulačných orgánov vydá stanovisko k návrhu podmienok alebo metodík, alebo plánov do šiestich mesiacov od doručenia návrhov podmienok alebo metodík, alebo plánov a o tomto stanovisku upovedomí národné regulačné orgány a príslušné orgány. Národné regulačné orgány, príslušné orgány zodpovedné za kybernetickú bezpečnosť a všetky ostatné orgány určené za príslušné orgány svoju činnosť navzájom koordinujú pred tým, ako národné regulačné orgány požiadajú agentúru ACER o stanovisko. ACER môže do takéhoto stanoviska zahrnúť odporúčania. ACER pred vydaním stanoviska k návrhom uvedeným v článku 6 ods. 2 uskutoční konzultácie s agentúrou ENISA.

4. Príslušné orgány spolu konzultujú, úzko spolupracujú a koordinujú svoju činnosť v záujme dosiahnutia dohody o navrhovaných podmienkach, metodikách alebo plánoch. Pred schválením podmienok alebo metodík, alebo plánov príslušné návrhy podľa potreby zrevidujú a doplnia po konzultácii s ENTSO pre elektrinu a so subjektom PDS EÚ s cieľom zaistiť, aby boli návrhy v súlade s týmto nariadením a prispievali k vysokej spoločnej úrovni kybernetickej bezpečnosti v celej Únii.

5. Príslušné orgány rozhodnú o podmienkach alebo metodikách, alebo o plánoch do šiestich mesiacov od doručenia podmienok alebo metodík, alebo plánov relevantnému príslušnému orgánu, prípadne poslednému dotknutému relevantnému príslušnému orgánu.

6. Ak agentúra ACER vydá stanovisko, relevantné príslušné orgány ho zohľadnia a prijmú svoje rozhodnutia do šiestich mesiacov od doručenia stanoviska agentúry ACER.

7. Ak príslušné orgány spoločne požadujú zmenu navrhovaných podmienok alebo metodík, alebo plánov, na účely ich schválenia vypracujú PPS v spolupráci so subjektom PDS EÚ návrh na takúto zmenu podmienok alebo metodík, alebo plánov. PPS predložia zmenený návrh na schválenie do dvoch mesiacov od prijatia žiadosti príslušných orgánov. Príslušné orgány rozhodnú o zmenených podmienkach alebo metodikách, alebo plánoch do dvoch mesiacov od ich predloženia.

8. Ak príslušné orgány nedokážu dospieť k dohode v lehote uvedenej v odseku 5 alebo 7, informujú o tom Komisiu. Komisia môže prijať vhodné kroky, aby umožnila prijatie požadovaných podmienok alebo metodík, alebo plánov.

9. PPS s pomocou ENTSO pre elektrinu a subjekt PDS EÚ zverejnia podmienky alebo metodiky, alebo plány na svojich webových sídlach po schválení relevantnými príslušnými orgánmi okrem prípadov, keď sa takéto informácie považujú za dôverné v súlade s článkom 47.

10. Príslušné orgány môžu spoločne požiadať PPS a subjekt PDS EÚ o návrhy na zmeny schválených podmienok alebo metodík, alebo schválených plánov a určiť lehotu na predloženie týchto návrhov. PPS môžu v spolupráci so subjektom PDS EÚ navrhnúť príslušným orgánom zmeny aj z vlastnej iniciatívy. Návrhy na zmenu podmienok alebo metodík, alebo na zmeny plánov sa vypracujú a schvália v súlade s postupom stanoveným v tomto článku.

11. Najmenej každé tri roky po prvom prijatí príslušných podmienok alebo metodík, alebo príslušných prijatých plánov musia PPS v spolupráci so subjektom PDS EÚ preskúmať účinnosť prijatých podmienok alebo metodík, alebo prijatých plánov a bez zbytočného odkladu predložiť správu o zisteniach preskúmania príslušným orgánom a agentúre ACER.

Článok 9

Konzultácia

1. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ konzultujú so zainteresovanými stranami vrátane agentúry ACER, agentúry ENISA a príslušného orgánu jednotlivých členských štátov návrhy podmienok alebo metodík uvedených v článku 6 ods. 2 a návrhy plánov uvedených v článku 6 ods. 3 Tieto konzultácie trvajú najmenej jeden mesiac.

2. Návrhy podmienok alebo metodík uvedených v článku 6 ods. 2, ktoré predložia PPS v spolupráci so subjektom PDS EÚ, sa uverejnia a predložia na konzultáciu na úrovni Únie. Návrhy plánov uvedených v článku 6 ods. 3, ktoré predložia príslušní PPS v spolupráci so subjektom PDS EÚ na regionálnej úrovni, sa predložia na konzultáciu prinajmenšom na regionálnej úrovni.

3. PPS s pomocou ENTSO pre elektrinu a subjekt PDS EÚ zodpovedný za návrh podmienok alebo metodík, alebo plánov pred predložením návrhu na schválenie regulačným orgánom náležite zohľadnia názory zainteresovaných strán vyplývajúce z konzultácií uskutočnených v súlade s odsekom 1. Vo všetkých prípadoch sa pri predložení musí poskytnúť a včas uverejniť riadne odôvodnenie začlenenia alebo nezačlenenia názorov vyplývajúcich z konzultácie, a to ešte pred uverejnením návrhu podmienok alebo metodík, alebo zároveň s týmto uverejnením.

Článok 10

Zapojenie zainteresovaných strán

Agentúra ACER v úzkej spolupráci s ENTSO pre elektrinu a so subjektom PDS EÚ organizuje zapojenie zainteresovaných strán vrátane pravidelných stretnutí so zainteresovanými stranami s cieľom identifikovať problémy a navrhovať zlepšenia súvisiace s vykonávaním tohto nariadenia.

Článok 11

Náhrada nákladov

1. Náklady, ktoré znášajú PPS a PDS podliehajúci regulácii sieťových taríf a ktoré vyplývajú z povinností stanovených v tomto nariadení, vrátane nákladov, ktoré znáša ENTSO pre elektrinu a subjekt PDS EÚ, posudzuje relevantný národný regulačný orgán každého členského štátu.

2. Náklady, ktoré sa posúdia ako primerané, efektívne a proporcionálne, sa nahradia prostredníctvom sieťových taríf alebo iných vhodných mechanizmov, ktoré určí relevantný národný regulačný orgán.

3. Na žiadosť relevantných národných regulačných orgánov poskytnú PPS a PDS uvedení v odseku 1 v primeranej lehote, ktorú určil národný regulačný orgán, informácie potrebné na uľahčenie posúdenia vzniknutých nákladov.

Článok 12

Monitorovanie

1. Agentúra ACER monitoruje vykonávanie tohto nariadenia v súlade s článkom 32 ods. 1 nariadenia (EÚ) 2019/943 a článkom 4 ods. 2 nariadenia (EÚ) 2019/942. Pri vykonávaní tohto monitorovania môže agentúra ACER spolupracovať s agentúrou ENISA a požiadať o podporu ENTSO pre elektrinu a subjekt PDS EÚ. Agentúra ACER pravidelne informuje skupinu pre koordináciu v oblasti elektrickej energie a skupinu pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti o vykonávaní tohto nariadenia.

2. Agentúra ACER najmenej každé tri roky po nadobudnutí účinnosti tohto nariadenia uverejní správu, v ktorej

a) preskúma stav vykonávania platných opatrení na riadenie kybernetickobezpečnostných rizík, pokiaľ ide o subjekty s veľkým a kritickým vplyvom;

b) určí, či môžu byť potrebné ďalšie pravidlá týkajúce sa spoločných požiadaviek, plánovania, monitorovania, podávania správ a krízového riadenia, aby sa predišlo rizikám pre odvetvie elektroenergetiky, a

c) identifikuje oblasti zlepšenia pri revízii tohto nariadenia alebo určí nepokryté oblasti a nové priority, ktoré sa môžu objaviť v dôsledku technologického vývoja.

3. Agentúra ACER v spolupráci s agentúrou ENISA a po konzultácii s ENTSO pre elektrinu a so subjektom PDS EÚ môže do 13. júna 2025 vydať usmernenia k relevantným informáciám, ktoré sa majú oznamovať agentúre ACER na účely monitorovania, ako aj o postupe a frekvencii ich zhromažďovania na základe ukazovateľov výkonnosti vymedzených v súlade s odsekom 5.

4. Príslušným orgánom môže byť poskytnutý prístup k relevantným informáciám uchovávaným agentúrou ACER, ktoré agentúra zhromaždila v súlade s týmto článkom.

5. Agentúra ACER v spolupráci s agentúrou ENISA a s podporou ENTSO pre elektrinu a subjektu PDS EÚ vydá nezáväzné ukazovatele výkonnosti na posudzovanie prevádzkovej spoľahlivosti, ktoré sa týkajú aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny.

6. Subjekty uvedené v článku 2 ods. 1 tohto nariadenia predkladajú agentúre ACER informácie, ktoré agentúra ACER potrebuje na plnenie úloh uvedených v odseku 2.

Článok 13

Referenčné porovnávanie

1. Agentúra ACER v spolupráci s agentúrou ENISA do 13. júna 2025 vypracuje nezáväznú príručku k referenčnému porovnávaniu v oblasti kybernetickej bezpečnosti. Príručka obsahuje vysvetlenia pre národné regulačné orgány týkajúce sa zásad referenčného porovnávania zavedených kontrol kybernetickej bezpečnosti podľa odseku 2 tohto článku s prihliadnutím na náklady spojené so zavedením kontrol a na účinnosť funkcie, ktorú plnia procesy, produkty, služby, systémy a riešenia používané na zavedenie takýchto kontrol. Pri vypracovaní nezáväznej príručky k referenčnému porovnávaniu v oblasti kybernetickej bezpečnosti agentúra ACER zohľadní existujúce správy o referenčnom porovnávaní. Agentúra ACER predloží nezáväznú príručku k referenčnému porovnávaniu v oblasti kybernetickej bezpečnosti národným regulačným orgánom na informačné účely.

2. Národné regulačné orgány vykonajú do 12 mesiacov od vypracovania príručky k referenčnému porovnávaniu podľa odseku 1 porovnávaciu analýzu s cieľom posúdiť, či súčasné investície do kybernetickej bezpečnosti:

a) zmierňujú riziká, ktoré majú vplyv na cezhraničné toky elektriny;

b) prinášajú požadované výsledky a zvyšujú efektívnosť rozvoja elektrizačných sústav;

c) sú efektívne a integrované do celkového obstarávania aktív a služieb.

3. Pri porovnávacej analýze môžu vnútroštátne regulačné orgány zohľadniť nezáväznú príručku k referenčnému porovnávaniu v oblasti kybernetickej bezpečnosti, ktorú vypracovala agentúra ACER, a posúdia najmä:

a) priemerné výdavky súvisiace s kybernetickou bezpečnosťou na zmiernenie rizík, ktoré majú vplyv na cezhraničné toky elektriny, najmä pokiaľ ide o subjekty s veľkým a kritickým vplyvom;

b) v spolupráci s ENTSO pre elektrinu a so subjektom PDS EÚ priemerné ceny služieb, systémov a produktov kybernetickej bezpečnosti, ktoré vo veľkej miere prispievajú k zlepšeniu a udržiavaniu opatrení na riadenie kybernetickobezpečnostných rizík v rôznych regiónoch prevádzky sústavy;

c) existenciu a úroveň porovnateľnosti nákladov a funkcií služieb, systémov a riešení kybernetickej bezpečnosti vhodných na vykonávanie tohto nariadenia, pričom sa identifikujú možné opatrenia potrebné na podporu efektívnosti výdavkov, najmä v prípadoch, keď môžu byť potrebné investície do technológií kybernetickej bezpečnosti.

4. Zaobchádzanie so všetkými informáciami týkajúcimi sa porovnávacej analýzy a ich spracúvanie podliehajú požiadavkám na utajenie údajov stanoveným v tomto nariadení, minimálnym kontrolám kybernetickej bezpečnosti a sú predmetom správy o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny. Porovnávacia analýza uvedená v odsekoch 2 a 3 sa nezverejňuje.

5. Bez toho, aby boli dotknuté požiadavky týkajúce sa dôvernosti uvedené v článku 47 a potreba chrániť bezpečnosť subjektov, na ktoré sa vzťahujú ustanovenia tohto nariadenia, sa porovnávacia analýza uvedená v odsekoch 2 a 3 tohto článku predloží všetkým národným regulačným orgánom, všetkým príslušným orgánom, agentúre ACER, agentúre ENISA a Komisii.

Článok 14

Dohody s PPS mimo Únie

1. PPS v regióne prevádzky sústavy, ktorý susedí s treťou krajinou, sa usilujú do 18 mesiacov od nadobudnutia účinnosti tohto nariadenia uzavrieť s PPS susediacej tretej krajiny dohody, ktoré sú v súlade s príslušným právom Únie a v ktorých sa stanovuje základ spolupráce v oblasti ochrany kybernetickej bezpečnosti, a mechanizmy spolupráce v oblasti kybernetickej bezpečnosti s týmito PPS.

2. PPS informujú príslušný orgán o dohodách uzavretých podľa odseku 1.

Článok 15

Právni zástupcovia

1. Subjekty, ktoré nie sú usadené v Únii, ale poskytujú služby subjektom v Únii a boli v súlade s článkom 24 ods. 6 informované, že sú subjektmi s veľkým alebo kritickým vplyvom, do troch mesiacov, odkedy boli informované, písomne určia zástupcu v Únii a informujú o tom príslušný oznamujúci orgán.

2. Tento zástupca má poverenie, v zmysle ktorého sa akýkoľvek príslušný orgán alebo jednotka CSIRT v Únii v súvislosti s povinnosťami subjektu s veľkým alebo kritickým vplyvom podľa tohto nariadenia obracia okrem alebo namiesto daného subjektu na tohto zástupcu. Subjekt s veľkým alebo kritickým vplyvom poskytne svojmu právnemu zástupcovi potrebné právomoci a dostatočné zdroje na zaručenie efektívnej a včasnej spolupráce s relevantnými príslušnými orgánmi alebo jednotkami CSIRT.

3. Zástupca musí byť usadený v jednom z členských štátov, v ktorých subjekt ponúka svoje služby. Predpokladá sa, že subjekt podlieha jurisdikcii toho členského štátu, v ktorom je usadený jeho zástupca. Subjekty s veľkým alebo kritickým vplyvom oznámia meno, poštovú adresu, e-mailovú adresu a telefónne číslo svojho právneho zástupcu príslušnému orgánu v členskom štáte, v ktorom má tento právny zástupca pobyt alebo je usadený.

4. Musí byť možné brať určeného právneho zástupcu na zodpovednosť za nedodržanie povinností podľa tohto nariadenia bez toho, aby bola dotknutá zodpovednosť a právne kroky uplatniteľné voči samotnému subjektu s veľkým alebo kritickým vplyvom.

5. Ak v zmysle tohto článku nie je v Únii určený zástupca, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky pre nedodržanie povinností podľa tohto nariadenia.

6. Určenie právneho zástupcu v Únii podľa odseku 1 nepredstavuje usadenie sa v Únii.

Článok 16

Spolupráca medzi ENTSO pre elektrinu a subjektom PDS EÚ

1. ENTSO pre elektrinu a subjekt PDS EÚ spolupracujú pri vykonávaní posúdení kybernetickobezpečnostných rizík podľa článku 19 a článku 21, a to najmä pri plnení týchto úloh:

a) vypracovanie metodík posudzovania kybernetickobezpečnostných rizík podľa článku 18 ods. 1;

b) vypracovanie komplexnej správy o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny podľa článku 23;

c) vypracovanie spoločného rámca pre kybernetickú bezpečnosť v odvetví elektrickej energie podľa kapitoly III;

d) vypracovanie odporúčaní týkajúcich sa obstarávania kybernetickej bezpečnosti podľa článku 35;

e) vypracovanie metodiky určenia klasifikačnej stupnice kybernetických útokov podľa článku 37 ods. 8;

f) vypracovanie predbežného indexu vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy (ďalej len „ECII“) podľa článku 48 ods. 1 písm. a);

g) vypracovanie konsolidovaného predbežného zoznamu subjektov s veľkým a kritickým vplyvom podľa článku 48 ods. 3;

h) vypracovanie predbežného zoznamu procesov s veľkým a kritickým vplyvom na celú Úniu podľa článku 48 ods. 4;

i) vypracovanie predbežného zoznamu európskych a medzinárodných noriem a kontrol podľa článku 48 ods. 6;

j) vykonanie posúdenia kybernetickobezpečnostných rizík v celej Únii podľa článku 19;

k) vykonanie regionálnych posúdení kybernetickobezpečnostných rizík podľa článku 21;

l) určenie regionálnych plánov na zmiernenie kybernetickobezpečnostných rizík podľa článku 22;

m) vypracovanie usmernení k európskym systémom certifikácie kybernetickej bezpečnosti pre produkty IKT, služby IKT a procesy IKT v súlade s článkom 36;

n) vypracovanie usmernení k vykonávaniu tohto nariadenia po konzultácii s agentúrou ACER a agentúrou ENISA.

2. Spolupráca medzi ENTSO pre elektrinu a subjektom PDS EÚ môže mať formu pracovnej skupiny pre kybernetickobezpečnostné riziká.

3. ENTSO pre elektrinu a subjekt PDS EÚ pravidelne informujú agentúru ACER, agentúru ENISA, skupinu pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a skupinu pre koordináciu v oblasti elektrickej energie o pokroku pri vykonávaní posúdenia kybernetickobezpečnostných rizík v celej Únii podľa článku 19 a regionálnych posúdení kybernetickobezpečnostných rizík podľa článku 21.

Článok 17

Spolupráca medzi agentúrou ACER a príslušnými orgánmi

Agentúra ACER v spolupráci s jednotlivými príslušnými orgánmi:

1. monitoruje vykonávanie opatrení na riadenie kybernetickobezpečnostných rizík podľa článku 12 ods. 2 písm. a) a plnenie povinností týkajúcich sa predkladania správ podľa článku 27 a článku 39 a

2. monitoruje proces prijímania a vykonávanie podmienok, metodík alebo plánov podľa článku 6 ods. 2 a 3. Spolupráca medzi agentúrou ACER, agentúrou ENISA a jednotlivými príslušnými orgánmi môže mať formu orgánu pre monitorovanie kybernetickobezpečnostných rizík.

KAPITOLA II

POSUDZOVANIE RIZÍK A IDENTIFIKÁCIA RELEVANTNÝCH KYBERNETICKOBEZPEČNOSTNÝCH RIZÍK

Článok 18

Metodiky posudzovania kybernetickobezpečnostných rizík

1. PPS s pomocou ENTSO pre elektrinu, v spolupráci so subjektom PDS EÚ a po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti predloží do 13. marca 2025 návrh metodík posudzovania kybernetickobezpečnostných rizík na úrovni Únie, na regionálnej úrovni a na úrovni členských štátov.

2. Metodiky posudzovania kybernetickobezpečnostných rizík na úrovni Únie, na regionálnej úrovni a na úrovni členských štátov zahŕňajú:

a) zoznam kybernetických hrozieb, ktoré treba zvážiť, vrátane prinajmenšom týchto hrozieb pre dodávateľské reťazce:

   i) závažné a neočakávané narušenie dodávateľského reťazca;

   ii) nedostupnosť produktov IKT, služieb IKT alebo procesov IKT z dodávateľského reťazca;

iii) kybernetické útoky iniciované prostredníctvom účastníkov dodávateľského reťazca;

iv) únik citlivých informácií cez dodávateľský reťazec vrátane sledovania v rámci dodávateľského reťazca;

v) zavedenie slabých miest alebo tzv. zadných dvierok do produktov IKT, služieb IKT alebo procesov IKT prostredníctvom účastníkov dodávateľského reťazca;

b) kritériá, na základe ktorých sa vplyv kybernetickobezpečnostných rizík vyhodnocuje ako veľký alebo kritický s použitím vymedzených prahových hodnôt pre dôsledky a pravdepodobnosť;

c) prístup k analýze kybernetickobezpečnostných rizík vyplývajúcich z pôvodných systémov, kaskádových účinkov kybernetických útokov a povahy systémov prevádzkujúcich sústavu v reálnom čase;

d) prístup k analýze kybernetickobezpečnostných rizík vyplývajúcich zo závislosti od jedného dodávateľa produktov IKT, služieb IKT alebo procesov IKT.

3. V rámci metodík posudzovania kybernetickobezpečnostných rizík na úrovni Únie, na regionálnej úrovni a na úrovni členských štátov sa posudzujú kybernetickobezpečnostné riziká pomocou rovnakej matice vplyvu rizika. Maticou vplyvu rizika sa:

a) merajú dôsledky kybernetických útokov na základe týchto kritérií:

i) výpadok zaťaženia;

ii) zníženie výroby elektriny;

iii) strata kapacity v rámci primárnej frekvenčnej rezervy;

iv) strata kapacity na obnovenie prevádzky elektrizačnej sústavy bez závislosti od externej prenosovej sústavy po úplnom alebo čiastočnom odstavení (nazýva sa aj „štart z tmy“);

v) predpokladané trvanie výpadku elektriny ovplyvňujúceho odberateľov v kombinácii s rozsahom tohto výpadku vyjadreným ako počet odberateľov a

vi) akékoľvek iné kvantitatívne alebo kvalitatívne kritériá, ktoré by mohli primerane slúžiť ako ukazovateľ vplyvu kybernetického útoku na cezhraničné toky elektriny;

b) meria pravdepodobnosť vzniku incidentu ako frekvencia kybernetických útokov za rok.

4. V metodikách posudzovania kybernetickobezpečnostných rizík na úrovni Únie sa opisuje, ako budú vymedzené hodnoty ECII, pokiaľ ide o prahové hodnoty veľkého a kritického vplyvu. Počas posudzovania vplyvu na obchodnú činnosť, ktoré subjekty vykonávajú podľa článku 26 ods. 4 písm. c) bodu i), im ECII umožňuje odhadovať s pomocou kritérií uvedených v odseku 2 písm. b) vplyv rizík na ich obchodné procesy.

5. ENTSO pre elektrinu v koordinácii so subjektom PDS EÚ informuje skupinu pre koordináciu v oblasti elektrickej energie o návrhoch metodík posudzovania kybernetickobezpečnostných rizík, ktoré sú vypracované podľa odseku 1.

Článok 19

Posúdenie kybernetickobezpečnostných rizík v celej Únii

1. Bez toho, aby bol dotknutý článok 22 smernice (EÚ) 2022/2555, ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ a po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti vykoná do deviatich mesiacov od schválenia metodík posudzovania kybernetickobezpečnostných rizík podľa článku 8 a potom každé tri roky posúdenie kybernetickobezpečnostných rizík v celej Únii a vypracuje návrh správy o posúdení kybernetickobezpečnostných rizík v celej Únii. Na tento účel použijú metodiky vypracované podľa článku 18 a schválené podľa článku 8, na základe ktorých identifikujú, zanalyzujú a vyhodnotia možné dôsledky kybernetických útokov, ktoré ovplyvňujú prevádzkovú bezpečnosť elektrizačnej sústavy a narúšajú cezhraničné toky elektriny. V posúdení kybernetickobezpečnostných rizík v celej Únii sa nezohľadňujú právne, finančné škody ani poškodenie dobrej povesti spôsobené kybernetickými útokmi.

2. Správa o posúdení kybernetickobezpečnostných rizík v celej Únii obsahuje tieto prvky:

a) procesy s veľkým vplyvom na celú Úniu a procesy s kritickým vplyvom na celú Úniu;

b) maticu vplyvu rizika, ktorú subjekty a príslušné orgány používajú na posúdenie kybernetickobezpečnostného rizika identifikovaného v posúdení kybernetickobezpečnostných rizík na úrovni členského štátu vykonanom podľa článku 20 a v posúdení kybernetickobezpečnostných rizík na úrovni subjektu podľa článku 26 ods. 2 písm. b).

3. Pokiaľ ide o procesy s veľkým vplyvom na celú Úniu a procesy s kritickým vplyvom na celú Úniu, správa o posúdení kybernetickobezpečnostných rizík v celej Únii obsahuje:

a) posúdenie možných dôsledkov kybernetického útoku s použitím ukazovateľov vymedzených v metodike posudzovania kybernetickobezpečnostných rizík vypracovanej podľa článku 18 ods. 2, 3 a 4 a schválenej podľa článku 8;

b) ECII a prahové hodnoty veľkého a kritického vplyvu, ktoré príslušné orgány používajú podľa článku 24 ods. 1 a 2 na identifikáciu subjektov s veľkým a kritickým vplyvom zapojených do procesov s veľkým vplyvom na celú Úniu a do procesov s kritickým vplyvom na celú Úniu.

4. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ predloží agentúre ACER na účely vydania stanoviska návrh správy o posúdení kybernetickobezpečnostných rizík v celej Únii s výsledkami posúdenia kybernetickobezpečnostných rizík v celej Únii. Agentúra ACER vydá stanovisko k návrhu správy do troch mesiacov od jeho doručenia. ENTSO pre elektrinu a subjekt PDS EÚ pri finalizácii tejto správy v čo najväčšej miere zohľadnia stanovisko agentúry ACER.

5. Do troch mesiacov od doručenia stanoviska agentúry ACER informuje ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ agentúru ACER, Komisiu, agentúru ENISA a príslušné orgány o záverečnej správe o posúdení kybernetickobezpečnostných rizík v celej Únii.

Článok 20

Posúdenie kybernetickobezpečnostných rizík v členskom štáte

1. Každý príslušný orgán vykoná posúdenie kybernetickobezpečnostných rizík v členskom štáte týkajúce sa všetkých subjektov s veľkým a kritickým vplyvom v danom členskom štáte s použitím metodík vypracovaných podľa článku 18 a schválených podľa článku 8. V posúdení kybernetickobezpečnostných rizík v členskom štáte sa identifikujú a analyzujú riziká kybernetických útokov, ktoré ovplyvňujú prevádzkovú bezpečnosť elektrizačnej sústavy a narúšajú cezhraničné toky elektriny. V posúdení kybernetickobezpečnostných rizík v členskom štáte sa nezohľadňujú právne, finančné škody ani poškodenie dobrej povesti spôsobené kybernetickými útokmi.

2. Každý príslušný orgán s podporou jednotky CSIRT do 21 mesiacov od informovania subjektov s veľkým a kritickým vplyvom podľa článku 24 ods. 6 a každé tri roky po tomto dátume a po konzultácii s príslušným orgánom zodpovedným za kybernetickú bezpečnosť v oblasti elektroenergetiky predloží ENTSO pre elektrinu a subjektu PDS EÚ správu o posúdení kybernetickobezpečnostných rizík v členskom štáte, ktorá obsahuje tieto informácie o každom obchodnom procese s veľkým a kritickým vplyvom:

a) stav vykonávania minimálnych a pokročilých kontrol kybernetickej bezpečnosti podľa článku 29;

b) zoznam všetkých kybernetických útokov oznámených za predchádzajúce tri roky podľa článku 38 ods. 3;

c) súhrn informácií o kybernetických útokoch oznámených za predchádzajúce tri roky podľa článku 38 ods. 6;

d) v prípade každého procesu s veľkým alebo kritickým vplyvom na celú Úniu odhad rizík ohrozenia dôvernosti, integrity a dostupnosti informácií a príslušných aktív;

e) podľa potreby zoznam ďalších subjektov identifikovaných ako subjekty s veľkým alebo kritickým vplyvom podľa článku 24 ods. 1, 2, 3 a 5.

3. V správe o posúdení kybernetickobezpečnostných rizík v členskom štáte sa zohľadní plán pripravenosti členského štátu na riziká vypracovaný podľa článku 10 nariadenia (EÚ) 2019/941.

4. Informácie obsiahnuté v správe o posúdení kybernetickobezpečnostných rizík v členskom štáte podľa odseku 2 písm. a) až d) nesmú byť spojené s konkrétnymi subjektmi ani aktívami. Správa o posúdení kybernetickobezpečnostných rizík v členskom štáte obsahuje aj posúdenie rizík týkajúce sa dočasných výnimiek udelených príslušnými orgánmi v členských štátoch podľa článku 30.

5. ENTSO pre elektrinu a subjekt PDS EÚ môžu v súvislosti s úlohami uvedenými v odseku 2 písm. a) a c) požiadať príslušné orgány o doplňujúce informácie.

6. Príslušné orgány zabezpečia, aby informácie, ktoré poskytujú, boli presné a správne.

Článok 21

Regionálne posúdenia kybernetickobezpečnostných rizík

1. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ a po konzultácii s príslušným regionálnym koordinačným centrom vykoná regionálne posúdenie kybernetickobezpečnostných rizík za každý región prevádzky sústavy s použitím metodík vypracovaných podľa článku 19 a schválených podľa článku 8 s cieľom identifikovať, analyzovať a vyhodnotiť riziká kybernetických útokov, ktoré ovplyvňujú prevádzkovú bezpečnosť elektrizačnej sústavy a narúšajú cezhraničné toky elektriny. V regionálnych posúdeniach kybernetickobezpečnostných rizík sa nezohľadňujú právne, finančné škody ani poškodenie dobrej povesti spôsobené kybernetickými útokmi.

2. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ a po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti do 30 mesiacov od informovania subjektov s veľkým vplyvom a subjektov s kritickým vplyvom podľa článku 24 ods. 6 a potom každé tri roky vypracuje správu o regionálnom posúdení kybernetickobezpečnostných rizík za každý región prevádzky sústavy.

3. V správe o regionálnom posúdení kybernetickobezpečnostných rizík sa zohľadňujú relevantné informácie obsiahnuté v správach o posúdení kybernetickobezpečnostných rizík v celej Únii a v správach o posúdení kybernetickobezpečnostných rizík v členských štátoch.

4. V regionálnom posúdení kybernetickobezpečnostných rizík sa zohľadnia regionálne scenáre krízy dodávok elektriny týkajúce sa kybernetickej bezpečnosti identifikované podľa článku 6 nariadenia (EÚ) 2019/941.

Článok 22

Regionálne plány na zmiernenie kybernetickobezpečnostných rizík

1. PPS s pomocou ENTSO pre elektrinu, v spolupráci so subjektom PDS EÚ a po konzultácii s regionálnymi koordinačnými centrami a so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti do 36 mesiacov od informovania subjektov s veľkým a kritickým vplyvom podľa článku 24 ods. 6, najneskôr však do 13. júna 2031 a každé tri roky po tomto dátume vypracujú regionálny plán na zmiernenie kybernetickobezpečnostných rizík za každý región prevádzky sústavy.

2. Regionálne plány na zmiernenie kybernetickobezpečnostných rizík zahŕňajú:

a) minimálne a pokročilé kontroly kybernetickej bezpečnosti, ktoré subjekty s veľkým vplyvom a subjekty s kritickým vplyvom uplatnia v regióne prevádzky sústavy;

b) zostávajúce kybernetickobezpečnostné riziká v regiónoch prevádzky sústavy po uplatnení kontrol uvedených v písmene a).

3. ENTSO pre elektrinu predloží regionálne plány na zmiernenie rizík príslušným prevádzkovateľom prenosových sústav, príslušným orgánom a skupine pre koordináciu v oblasti elektrickej energie. Skupina pre koordináciu v oblasti elektrickej energie môže odporučiť zmeny.

4. PPS s pomocou ENTSO pre elektrinu, v spolupráci so subjektom PDS EÚ a po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti každé tri roky aktualizujú regionálne plány na zmiernenie rizík, pokiaľ si okolnosti nevyžadujú častejšiu aktualizáciu.

Článok 23

Komplexná správa o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny

1. PPS s pomocou ENTSO pre elektrinu, v spolupráci so subjektom PDS EÚ a po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti do 40 mesiacov od informovania subjektov s veľkým a kritickým vplyvom podľa článku 24 ods. 6 a potom každé tri roky predložia skupine pre koordináciu v oblasti elektrickej energie správu o výsledku posúdenia kybernetickobezpečnostných rizík v súvislosti s cezhraničnými tokmi elektriny (ďalej len „komplexná správa o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny“).

2. Komplexná správa o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny vychádza zo správy o posúdení kybernetickobezpečnostných rizík v celej Únii, zo správ o posúdení kybernetickobezpečnostných rizík v členských štátoch a zo správ o regionálnom posúdení kybernetickobezpečnostných rizík a obsahuje tieto informácie:

a) zoznam procesov s veľkým a kritickým vplyvom na celú Úniu identifikovaných v správe o posúdení kybernetickobezpečnostných rizík v celej Únii v súlade s článkom 19 ods. 2 písm. a) vrátane odhadu pravdepodobnosti a vplyvu kybernetickobezpečnostných rizík vyhodnotených v rámci správ o regionálnom posúdení kybernetickobezpečnostných rizík podľa článku 21 ods. 2 a článku 19 ods. 3 písm. a);

b) aktuálne kybernetické hrozby s osobitným zameraním na vznikajúce hrozby a riziká pre elektrizačnú sústavu;

c) kybernetické útoky za predchádzajúce obdobie na úrovni Únie, pričom sa uvedie kritický prehľad o tom, aký vplyv mohli mať takéto kybernetické útoky na cezhraničné toky elektriny;

d) celkový stav vykonávania opatrení kybernetickej bezpečnosti;

e) stav vykonávania informačných tokov podľa článkov 37 a 38;

f) zoznam informácií alebo osobitné kritériá vzťahujúce sa na utajovanie informácií podľa článku 46;

g) identifikované a zvýraznené riziká, ktoré môžu vyplývať z nedostatočného riadenia dodávateľského reťazca;

h) výsledky a zozbierané skúsenosti z regionálnych a medziregionálnych kybernetickobezpečnostných cvičení organizovaných podľa článku 44;

i) analýzu vývoja celkových cezhraničných kybernetickobezpečnostných rizík v odvetví elektroenergetiky od posledného regionálneho posúdenia kybernetickobezpečnostných rizík;

j) akékoľvek ďalšie informácie, ktoré môžu byť užitočné na identifikáciu možných zlepšení tohto nariadenia alebo potreby revízie tohto nariadenia, alebo ktoréhokoľvek z jeho nástrojov, a

k) agregované a anonymizované informácie o výnimkách udelených podľa článku 30 ods. 3

3. Subjekty uvedené v článku 2 ods. 1 môžu prispieť k vypracovaniu komplexnej správy o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny, pričom dodržiavajú dôvernosť informácií v súlade s článkom 47. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ sa najprv radia s týmito subjektmi.

4. Komplexná správa o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny podlieha pravidlám týkajúcim sa ochrany výmeny informácií podľa článku 46. Bez toho, aby bol dotknutý článok 10 ods. 4 a článok 47 ods. 4, ENTSO pre elektrinu a subjekt PDS EÚ vydajú verejnú verziu uvedenej správy, ktorá neobsahuje informácie, ktoré by mohli poškodiť subjekty uvedené v článku 2 ods. 1 Vydanie verejnej verzie tejto správy je podmienené súhlasom skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a skupiny pre koordináciu v oblasti elektrickej energie. Za zostavenie a vydanie verejnej verzie správy zodpovedá ENTSO pre elektrinu v koordinácii so subjektom PDS EÚ.

Článok 24

Identifikácia subjektov s veľkým a kritickým vplyvom

1. Každý príslušný orgán pomocou ECII a prahových hodnôt veľkého a kritického vplyvu, ktoré sú zahrnuté v správe o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 3 písm. b), identifikuje subjekty s veľkým a kritickým vplyvom vo svojom členskom štáte, ktoré sú zapojené do procesov s veľkým a kritickým vplyvom na celú Úniu. Príslušné orgány môžu požiadať o informácie subjekt vo svojom členskom štáte, aby pre tento subjekt určili hodnoty ECII. Ak zistený ECII subjektu presahuje prahovú hodnotu veľkého alebo kritického vplyvu, identifikovaný subjekt sa uvedie v správe o posúdení kybernetickobezpečnostných rizík v členskom štáte uvedenej v článku 20 ods. 2

2. Každý príslušný orgán pomocou ECII a prahových hodnôt veľkého a kritického vplyvu, ktoré sú zahrnuté v správe o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 3 písm. b), identifikuje subjekty s veľkým a kritickým vplyvom, ktoré nie sú usadené v Únii, pokiaľ pôsobia v Únii. Príslušný orgán môže požiadať o informácie subjekt, ktorý nie je usadený v Únii, aby pre tento subjekt určil hodnoty ECII.

3. Každý príslušný orgán môže identifikovať ďalšie subjekty vo svojom členskom štáte ako subjekty s veľkým alebo kritickým vplyvom, ak sú splnené tieto kritériá:

a) subjekt je súčasťou skupiny subjektov, pri ktorých existuje významné riziko, že budú súbežne zasiahnuté kybernetickým útokom;

b) agregovaný ECII za skupinu subjektov presahuje prahovú hodnotu veľkého alebo kritického vplyvu.

4. Ak príslušný orgán identifikuje ďalšie subjekty v súlade s odsekom 3, všetky procesy v týchto subjektoch, v prípade ktorých agregovaný ECII za skupinu presahuje prahovú hodnotu veľkého vplyvu, sa považujú za procesy s veľkým vplyvom a všetky procesy v týchto subjektoch, v prípade ktorých agregovaný ECII za skupinu presahuje prahové hodnoty kritického vplyvu, sa považujú za procesy s kritickým vplyvom.

5. Ak príslušný orgán identifikuje subjekty uvedené v odseku 3 písm. a) vo viac než jednom členskom štáte, informuje ostatné príslušné orgány, ENTSO pre elektrinu a subjekt PDS EÚ. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ na základe informácií získaných od všetkých príslušných orgánov poskytne príslušným orgánom analýzu agregácie subjektov vo viac než jednom členskom štáte, ktorá môže spôsobiť distribuované narušenie cezhraničných tokov elektriny a môže viesť ku kybernetickému útoku. Ak je skupina subjektov vo viacerých členských štátoch identifikovaná ako agregácia, ktorej ECII presahuje prahovú hodnotu veľkého alebo kritického vplyvu, všetky dotknuté príslušné orgány identifikujú subjekty v takejto skupine ako subjekty s veľkým alebo kritickým vplyvom pre príslušný členský štát na základe agregovaného ECII za skupinu subjektov a identifikované subjekty sa uvedú v správe o posúdení kybernetickobezpečnostných rizík v celej Únii.

6. Každý príslušný orgán do deviatich mesiacov po tom, ako ho ENTSO pre elektrinu a subjekt PDS EÚ informoval o správe o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 5, a v každom prípade najneskôr do 13. júna 2028 informuje subjekty uvedené v zozname, že boli identifikované ako subjekty s veľkým alebo kritickým vplyvom v danom členskom štáte.

7. Ak je poskytovateľ služieb nahlásený príslušnému orgánu ako poskytovateľ kritických služieb IKT podľa článku 27 písm. c), uvedený príslušný orgán o tom informuje príslušné orgány členských štátov, na ktorých území sa nachádza jeho sídlo alebo zástupca. Dotknutý príslušný orgán poskytovateľa služieb informuje, že bol identifikovaný ako poskytovateľ kritických služieb.

Článok 25

Vnútroštátne systémy overovania

1. Príslušné orgány môžu zaviesť vnútroštátny systém overovania s cieľom overiť, či subjekty s kritickým vplyvom identifikované podľa článku 24 ods. 1 vykonali vnútroštátny legislatívny rámec, ktorý je zahrnutý v matici mapovania uvedenej v článku 34. Vnútroštátny systém overovania môže byť založený na inšpekcii vykonanej príslušným orgánom, nezávislých bezpečnostných auditoch alebo na vzájomných partnerských preskúmaniach vykonaných subjektmi s kritickým vplyvom v tom istom členskom štáte pod dohľadom príslušného orgánu.

2. Ak sa príslušný orgán rozhodne zaviesť vnútroštátny systém overovania, zabezpečí, aby sa overovanie vykonávalo v súlade s týmito požiadavkami:

a) každá strana vykonávajúca partnerské preskúmanie, audit alebo inšpekciu musí byť nezávislá od overovaného subjektu s kritickým vplyvom a nesmie byť v konflikte záujmov;

b) zamestnanci vykonávajúci partnerské preskúmanie, audit alebo inšpekciu musia mať preukázateľné znalosti o:

   i) kybernetickej bezpečnosti v odvetví elektroenergetiky;

   ii) systémoch riadenia kybernetickej bezpečnosti;

   iii) zásadách auditu;

   iv) posúdeniach kybernetickobezpečnostných rizík;

   v) spoločnom rámci pre kybernetickú bezpečnosť v odvetví elektrickej energie;

   vi) vnútroštátnom legislatívnom a regulačnom rámci a o európskych a medzinárodných normách v rozsahu overovania;

   vii) procesoch s kritickým vplyvom v rozsahu overovania;

c) strane vykonávajúcej partnerské preskúmanie, audit alebo inšpekciu sa musí poskytnúť dostatočný čas na vykonanie týchto činností;

d) strana vykonávajúca partnerské preskúmanie, audit alebo inšpekciu musí prijať vhodné opatrenia na ochranu informácií, ktoré počas overovania zhromaždí, v súlade s úrovňou ich dôvernosti a

e) partnerské preskúmania, audity alebo inšpekcie sa musia vykonávať aspoň raz ročne a musia pokrývať celý rozsah overovania aspoň raz za tri roky.

3. Ak sa príslušný orgán rozhodne zaviesť vnútroštátny systém overovania, každoročne podáva agentúre ACER správu o tom, ako často vykonával inšpekcie v rámci tohto systému.

Článok 26

Riadenie kybernetickobezpečnostných rizík na úrovni subjektu

1. Každý subjekt s veľkým a kritickým vplyvom, ktorý identifikovali príslušné orgány podľa článku 24 ods. 1, vykonáva riadenie kybernetickobezpečnostných rizík v prípade všetkých svojich aktív nachádzajúcich sa v jeho zónach veľkého vplyvu a kritického vplyvu. Každý subjekt s veľkým a kritickým vplyvom každé tri roky vykonáva riadenie rizík zahŕňajúce fázy uvedené v odseku 2.

2. Každý subjekt s veľkým a kritickým vplyvom vychádza pri riadení kybernetickobezpečnostných rizík z prístupu, ktorého cieľom je chrániť jeho sieť a informačné systémy a ktorý zahŕňa tieto fázy:

a) určenie kontextu;

b) posúdenie kybernetickobezpečnostných rizík na úrovni subjektu;

c) ošetrenie kybernetickobezpečnostných rizík;

d) akceptácia kybernetickobezpečnostných rizík.

3. Vo fáze určenia kontextu každý subjekt s veľkým a kritickým vplyvom:

a) vymedzí rozsah posúdenia kybernetickobezpečnostných rizík vrátane procesov s veľkým a kritickým vplyvom, ktoré identifikoval ENTSO pre elektrinu a subjekt PDS EÚ, a ďalších procesov, ktoré môžu byť cieľom kybernetických útokov s veľkým alebo kritickým vplyvom na cezhraničné toky elektriny, a

b) určí kritériá hodnotenia rizík a akceptácie rizík v súlade s maticou vplyvu rizika, ktorú subjekty a príslušné orgány používajú na posudzovanie kybernetickobezpečnostných rizík v metodikách posudzovania kybernetickobezpečnostných rizík na úrovni Únie, na regionálnej úrovni a na úrovni členských štátov, ako ich vypracoval ENTSO pre elektrinu a subjekt PDS EÚ v súlade s článkom 19 ods. 2

4. Vo fáze posúdenia kybernetickobezpečnostných rizík každý subjekt s veľkým a kritickým vplyvom:

a) identifikuje kybernetickobezpečnostné riziká s prihliadnutím na:

   i) všetky aktíva podporujúce procesy s veľkým a kritickým vplyvom na celú Úniu s posúdením možného vplyvu na cezhraničné toky elektriny v prípade kompromitácie daného aktíva;

   ii) možné kybernetické hrozby so zreteľom na kybernetické hrozby identifikované v najnovšej komplexnej správe o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny uvedenej v článku 23 a hrozby pre dodávateľské reťazce;

   iii) zraniteľnosti vrátane zraniteľností v pôvodných systémoch;

   iv) možné scenáre kybernetických útokov vrátane kybernetických útokov, ktoré ovplyvňujú prevádzkovú bezpečnosť elektrizačnej sústavy a narúšajú cezhraničné toky elektriny;

   v) príslušné hodnotenia a posúdenia rizík vykonané na úrovni Únie vrátane koordinovaných posúdení rizík kritických dodávateľských reťazcov v súlade s článkom 22 smernice (EÚ) 2022/2555 a

   vi) existujúce zavedené kontroly;

b) zanalyzuje pravdepodobnosť a dôsledky kybernetickobezpečnostných rizík identifikovaných podľa písmena a) a určí úroveň kybernetickobezpečnostných rizík pomocou matice vplyvu rizika, ktorá sa používa na posudzovanie kybernetickobezpečnostných rizík v metodikách posudzovania kybernetickobezpečnostných rizík na úrovni Únie, na regionálnej úrovni a na úrovni členských štátov, ako ich vypracovali PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ v súlade s článkom 19 ods. 2;

c) klasifikuje aktíva podľa možných dôsledkov v prípade kompromitácie kybernetickej bezpečnosti a určí zónu veľkého vplyvu a zónu kritického vplyvu na základe týchto krokov:

   i) v prípade všetkých procesov, na ktoré sa vzťahuje posúdenie kybernetickobezpečnostných rizík, vykoná posúdenie vplyvu na obchodnú činnosť pomocou ECII;

   ii) klasifikuje proces ako proces s veľkým alebo kritickým vplyvom, ak príslušný ECII presahuje prahovú hodnotu veľkého, resp. kritického vplyvu;

   iii) určí všetky aktíva s veľkým vplyvom a aktíva s kritickým vplyvom potrebné pre procesy s veľkým, resp. kritickým vplyvom;

   iv) vymedzí zónu veľkého vplyvu a zónu kritického vplyvu, ktoré obsahujú všetky aktíva s veľkým a kritickým vplyvom, aby bolo možné kontrolovať prístup do týchto zón;

d) vyhodnotí kybernetickobezpečnostné riziká stanovením ich priorít prostredníctvom kritérií hodnotenia rizík a kritérií akceptácie rizík uvedených v odseku 3 písm. b).

5. Vo fáze ošetrenia kybernetickobezpečnostných rizík každý subjekt s veľkým a kritickým vplyvom vypracuje plán na zmiernenie rizík na úrovni subjektu, v ktorom vyberie možnosti ošetrenia rizík vhodné na riadenie týchto rizík a identifikuje zostávajúce riziká.

6. Vo fáze akceptácie kybernetickobezpečnostných rizík sa každý subjekt s veľkým a kritickým vplyvom rozhodne, či bude akceptovať zostávajúce riziko, na základe kritérií akceptácie rizík stanovených v odseku 3 písm. b).

7. Každý subjekt s veľkým a kritickým vplyvom zapíše aktíva identifikované v odseku 1 do inventára aktív. Tento inventár aktív nie je súčasťou správy o posúdení rizík.

8. Príslušný orgán môže počas inšpekcií skontrolovať aktíva v inventári.

Článok 27

Podávanie správ o posudzovaní rizík na úrovni subjektu

Každý subjekt s veľkým a kritickým vplyvom do 12 mesiacov od informovania subjektov s veľkým a kritickým vplyvom podľa článku 24 ods. 6 a potom každé tri roky predloží príslušnému orgánu správu obsahujúcu tieto informácie:

1. zoznam kontrol vybraných do plánu na zmiernenie rizík na úrovni subjektu podľa článku 26 ods. 5 s aktuálnym stavom vykonávania každej kontroly;

2. v prípade každého procesu s veľkým alebo kritickým vplyvom na celú Úniu odhad rizika ohrozenia dôvernosti, integrity a dostupnosti informácií a príslušných aktív. Odhad tohto rizika sa uvádza v súlade s maticou vplyvu rizika uvedenou v článku 19 ods. 2;

3. zoznam poskytovateľov kritických služieb IKT v rámci jeho procesov s kritickým vplyvom.

KAPITOLA III

SPOLOČNÝ RÁMEC PRE KYBERNETICKÚ BEZPEČNOSŤ V ODVETVÍ ELEKTRICKEJ ENERGIE

Článok 28

Zloženie, fungovanie a preskúmanie spoločného rámca pre kybernetickú bezpečnosť v odvetví elektrickej energie

1. Spoločný rámec pre kybernetickú bezpečnosť v odvetví elektrickej energie tvoria tieto kontroly a systém riadenia kybernetickej bezpečnosti:

a) minimálne kontroly kybernetickej bezpečnosti vypracované v súlade s článkom 29;

b) pokročilé kontroly kybernetickej bezpečnosti vypracované v súlade s článkom 29;

c) matica mapovania vypracovaná v súlade s článkom 34, ktorou sa mapujú kontroly uvedené v písmenách a) a b) z hľadiska vybraných európskych a medzinárodných noriem a vnútroštátnych právnych alebo regulačných rámcov;

d) systém riadenia kybernetickej bezpečnosti zavedený podľa článku *32*.

2. Všetky subjekty s veľkým vplyvom uplatňujú minimálne kontroly kybernetickej bezpečnosti podľa odseku 1 písm. a) v rámci svojej zóny veľkého vplyvu.

3. Všetky subjekty s kritickým vplyvom uplatňujú pokročilé kontroly kybernetickej bezpečnosti podľa odseku 1 písm. b) v rámci svojej zóny kritického vplyvu.

4. Do siedmich mesiacov od predloženia prvého návrhu správy o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 4 sa spoločný rámec pre kybernetickú bezpečnosť v odvetví elektrickej energie uvedený v odseku 1 doplní o minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci vypracované podľa článku 33.

Článok 29

Minimálne a pokročilé kontroly kybernetickej bezpečnosti

1. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ vypracujú do siedmich mesiacov od predloženia prvého návrhu správy o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 4 návrh minimálnych a pokročilých kontrol kybernetickej bezpečnosti.

2. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ do šiestich mesiacov od vypracovania jednotlivých správ o regionálnom posúdení kybernetickobezpečnostných rizík podľa článku 21 ods. 2 predložia príslušnému orgánu návrh zmeny minimálnych a pokročilých kontrol kybernetickej bezpečnosti. Návrh sa vypracuje v súlade s článkom 8 ods. 10 a zohľadnia sa v ňom riziká identifikované v regionálnom posúdení rizík.

3. Minimálne a pokročilé kontroly kybernetickej bezpečnosti musia byť overiteľné na základe účasti na vnútroštátnom systéme overovania v súlade s postupom stanoveným v článku 31 alebo podrobením nezávislým bezpečnostným auditom tretej strany vykonaným v súlade s požiadavkami uvedenými v článku 25 ods. 2

4. Prvotné minimálne a pokročilé kontroly kybernetickej bezpečnosti vypracované podľa odseku 1 sú založené na rizikách, ktoré sú identifikované v správe o posúdení kybernetickobezpečnostných rizík v celej Únii uvedenej v článku 19 ods. 5 Zmenené minimálne a pokročilé kontroly kybernetickej bezpečnosti vypracované podľa odseku 2 sú založené na správe o regionálnom posúdení kybernetickobezpečnostných rizík uvedenej v článku 21 ods. 2

5. Minimálne kontroly kybernetickej bezpečnosti zahŕňajú kontroly na ochranu informácií, ktoré sa vymieňajú podľa článku 46.

6. Subjekty uvedené v článku 2 ods. 1 a identifikované ako subjekty s kritickým a veľkým vplyvom podľa článku 24 do 12 mesiacov od schválenia minimálnych a pokročilých kontrol kybernetickej bezpečnosti podľa článku 8 ods. 5 alebo po každej aktualizácii podľa článku 8 ods. 10 uplatňujú počas vypracovania plánu na zmiernenie rizík na úrovni subjektu podľa článku 26 ods. 5 minimálne kontroly kybernetickej bezpečnosti v rámci zóny veľkého vplyvu a pokročilé kontroly kybernetickej bezpečnosti v rámci zóny kritického vplyvu.

Článok 30

Výnimky z minimálnych a pokročilých kontrol kybernetickej bezpečnosti

1. Subjekty uvedené v článku 2 ods. 1 môžu požiadať relevantný príslušný orgán o udelenie výnimky z povinnosti uplatňovať minimálne a pokročilé kontroly kybernetickej bezpečnosti uvedené v článku 29 ods. 6 Príslušný orgán môže udeliť takúto výnimku na základe jedného z týchto dôvodov:

a) za výnimočných okolností, ak subjekt vie preukázať, že náklady na zavedenie primeraných kontrol kybernetickej bezpečnosti výrazne prevyšujú prínosy. Agentúra ACER a ENTSO pre elektrinu v spolupráci so subjektom DSO môžu na pomoc subjektom spoločne vypracovať usmernenia k odhadovaniu nákladov na kontroly kybernetickej bezpečnosti;

b) ak subjekt predloží plán ošetrenia rizík na úrovni subjektu, ktorým sa zmierňujú kybernetickobezpečnostné riziká pomocou alternatívnych kontrol na úroveň, ktorá je prijateľná v súlade s kritériami akceptácie rizík uvedenými v článku 26 ods. 3 písm. b).

2. Každý príslušný orgán do troch mesiacov od doručenia žiadosti uvedenej v odseku 1 rozhodne, či sa má udeliť výnimka z minimálnych a pokročilých kontrol kybernetickej bezpečnosti. Výnimky z minimálnych alebo pokročilých kontrol kybernetickej bezpečnosti sa udeľujú maximálne na tri roky s možnosťou predĺženia.

3. Agregované a anonymizované informácie o udelených výnimkách sa uvedú ako príloha ku komplexnej správe o posúdení kybernetickobezpečnostných rizík cezhraničných tokov elektriny uvedenej v článku 23. ENTSO pre elektrinu a subjekt PDS EÚ podľa potreby tento zoznam spoločne aktualizujú.

Článok 31

Overovanie spoločného rámca pre kybernetickú bezpečnosť v odvetví elektrickej energie

1. Každý subjekt s kritickým vplyvom identifikovaný v súlade s článkom 24 ods. 1 musí byť najneskôr 24 mesiacov od prijatia kontrol uvedených v článku 28 ods. 1 písm. a), b) a c) a od zavedenia systému riadenia kybernetickej bezpečnosti uvedeného v písmene d) predmetného článku schopný na žiadosť príslušného orgánu preukázať, že dodržiava systém riadenia kybernetickej bezpečnosti a minimálne alebo pokročilé kontroly kybernetickej bezpečnosti.

2. Každý subjekt s kritickým vplyvom si splní povinnosť uvedenú v odseku 1 tým, že sa podrobí nezávislým bezpečnostným auditom tretej strany v súlade s požiadavkami uvedenými v článku 25 ods. 2 alebo sa zúčastní na vnútroštátnom systéme overovania v súlade s článkom 25 ods. 1

3. Overenie, či subjekt s kritickým vplyvom dodržiava systém riadenia kybernetickej bezpečnosti, a minimálne alebo pokročilé kontroly kybernetickej bezpečnosti sa vzťahujú na všetky aktíva nachádzajúce sa v zóne kritického vplyvu subjektu s kritickým vplyvom.

4. Overenie, či subjekt s kritickým vplyvom dodržiava systém riadenia kybernetickej bezpečnosti, a minimálne alebo pokročilé kontroly kybernetickej bezpečnosti sa pravidelne opakujú najneskôr 36 mesiacov od skončenia prvého overenia a potom každé tri roky.

5. Každý subjekt s kritickým vplyvom určený v súlade s článkom 24 preukáže, že dodržiava kontroly uvedené v článku 28 ods. 1 písm. a), b) a c) a zaviedol systém riadenia kybernetickej bezpečnosti uvedený v písmene d) predmetného článku, tak, že príslušnému orgánu predloží správu o výsledku overenia dodržiavania súladu.

Článok 32

Systém riadenia kybernetickej bezpečnosti

1. Každý subjekt s veľkým vplyvom a subjekt s kritickým vplyvom do 24 mesiacov od dátumu, keď ho príslušný orgán v súlade s článkom 24 ods. 6 informoval, že bol identifikovaný ako subjekt s veľkým alebo kritickým vplyvom, zavedie systém riadenia kybernetickej bezpečnosti a následne ho každé tri roky preskúma s cieľom:

a) určiť rozsah systému riadenia kybernetickej bezpečnosti s ohľadom na rozhrania a závislosti vo vzťahu s inými subjektmi;

b) zabezpečiť, aby bol celý jeho vrcholový manažment informovaný o príslušných právnych povinnostiach a aktívne prispieval k vykonávaniu systému riadenia kybernetickej bezpečnosti prostredníctvom včasných rozhodnutí a pohotových reakcií;

c) zabezpečiť dostupnosť zdrojov potrebných pre systém riadenia kybernetickej bezpečnosti;

d) zaviesť politiku kybernetickej bezpečnosti, ktorá sa zdokumentuje a oznámi v rámci subjektu a stranám ovplyvneným bezpečnostnými rizikami;

e) prideliť a oznámiť zodpovednosti za úlohy súvisiace s kybernetickou bezpečnosťou;

f) vykonávať riadenie kybernetickobezpečnostných rizík na úrovni subjektu v zmysle článku 26;

g) určiť a poskytnúť zdroje potrebné na vykonávanie, údržbu a sústavné zlepšovanie systému riadenia kybernetickej bezpečnosti pri zohľadnení potrebnej odbornej spôsobilosti a informovanosti o zdrojoch kybernetickej bezpečnosti;

h) určiť internú a externú komunikáciu, ktorá je relevantná pre kybernetickú bezpečnosť;

i) vytvárať, aktualizovať a kontrolovať zdokumentované informácie týkajúce sa systému riadenia kybernetickej bezpečnosti;

j) vyhodnocovať výkonnosť a účinnosť systému riadenia kybernetickej bezpečnosti;

k) v plánovaných intervaloch vykonávať interné audity, aby sa zabezpečilo účinné vykonávanie a údržba systému riadenia kybernetickej bezpečnosti;

l) v plánovaných intervaloch preskúmať vykonávanie systému riadenia kybernetickej bezpečnosti a kontrolovať a napraviť nesúlad zdrojov a činností so zásadami, s postupmi a usmerneniami v systéme riadenia kybernetickej bezpečnosti.

2. Do pôsobnosti systému riadenia kybernetickej bezpečnosti patria všetky aktíva v rámci zóny veľkého vplyvu a zóny kritického vplyvu subjektu s veľkým a kritickým vplyvom.

3. Príslušné orgány podporujú uplatňovanie európskych alebo medzinárodných noriem a špecifikácií týkajúcich sa systémov riadenia a súvisiacich s bezpečnosťou sietí a informačných systémov, pričom neukladajú povinnosť používať určitý typ technológie ani ju nediskriminujú.

Článok 33

Minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci

1. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ vypracujú do siedmich mesiacov od predloženia prvého návrhu správy o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 4 návrh minimálnych a pokročilých kontrol kybernetickej bezpečnosti v dodávateľskom reťazci, ktorými sa zmierňujú riziká dodávateľského reťazca identifikované v posúdeniach kybernetickobezpečnostných rizík v celej Únii a ktoré dopĺňajú minimálne a pokročilé kontroly kybernetickej bezpečnosti vypracované podľa článku 29. Minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci sa vypracujú spolu s minimálnymi a pokročilými kontrolami kybernetickej bezpečnosti podľa článku 29. Minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci sa vzťahujú na celý životný cyklus všetkých produktov IKT, služieb IKT a procesov IKT v rámci zóny veľkého vplyvu a zóny kritického vplyvu subjektu s veľkým alebo kritickým vplyvom. Pri vypracúvaní návrhu minimálnych a pokročilých kontrol kybernetickej bezpečnosti v dodávateľskom reťazci sa uskutočňujú konzultácie so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

2. Minimálne kontroly kybernetickej bezpečnosti v dodávateľskom reťazci pozostávajú z kontrol vzťahujúcich sa na subjekty s veľkým a kritickým vplyvom, ktoré:

a) zahŕňajú odporúčania k obstarávaniu produktov IKT, služieb IKT a procesov IKT s uvedením špecifikácií kybernetickej bezpečnosti a obsahujúce prinajmenšom tieto prvky:

   i) previerky osôb zamerané na zamestnancov dodávateľa, ktorí sú zapojení do dodávateľského reťazca a narábajú s citlivými informáciami alebo majú prístup k aktívam s veľkým alebo kritickým vplyvom daného subjektu. Previerky osôb môžu zahŕňať overenie totožnosti a minulosti zamestnancov alebo zmluvných dodávateľov subjektu v súlade s vnútroštátnymi právnymi predpismi a postupmi a s príslušnými a uplatniteľnými právnymi predpismi Únie vrátane nariadenia (EÚ) 2016/679 a smernice Európskeho parlamentu a Rady (EÚ) 2016/680 ([18]). Previerky osôb musia byť primerané a prísne obmedzené na to, čo je nevyhnutné. Vykonávajú sa výlučne na účely hodnotenia potenciálneho bezpečnostného rizika pre dotknutý subjekt. Musia byť primerané obchodným požiadavkám, stupňu utajenia informácií, ku ktorým má byť poskytnutý prístup, a vnímaným rizikám a môže ich vykonávať samotný subjekt, externá spoločnosť vykonávajúca preverenie alebo prostredníctvom odsúhlasenia vládneho orgánu;

   ii) procesy bezpečného a kontrolovaného návrhu, vývoja a výroby produktov IKT, služieb IKT a procesov IKT podporujúce navrhovanie a vývoj produktov IKT, služieb IKT a procesov IKT, ktoré zahŕňajú primerané technické opatrenia na zaistenie kybernetickej bezpečnosti;

   iii) návrh sietí a informačných systémov, v ktorých sa zariadenia nepovažujú za dôveryhodné ani vtedy, keď sa nachádzajú v zabezpečenej zóne, a v ktorých sa vyžaduje overenie každej prijatej žiadosti a uplatňuje sa princíp minimálneho privilégia;

   iv) prístup dodávateľa k aktívam subjektu;

([18]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4.5.2016, s. 89).

v) zmluvné záväzky dodávateľa chrániť citlivé informácie subjektu a obmedziť prístup k nim;

vi) podkladové špecifikácie obstarávania kybernetickej bezpečnosti pre subdodávateľov dodávateľa;

vii) vysledovateľnosť uplatňovania špecifikácií kybernetickej bezpečnosti od vývoja cez výrobu až po dodanie produktov IKT, služieb IKT alebo procesov IKT;

viii) podporu bezpečnostných aktualizácií počas celého životného cyklu produktov IKT, služieb IKT alebo procesov IKT;

ix) právo na audit kybernetickej bezpečnosti v procesoch návrhu, vývoja a výroby dodávateľa a

x) posúdenie rizikového profilu dodávateľa;

b) vyžadujú, aby takéto subjekty pri uzatváraní zmlúv s dodávateľmi, spolupracujúcimi partnermi a inými stranami v dodávateľskom reťazci zohľadňovali odporúčania týkajúce sa obstarávania uvedené v písmene a), a to pri bežných dodávkach produktov IKT, služieb IKT a procesov IKT, ako aj pri nežiaducich udalostiach a okolnostiach, ako je vypovedanie zmluvy a jej prenos v prípade nedbanlivosti zmluvného partnera;

c) vyžadujú, aby takéto subjekty zohľadňovali výsledky príslušných koordinovaných posúdení bezpečnostných rizík v kritických dodávateľských reťazcoch vykonaných v súlade s článkom 22 ods. 1 smernice (EÚ) 2022/2555;

d) zahŕňajú kritériá na výber dodávateľov a uzatváranie zmlúv s dodávateľmi, ktorí dokážu splniť špecifikácie kybernetickej bezpečnosti uvedené v písmene a) a ktorí majú úroveň kybernetickej bezpečnosti primeranú kybernetickobezpečnostným rizikám produktu IKT, služby IKT alebo procesov IKT, ktoré dodávateľ dodáva;

e) zahŕňajú kritériá na diverzifikáciu zdrojov dodávok produktov IKT, služieb IKT a procesov IKT a znižujú riziko odkázanosti na určitého dodávateľa;

f) zahŕňajú kritériá na pravidelné monitorovanie, preskúmanie alebo audit špecifikácií kybernetickej bezpečnosti interných prevádzkových procesov dodávateľa počas celého životného cyklu každého produktu IKT, služby IKT a procesu IKT.

3. Pokiaľ ide o špecifikácie kybernetickej bezpečnosti v odporúčaniach týkajúcich sa obstarávania kybernetickej bezpečnosti uvedených v odseku 2 písm. a), subjekty s veľkým alebo kritickým vplyvom uplatňujú zásady obstarávania podľa smernice Európskeho parlamentu a Rady 2014/24/EÚ ([19]) v súlade s článkom 35 ods. 4 alebo vymedzia vlastné špecifikácie na základe výsledkov posúdenia kybernetickobezpečnostných rizík na úrovni subjektu.

4. Pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci zahŕňajú kontroly vzťahujúce sa na subjekty s kritickým vplyvom s cieľom počas obstarávania overiť, či produkty IKT, služby IKT a procesy IKT, ktoré sa budú používať ako aktíva s kritickým vplyvom, spĺňajú špecifikácie kybernetickej bezpečnosti. Produkt IKT, služba IKT alebo proces IKT sa overí buď prostredníctvom európskeho systému certifikácie kybernetickej bezpečnosti uvedeného v článku 31, alebo prostredníctvom overovacích činností, ktoré si subjekt sám vyberie a zorganizuje. Hĺbka a rozsah overovacích činností musia byť dostatočné na to, aby poskytli záruku, že produkt IKT, službu IKT alebo proces IKT možno použiť na zmiernenie rizík identifikovaných v posúdení rizík na úrovni subjektu. Subjekt s kritickým vplyvom zdokumentuje kroky prijaté na zníženie identifikovaných rizík.

5. Minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci sa vzťahujú na obstarávanie príslušných produktov IKT, služieb IKT a procesov IKT. Minimálne a pokročilé kontroly kybernetickej bezpečnosti v dodávateľskom reťazci sa vzťahujú na procesy obstarávania v subjektoch identifikovaných ako subjekty s kritickým a veľkým vplyvom podľa článku 24, ktoré sa začnú šesť mesiacov od prijatia alebo aktualizácie minimálnych a pokročilých kontrol kybernetickej bezpečnosti uvedených v článku 29.

([19]) Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

6. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ do šiestich mesiacov od vypracovania jednotlivých správ o regionálnom posúdení kybernetickobezpečnostných rizík podľa článku 21 ods. 2 predložia príslušnému orgánu návrh zmeny minimálnych a pokročilých kontrol kybernetickej bezpečnosti v dodávateľskom reťazci. Návrh sa vypracuje v súlade s článkom 8 ods. 10 a zohľadnia sa v ňom riziká identifikované v regionálnom posúdení rizík.

Článok 34

Matica mapovania na účely kontroly kybernetickej bezpečnosti v odvetví elektrickej energie z hľadiska noriem

1. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ a po konzultácii s agentúrou ENISA do siedmich mesiacov od predloženia prvého návrhu správy o posúdení kybernetickobezpečnostných rizík v celej Únii podľa článku 19 ods. 4 vypracujú návrh matice na mapovanie kontrol stanovených v článku 28 ods. 1 písm. a) a b) z hľadiska vybraných európskych a medzinárodných noriem, ako aj príslušných technických špecifikácií (ďalej len „matica mapovania“). ENTSO pre elektrinu a subjekt PDS EÚ zdokumentujú rovnocennosť rôznych kontrol s kontrolami stanovenými v článku 28 ods. 1 písm. a) a b).

2. Príslušné orgány môžu poskytnúť ENTSO pre elektrinu a subjektu PDS EÚ mapovanie kontrol uvedených v článku 28 ods. 1 písm. a) a b) s odkazom na súvisiace vnútroštátne právne predpisy alebo regulačné rámce vrátane príslušných vnútroštátnych noriem členských štátov podľa článku 25 smernice (EÚ) 2022/2555. Ak príslušný orgán členského štátu poskytne takéto mapovanie, ENTSO pre elektrinu a subjekt PDS EÚ začlenia toto vnútroštátne mapovanie do matice mapovania.

3. PPS s pomocou ENTSO pre elektrinu, v spolupráci so subjektom PDS EÚ a po konzultácii s agentúrou ENISA do šiestich mesiacov od vypracovania jednotlivých správ o regionálnom posúdení kybernetickobezpečnostných rizík podľa článku 21 ods. 2 predložia príslušnému orgánu návrh zmeny matice mapovania. Návrh sa vypracuje v súlade s článkom 8 ods. 10 a zohľadnia sa v ňom riziká identifikované v regionálnom posúdení rizík.

KAPITOLA IV

ODPORÚČANIA TÝKAJÚCE SA OBSTARÁVANIA KYBERNETICKEJ BEZPEČNOSTI

Článok 35

Odporúčania týkajúce sa obstarávania kybernetickej bezpečnosti

1. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ vypracujú v pracovnom programe, ktorý sa stanoví a aktualizuje vždy po prijatí správy o regionálnom posúdení kybernetickobezpečnostných rizík, súbory nezáväzných odporúčaní týkajúcich sa obstarávania kybernetickej bezpečnosti, ktoré môžu subjekty s veľkým a kritickým vplyvom použiť ako základ pri obstarávaní produktov IKT, služieb IKT a procesov IKT nachádzajúcich sa v rámci hranice veľkého vplyvu a perimetra kritického vplyvu. Tento pracovný program zahŕňa:

a) opis a klasifikáciu typov produktov IKT, služieb IKT a procesov IKT, ktoré používajú subjekty s veľkým a kritickým vplyvom v rámci hranice veľkého vplyvu a perimetra kritického vplyvu;

b) zoznam typov produktov IKT, služieb IKT a procesov IKT, v súvislosti s ktorými sa vypracuje súbor nezáväzných odporúčaní v oblasti kybernetickej bezpečnosti na základe príslušných správ o regionálnom posúdení kybernetickobezpečnostných rizík a na základe priorít subjektov s veľkým a kritickým vplyvom.

2. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do šiestich mesiacov od prijatia alebo aktualizácie správy o regionálnom posúdení kybernetickobezpečnostných rizík predloží agentúre ACER zhrnutie uvedeného pracovného programu.

3. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ sa usilujú zabezpečiť, aby nezáväzné odporúčania týkajúce sa obstarávania kybernetickej bezpečnosti vypracované na základe príslušného regionálneho posúdenia kybernetickobezpečnostných rizík boli podobné alebo porovnateľné v rôznych regiónoch prevádzky sústavy. Súbory odporúčaní týkajúcich sa obstarávania kybernetickej bezpečnosti sa vzťahujú prinajmenšom na špecifikácie uvedené v článku 33 ods. 2 písm. a). Ak je to možné, špecifikácie sa vyberajú z európskych a medzinárodných noriem.

4. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ zabezpečia, aby súbory odporúčaní týkajúcich sa obstarávania kybernetickej bezpečnosti:

a) boli v súlade so zásadami obstarávania podľa smernice 2014/24/EÚ a

b) boli kompatibilné s najnovšími dostupnými európskymi systémami certifikácie kybernetickej bezpečnosti vzťahujúcimi sa na daný produkt IKT, službu IKT alebo proces IKT a aby ich zohľadňovali.

Článok 36

Usmernenie k používaniu európskych systémov certifikácie kybernetickej bezpečnosti pri obstarávaní produktov IKT, služieb IKT a procesov IKT

1. Nezáväzné odporúčania týkajúce sa obstarávania kybernetickej bezpečnosti vypracované podľa článku 35 môžu zahŕňať odvetvové usmernenia k používaniu európskych systémov certifikácie kybernetickej bezpečnosti vždy, keď je k dispozícii vhodný systém pre typ produktu IKT, služby IKT alebo procesu IKT, ktoré používajú subjekty s kritickým vplyvom, pričom tým nie je dotknutý rámec pre zavádzanie európskych systémov certifikácie kybernetickej bezpečnosti podľa článku 46 nariadenia (EÚ) 2019/881.

2. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ úzko spolupracujú s agentúrou ENISA pri poskytovaní odvetvových usmernení, ktoré sú súčasťou nezáväzných odporúčaní týkajúcich sa obstarávania kybernetickej bezpečnosti podľa odseku 1.

KAPITOLA V

INFORMAČNÉ TOKY, KYBERNETICKÉ ÚTOKY A KRÍZOVÉ RIADENIE

Článok 37

Pravidlá výmeny informácií

1. Ak príslušný orgán získa informácie, ktoré sa týkajú kybernetického útoku podliehajúceho oznamovacej povinnosti, tento príslušný orgán:

a) bez zbytočného odkladu a najneskôr do 24 hodín od získania informácií posúdi úroveň dôvernosti týchto informácií a informuje subjekt o výsledku svojho posúdenia;

b) sa pokúsi nájsť akýkoľvek iný podobný kybernetický útok v Únii oznámený iným príslušným orgánom, aby porovnal informácie získané v súvislosti s predmetným kybernetickým útokom podliehajúcim oznamovacej povinnosti s informáciami poskytnutými v súvislosti s inými kybernetickými útokmi a obohatil existujúce informácie, posilnil a koordinoval reakcie v oblasti kybernetickej bezpečnosti;

c) zodpovedá za odstránenie obchodných tajomstiev a anonymizáciu informácií v súlade s príslušnými vnútroštátnymi pravidlami a pravidlami Únie;

d) bez zbytočného odkladu a najneskôr do 24 hodín od získania informácií o kybernetickom útoku podliehajúcom oznamovacej povinnosti poskytne informácie vnútroštátnym jednotným kontaktným miestam, jednotkám CSIRT a všetkým príslušným orgánom určeným podľa článku 4 v iných členských štátoch a pravidelne poskytuje týmto orgánom alebo subjektom aktualizované informácie;

e) po anonymizácii a odstránení obchodných tajomstiev podľa odseku 1 písm. c) bez zbytočného odkladu a najneskôr do 24 hodín od získania informácií podľa odseku 1 písm. a) postúpi informácie o kybernetickom útoku subjektom s kritickým a veľkým vplyvom vo svojom členskom štáte a pravidelne im poskytuje aktualizované informácie, ktoré týmto subjektom umožnia účinne organizovať svoju obranu;

f) môže požiadať oznamujúci subjekt s veľkým alebo kritickým vplyvom, aby ďalej bezpečným spôsobom postúpil informácie o kybernetickom útoku podliehajúcom oznamovacej povinnosti ostatným subjektom, ktoré ním môžu byť zasiahnuté, s cieľom vytvoriť situačné povedomie v odvetví elektroenergetiky a predísť naplneniu rizika, ktoré môže prerásť do cezhraničného kybernetickobezpečnostného incidentu v odvetví elektroenergetiky;

g) po anonymizácii a odstránení obchodných tajomstiev predloží agentúre ENISA súhrnnú správu s informáciami o kybernetickom útoku.

2. Ak sa jednotka CSIRT dozvie o neopravenej aktívne zneužívanej zraniteľnosti:

a) bezodkladne o tom informuje agentúru ENISA prostredníctvom vhodného zabezpečeného kanála na výmenu informácií, pokiaľ nie je v iných právnych predpisoch Únie stanovené inak;

b) poskytne dotknutému subjektu podporu, aby od výrobcu alebo poskytovateľa dostal účinné, koordinované a rýchle riešenie neopravenej aktívne zneužívanej zraniteľnosti alebo účinné a efektívne opatrenia na jej zmiernenie;

c) poskytne dostupné informácie dodávateľovi, a ak je to možné, požiada výrobcu alebo poskytovateľa, aby identifikoval zoznam jednotiek CSIRT v členských štátoch, ktorých sa neopravená aktívne zneužívaná zraniteľnosť týka, a ktoré musia byť informované;

d) poskytne dostupné informácie jednotkám CSIRT identifikovaným podľa predchádzajúceho písmena na základe potreby poznať;

e) poskytne stratégie a opatrenia na zmiernenie oznámených neopravených aktívne zneužívaných zraniteľností, ak takéto stratégie a opatrenia existujú.

3. Ak sa príslušný orgán dozvie o neopravenej aktívne zneužívanej zraniteľnosti:

a) v koordinácii s jednotkami CSIRT vo svojom členskom štáte poskytne stratégie a opatrenia na zmiernenie oznámených neopravených aktívne zneužívaných zraniteľností, ak takéto stratégie a opatrenia existujú;

b) poskytne informácie jednotkám CSIRT v členskom štáte, v ktorom bola neopravená aktívne zneužívaná zraniteľnosť oznámená.

4. Ak sa príslušný orgán dozvie o neopravenej zraniteľnosti, pričom zatiaľ neexistujú dôkazy o jej aktívnom zneužívaní, bez zbytočného odkladu koordinuje svoj postup s jednotkou CSIRT na účely koordinovaného zverejňovania zraniteľností, ako sa stanovuje v článku 12 ods. 1 smernice (EÚ) 2022/2555.

5. Ak jednotka CSIRT získa informácie týkajúce sa kybernetických hrozieb od jedného alebo viacerých subjektov s veľkým alebo kritickým vplyvom podľa článku 38 ods. 6, bez zbytočného odkladu a najneskôr do štyroch hodín od ich získania postúpi tieto informácie alebo akékoľvek iné informácie dôležité z hľadiska prevencie, odhaľovania, reakcie alebo zmiernenia súvisiaceho rizika subjektom s kritickým a veľkým vplyvom vo svojom členskom štáte a prípadne všetkým dotknutým jednotkám CSIRT a svojmu vnútroštátnemu jednotnému kontaktnému miestu.

6. Ak sa príslušný orgán dozvie o informáciách týkajúcich sa kybernetických hrozieb od jedného alebo viacerých subjektov s veľkým alebo kritickým vplyvom, postúpi tieto informácie jednotke CSIRT na účely odseku 5.

7. Príslušné orgány môžu na základe dohody medzi dotknutými príslušnými orgánmi úplne alebo čiastočne delegovať povinnosti podľa odsekov 3 a 4 týkajúce sa jedného alebo viacerých subjektov s veľkým alebo kritickým vplyvom, ktoré pôsobia vo viac než jednom členskom štáte, na iný príslušný orgán v jednom z týchto členských štátov.

8. PPS s pomocou ENTSO pre elektrinu a v spolupráci so subjektom PDS EÚ do 13. júna 2025 vypracujú metodiku klasifikačnej stupnice kybernetických útokov. PPS s pomocou ENTSO pre elektrinu a subjektu PDS EÚ môžu požiadať príslušné orgány, aby konzultovali s agentúrou ENISA, a môžu svoje príslušné orgány zodpovedné za kybernetickú bezpečnosť požiadať o pomoc pri vypracovaní takejto klasifikačnej stupnice. V metodike sa stanoví klasifikácia závažnosti kybernetického útoku na základe piatich úrovní, pričom dve najvyššie úrovne sú „vysoká“ a „kritická“. Klasifikácia vychádza z posúdenia týchto parametrov:

a) potenciálny vplyv vzhľadom na exponované aktíva a zóny, ktorý sa určí v súlade s článkom 26 ods. 4 písm. c), a

b) závažnosť kybernetického útoku.

9. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ vykoná do 13. júna 2026 štúdiu uskutočniteľnosti s cieľom posúdiť možnosti a potrebné finančné náklady spojené s vytvorením spoločného nástroja umožňujúceho všetkým subjektom vymieňať si informácie s príslušnými vnútroštátnymi orgánmi.

10. Štúdia uskutočniteľnosti sa zaoberá tým, ako možno dosiahnuť, aby takýto spoločný nástroj:

a) podporoval subjekty s kritickým a veľkým vplyvom prostredníctvom relevantných informácií týkajúcich sa bezpečnosti pri prevádzke cezhraničných tokov elektriny, ako sú napríklad správy o kybernetických útokoch v takmer reálnom čase, včasné varovania týkajúce sa otázok kybernetickej bezpečnosti a nezverejnených zraniteľností zariadení používaných v elektrizačnej sústave;

b) bol udržiavaný vo vhodnom a vysoko dôveryhodnom prostredí;

c) umožňoval zhromažďovanie údajov od subjektov s kritickým a veľkým vplyvom a uľahčoval odstránenie dôverných informácií a anonymizáciu údajov a ich rýchle postúpenie subjektom s kritickým a veľkým vplyvom.

11. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ:

a) sa pri posudzovaní uskutočniteľnosti radí s agentúrou ENISA a so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, s vnútroštátnymi jednotnými kontaktnými miestami a so zástupcami hlavných zainteresovaných strán;

b) predloží výsledky štúdie uskutočniteľnosti agentúre ACER a skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

12. ENTSO pre elektrinu môže v spolupráci so subjektom PDS EÚ analyzovať a uľahčovať iniciatívy navrhované subjektmi s kritickým a veľkým vplyvom na účely vyhodnocovania a testovania takýchto nástrojov na výmenu informácií.

Článok 38

Úloha subjektov s veľkým a kritickým vplyvom, pokiaľ ide o výmenu informácií

1. Každý subjekt s veľkým a kritickým vplyvom:

a) v prípade všetkých aktív vo svojej zóne kybernetickej bezpečnosti určenej podľa článku 26 ods. 4 písm. c) vytvorí prinajmenšom spôsobilosti operačného centra kybernetickej bezpečnosti s cieľom:

   i) zabezpečiť, aby príslušné siete a informačné systémy a aplikácie poskytovali bezpečnostné protokoly na monitorovanie bezpečnosti s cieľom umožniť odhaľovanie anomálií a zhromažďovanie informácií o kybernetických útokoch;

   ii) vykonávať monitorovanie bezpečnosti vrátane odhaľovania narušení a posudzovania zraniteľností sietí a informačných systémov;

   iii) analyzovať a podľa potreby prijať všetky opatrenia, ktoré sú v rámci jeho zodpovednosti a spôsobilosti potrebné na ochranu daného subjektu;

   iv) podieľať sa na zhromažďovaní a výmene informácií opísaných v tomto článku;

b) má právo obstarávať všetky tieto spôsobilosti alebo ich časti podľa písmena a) prostredníctvom poskytovateľov riadených bezpečnostných služieb. Subjekty s kritickým a veľkým vplyvom sú naďalej zodpovedné za poskytovateľov riadených bezpečnostných služieb a dohliadajú na ich úsilie;

c) určí jednotné kontaktné miesto na úrovni subjektu na účely výmeny informácií.

2. Agentúra ENISA môže v rámci úlohy vymedzenej v článku 6 ods. 2 nariadenia (EÚ) 2019/881 vydať nezáväzné usmernenie týkajúce sa vytvárania takýchto spôsobilostí alebo využívania subdodávateľských zmlúv s poskytovateľmi riadených bezpečnostných služieb.

3. Každý subjekt s kritickým a veľkým vplyvom poskytne relevantné informácie týkajúce sa kybernetického útoku podliehajúceho oznamovacej povinnosti svojim jednotkám CSIRT a príslušnému orgánu bez zbytočného odkladu a najneskôr do štyroch hodín od zistenia, že incident podlieha oznamovacej povinnosti.

4. Informácie týkajúce sa kybernetického útoku sa považujú za podliehajúce oznamovacej povinnosti, ak zasiahnutý subjekt vyhodnotí závažnosť kybernetického útoku na úrovni v rozsahu od „vysoká“ po „kritická“ na základe metodiky určenia klasifikačnej stupnice kybernetických útokov podľa článku 37 ods. 8 Jednotné kontaktné miesto na úrovni subjektu určené podľa odseku 1 písm. c) oznámi klasifikáciu incidentu.

5. Ak subjekty s kritickým a veľkým vplyvom oznámia relevantné informácie týkajúce sa neopravených aktívne zneužívaných zraniteľností jednotke CSIRT, jednotka CSIRT môže tieto informácie postúpiť svojmu príslušnému orgánu. S ohľadom na úroveň citlivosti oznamovaných informácií môže jednotka CSIRT tieto informácie neposkytnúť alebo ich postúpenie odložiť, ak na to existujú opodstatnené dôvody súvisiace s kybernetickou bezpečnosťou.

6. Každý subjekt s kritickým a veľkým vplyvom bez zbytočného odkladu poskytne svojim jednotkám CSIRT všetky informácie týkajúce sa kybernetickej hrozby podliehajúcej oznamovacej povinnosti, ktorá môže mať cezhraničný vplyv. Informácie týkajúce sa kybernetickej hrozby sa považujú za podliehajúce oznamovacej povinnosti, ak je splnená aspoň jedna z týchto podmienok:

a) ide o informácie, ktoré sú relevantné pre iné subjekty s kritickým a veľkým vplyvom z hľadiska prevencie a odhaľovania rizika, reakcie naň alebo zmierňovania jeho vplyvu;

b) identifikované techniky, taktiky a postupy použité v súvislosti s útokom vedú k informáciám, ako sú kompromitované URL alebo IP adresy, hašovacie znaky alebo akékoľvek iné atribúty, pomocou ktorých možno zistiť kontext a súvislosti útoku;

c) kybernetickú hrozbu možno ďalej posúdiť a dať do súvislosti s ďalšími informáciami, ktoré poskytnú poskytovatelia služieb alebo tretie strany, na ktoré sa toto nariadenie nevzťahuje.

7. Každý subjekt s kritickým a s veľkým vplyvom pri výmene informácií podľa tohto článku uvedie:

a) že informácie sa predkladajú v súlade s týmto nariadením;

b) či sa informácie týkajú:

i) kybernetického útoku podliehajúceho oznamovacej povinnosti uvedeného v odseku 3;

ii) neopravených aktívne zneužívaných zraniteľností, ktoré nie sú verejne známe, uvedených v odseku 4;

iii) kybernetickej hrozby podliehajúcej oznamovacej povinnosti uvedenej v odseku 5;

c) v prípade kybernetického útoku podliehajúceho oznamovacej povinnosti úroveň kybernetického útoku podľa metodiky určenia klasifikačnej stupnice kybernetických útokov uvedenej v článku 37 ods. 8 a informácie vedúce k tejto klasifikácii vrátane prinajmenšom závažnosti kybernetického útoku.

8. Ak subjekt s kritickým alebo s veľkým vplyvom oznámi významný incident podľa článku 23 smernice (EÚ) 2022/2555 a oznámenie tohto incidentu podľa uvedeného článku obsahuje relevantné informácie požadované podľa odseku 3 tohto článku, oznámenie subjektu podľa článku 23 ods. 1 uvedenej smernice predstavuje oznámenie informácií podľa odseku 3 tohto článku.

9. Každý subjekt s kritickým a veľkým vplyvom vykonáva oznámenia svojmu príslušnému orgánu alebo jednotke CSIRT, pričom jasne identifikuje konkrétne informácie, ktoré sa s príslušným orgánom alebo jednotkou CSIRT vymieňajú len v prípadoch, keď by výmena informácií mohla byť zdrojom kybernetického útoku. Každý subjekt s kritickým a veľkým vplyvom má právo predložiť príslušnej jednotke CSIRT verziu informácií, ktorá nemá dôverný charakter.

Článok 39

Odhaľovanie kybernetických útokov a spracovanie súvisiacich informácií

1. Subjekty s kritickým a veľkým vplyvom vyvinú potrebné spôsobilosti na riešenie odhalených kybernetických útokov, a to s potrebnou podporou príslušného orgánu, ENTSO pre elektrinu a subjektu PDS EÚ. Subjekty s kritickým a veľkým vplyvom môže podporovať jednotka CSIRT určená v príslušnom členskom štáte v rámci úlohy, ktorou sú jednotky CSIRT poverené podľa článku 11 ods. 5 písm. a) smernice (EÚ) 2022/2555. Subjekty s kritickým a veľkým vplyvom zavedú účinné procesy na identifikáciu, klasifikáciu kybernetických útokov, ktoré ovplyvnia alebo môžu ovplyvniť cezhraničné toky elektriny, a reakciu na ne s cieľom minimalizovať ich vplyv.

2. Ak má kybernetický útok vplyv na cezhraničné toky elektriny, jednotné kontaktné miesta na úrovni zasiahnutých subjektov s kritickým vplyvom a veľkým vplyvom spolupracujú v záujme vzájomnej výmeny informácií, pričom ich koordinuje príslušný orgán členského štátu, v ktorom bol kybernetický útok oznámený ako prvý.

3. Subjekty s kritickým vplyvom a subjekty s veľkým vplyvom:

a) zabezpečia, aby ich vlastné jednotné kontaktné miesto na úrovni subjektu malo, na základe potreby poznať, prístup k informáciám, ktoré tieto subjekty získali od vnútroštátneho jednotného kontaktného miesta prostredníctvom svojho príslušného orgánu;

b) pokiaľ tak ešte neurobili podľa článku 3 ods. 4 smernice (EÚ) 2022/2555, oznámia príslušnému orgánu členského štátu, v ktorom sú usadené, a vnútroštátnemu jednotnému kontaktnému miestu zoznam svojich jednotných kontaktných miest pre kybernetickú bezpečnosť na úrovni subjektu:

   i) od ktorých môže daný príslušný orgán a vnútroštátne jednotné kontaktné miesto očakávať poskytovanie informácií o kybernetických útokoch podliehajúcich oznamovacej povinnosti;

   ii) ktorým príslušné orgány a vnútroštátne jednotné kontaktné miesta môžu byť povinné poskytovať informácie;

c) stanovia postupy riadenia kybernetických útokov v prípade kybernetických útokov vrátane funkcií a zodpovedností, úloh a reakcií na základe pozorovateľného vývoja kybernetického útoku v rámci zóny veľkého vplyvu a zóny kritického vplyvu;

d) aspoň raz ročne otestujú postupy celkového riadenia kybernetických útokov tak, že otestujú aspoň jeden scenár, ktorý priamo alebo nepriamo ovplyvňuje cezhraničné toky elektriny. Tento každoročný test môžu vykonávať subjekty s kritickým vplyvom a subjekty s veľkým vplyvom počas pravidelných cvičení uvedených v článku 43. Ako každoročný test plánu reakcie na kybernetický útok môže slúžiť akákoľvek činnosť reakcie na skutočný kybernetický útok s dôsledkom klasifikovaným najmenej na 2. stupni podľa metodiky určenia klasifikačnej stupnice kybernetických útokov uvedenej v článku 37 ods. 8, ktorej hlavná príčina súvisí s kybernetickou bezpečnosťou.

4. Úlohy uvedené v odseku 1 môžu členské štáty delegovať aj na regionálne koordinačné centrá v súlade s článkom 37 ods. 2 nariadenia (EÚ) 2019/943.

Článok 40

Krízové riadenie

1. Ak príslušný orgán zistí, že kríza dodávok elektriny súvisí s kybernetickým útokom, ktorý má vplyv na viac než jeden členský štát, príslušné orgány z dotknutých členských štátov, príslušné orgány zodpovedné za kybernetickú bezpečnosť, príslušné orgány pre pripravenosť na riziká a orgány pre riadenie kybernetických kríz NIS zo zasiahnutých členských štátov spoločne vytvoria *ad hoc* skupinu pre cezhraničnú krízovú koordináciu.

2. *Ad hoc* skupina pre cezhraničnú krízovú koordináciu:

a) koordinuje efektívne vyhľadávanie všetkých relevantných informácií o kybernetickej bezpečnosti a ich ďalšie šírenie subjektom zapojeným do procesu krízového riadenia;

b) organizuje komunikáciu medzi všetkými subjektmi dotknutými krízou a príslušnými orgánmi s cieľom obmedziť prekrývanie sa a zvýšiť efektívnosť analýz a technických reakcií v záujme odstránenia súbežných kríz dodávok elektriny, ktorých hlavná príčina súvisí s kybernetickou bezpečnosťou;

c) v spolupráci s príslušnými jednotkami CSIRT poskytuje subjektom, ktoré sú incidentom dotknuté, potrebné odborné znalosti vrátane prevádzkového poradenstva pri vykonávaní možných zmierňujúcich opatrení;

d) informuje Komisiu a skupinu pre koordináciu v oblasti elektrickej energie o stave incidentu a pravidelne im poskytuje aktuálne informácie v súlade so zásadami ochrany stanovenými v článku 46;

e) požiada o poradenstvo relevantné orgány, agentúry alebo subjekty, ktoré by mohli byť nápomocné pri zmierňovaní krízy dodávok elektriny.

3. Ak sa kybernetický útok kvalifikuje alebo sa očakáva, že bude kvalifikovaný ako rozsiahly kybernetickobezpečnostný incident, *ad hoc* skupina pre cezhraničnú krízovú koordináciu bezodkladne informuje vnútroštátne orgány pre riadenie kybernetických kríz v súlade s článkom 9 ods. 1 smernice (EÚ) 2022/2555 v členských štátoch zasiahnutých incidentom, ako aj Komisiu a sieť EU-CyCLONe. V takejto situácii *ad hoc* skupina pre cezhraničnú krízovú koordináciu podporuje sieť EU-CyCLONe, pokiaľ ide o odvetvové špecifiká.

4. Subjekty s kritickým a veľkým vplyvom vyvinú a musia mať k dispozícii spôsobilosti, interné usmernenia, plány pripravenosti a zamestnancov, aby sa mohli podieľať na odhaľovaní a zmierňovaní cezhraničných kríz. Subjekt s kritickým alebo veľkým vplyvom, ktorý je dotknutý súbežnou krízou dodávok elektriny, vyšetrí hlavnú príčinu takejto krízy v spolupráci so svojím príslušným orgánom s cieľom určiť, do akej miery kríza súvisí s kybernetickým útokom.

5. Úlohy uvedené v odseku 4 môžu členské štáty delegovať aj na regionálne koordinačné centrá v súlade s článkom 37 ods. 2 nariadenia (EÚ) 2019/943.

Článok 41

Plány krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti

1. Agentúra ACER v úzkej spolupráci s agentúrou ENISA, ENTSO pre elektrinu, so subjektom PDS EÚ, s príslušnými orgánmi zodpovednými za kybernetickú bezpečnosť, príslušnými orgánmi, príslušnými orgánmi pre pripravenosť na riziká, národnými regulačnými orgánmi a vnútroštátnymi orgánmi pre riadenie kybernetických kríz NIS do 24 mesiacov po tom, ako bola agentúre ACER predložená správa o posúdení rizík v celej Únii, vypracuje plán krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti pre odvetvie elektroenergetiky na úrovni Únie.

2. Každý príslušný orgán do 12 mesiacov po tom, ako agentúra ACER vypracovala plán krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti pre odvetvie elektroenergetiky na úrovni Únie podľa odseku 1, vypracuje národný plán krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti pre cezhraničné toky elektriny, pričom zohľadní plán krízového riadenia v oblasti kybernetickej bezpečnosti na úrovni Únie a národný plán pripravenosti na riziká zostavený v súlade s článkom 10 nariadenia (EÚ) 2019/941. Tento plán musí byť v súlade s plánom reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy podľa článku 9 ods. 4 smernice (EÚ) 2022/2555. Príslušný orgán koordinuje svoj postup so subjektmi s kritickým a veľkým vplyvom a s príslušnými orgánmi zodpovednými za pripravenosť na riziká vo svojom členskom štáte.

3. Národný plán reakcie na rozsiahle kybernetickobezpečnostné incidenty a krízy požadovaný podľa článku 9 ods. 4 smernice (EÚ) 2022/2555 sa považuje za národný plán krízového riadenia v oblasti kybernetickej bezpečnosti podľa tohto článku, ak obsahuje ustanovenia o krízovom riadení a reakcii na krízy v súvislosti s cezhraničnými tokmi elektriny.

4. Úlohy vymenované v odsekoch 1 a 2 môžu členské štáty delegovať aj na regionálne koordinačné centrá v súlade s článkom 37 ods. 2 nariadenia (EÚ) 2019/943.

5. Subjekty s kritickým a vplyvom zabezpečia, aby ich procesy krízového riadenia súvisiace s kybernetickou bezpečnosťou:

a) zahŕňali kompatibilné postupy riešenia cezhraničných kybernetickobezpečnostných incidentov v zmysle článku 6 bode 8 smernice (EÚ) 2022/2555 formálne začlenené do ich plánov krízového riadenia;

b) boli súčasťou všeobecných činností krízového riadenia.

6. Subjekty s kritickým a veľkým vplyvom do 12 mesiacov od informovania subjektov s veľkým a kritickým vplyvom podľa článku 24 ods. 6 a potom každé tri roky vypracujú plán krízového riadenia na úrovni subjektu pre prípad krízy súvisiacej s kybernetickou bezpečnosťou, ktorý začlenia do svojho všeobecného plánu krízového riadenia. Tento plán obsahuje aspoň tieto údaje:

a) pravidlá vyhlásenia krízy, ako sú stanovené v článku 14 ods. 2 a 3 nariadenia (EÚ) 2019/941;

b) jasné úlohy a zodpovednosti za krízové riadenie vrátane úlohy ostatných relevantných subjektov s kritickým a veľkým vplyvom;

c) aktuálne kontaktné údaje, ako aj pravidlá komunikácie a výmeny informácií počas krízovej situácie vrátane prepojenia na jednotky CSIRT.

7. Opatrenia krízového riadenia podľa článku 21 ods. 2 písm. c) smernice (EÚ) 2022/2555 sa považujú za plán krízového riadenia na úrovni subjektu pre odvetvie elektroenergetiky podľa tohto článku, ak zahŕňajú všetky požiadavky uvedené v odseku 6.

8. Plány krízového riadenia sa testujú počas kybernetickobezpečnostných cvičení uvedených v článkoch 43, 44 a 45.

9. Subjekty s kritickým a veľkým vplyvom zahrnú svoje plány krízového riadenia na úrovni subjektu do svojich plánov na zabezpečenie kontinuity činností v prípade procesov s kritickým vplyvom a procesov s veľkým vplyvom. Plány krízového riadenia na úrovni subjektu zahŕňajú:

a) procesy závislé od dostupnosti, integrity a spoľahlivosti IT služieb;

b) všetky lokality relevantné pre zabezpečenie kontinuity činností vrátane lokalít pre hardvér a softvér;

c) všetky interné úlohy a zodpovednosti súvisiace s procesmi kontinuity činností.

10. Subjekty s kritickým a veľkým vplyvom aktualizujú svoje plány krízového riadenia na úrovni subjektu aspoň každé tri roky a vždy, keď je to potrebné.

11. Agentúra ACER aktualizuje plán krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti pre odvetvie elektroenergetiky na úrovni Únie vypracovaný podľa odseku 1 aspoň každé tri roky a vždy, keď je to potrebné.

12. Každý príslušný orgán aktualizuje národný plán krízového riadenia a reakcie na krízu v oblasti kybernetickej bezpečnosti pre cezhraničné toky elektriny vypracovaný podľa odseku 2 aspoň každé tri roky a vždy, keď je to potrebné.

13. Subjekty s kritickým a veľkým vplyvom testujú svoje plány na zabezpečenie kontinuity činností aspoň každé tri roky alebo po významných zmenách v procese s kritickým vplyvom. Výsledok testov plánu na zabezpečenie kontinuity činností sa zdokumentuje. Subjekty s kritickým a veľkým vplyvom môžu testovanie svojho plánu na zabezpečenie kontinuity činností zahrnúť do kybernetickobezpečnostných cvičení.

14. Subjekty s kritickým a veľkým vplyvom aktualizujú svoj plán na zabezpečenie kontinuity činností vždy, keď je to potrebné, a najmenej každé tri roky, pričom zohľadnia výsledok testu.

15. Ak sa pri testovaní zistia v pláne na zabezpečenie kontinuity činností nedostatky, subjekt s kritickým a veľkým vplyvom odstráni tieto nedostatky do 180 kalendárnych dní od testovania a vykoná nový test, aby poskytol dôkaz o účinnosti nápravných opatrení.

16. Ak subjekt s kritickým alebo veľkým vplyvom nedokáže nedostatky odstrániť do 180 kalendárnych dní, uvedie dôvody v správe, ktorú predloží svojmu príslušnému orgánu v súlade s článkom 27.

Článok 42

Spôsobilosti včasného varovania v oblasti kybernetickej bezpečnosti pre odvetvie elektroenergetiky

1. Príslušné orgány spolupracujú s agentúrou ENISA pri rozvíjaní spôsobilostí včasného varovania v oblasti kybernetickej bezpečnosti elektrizačnej sústavy (ECEAC) v rámci pomoci členským štátom podľa článku 6 ods. 2 a článku 7 nariadenia (EÚ) 2019/881.

2. Spôsobilosti včasného varovania v oblasti kybernetickej bezpečnosti elektrizačnej sústavy umožňujú agentúre ENISA pri plnení úloh uvedených v článku 7 ods. 7 nariadenia (EÚ) 2019/881:

a) zhromažďovať informácie na základe dobrovoľnej výmeny od:

   i) jednotiek CSIRT, príslušných orgánov;

   ii) subjektov uvedených v článku 2 tohto nariadenia;

   iii) akéhokoľvek iného subjektu, ktorý sa chce dobrovoľne zapojiť do výmeny relevantných informácií;

b) posudzovať a klasifikovať zhromaždené informácie;

c) posudzovať informácie, ku ktorým má prístup agentúra ENISA, na účely identifikácie podmienok kybernetického rizika a príslušných ukazovateľov týkajúcich sa aspektov cezhraničných tokov elektriny;

d) identifikovať podmienky a ukazovatele, ktoré často súvisia s kybernetickými útokmi v odvetví elektroenergetiky;

e) určiť, či sa má vykonať ďalšia analýza a preventívne opatrenia, prostredníctvom posúdenia a identifikácie rizikových faktorov;

f) informovať príslušné orgány o identifikovaných rizikách a odporúčaných preventívnych opatreniach špecifických pre dotknuté subjekty;

g) informovať všetky príslušné subjekty uvedené v článku 2 o výsledkoch posúdenia informácií v súlade s písmenami b), c) a d) tohto odseku;

h) pravidelne uvádzať relevantné informácie v správe o situačnom povedomí vydanej v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881;

i) ak je to možné, odvodiť zo zhromaždených informácií použiteľné údaje, ktoré naznačujú potenciálne narušenie bezpečnosti alebo kybernetický útok (ďalej len „ukazovatele narušenia“).

3. Jednotky CSIRT bezodkladne postúpia informácie získané od agentúry ENISA dotknutým subjektom v rámci svojich úloh vymedzených v článku 11 ods. 3 písm. b) smernice (EÚ) 2022/2555.

4. Agentúra ACER monitoruje účinnosť spôsobilostí včasného varovania v oblasti kybernetickej bezpečnosti elektrizačnej sústavy. Agentúra ENISA pomáha agentúre ACER poskytovaním všetkých potrebných informácií podľa článku 6 ods. 2 a článku 7 ods. 1 nariadenia (EÚ) 2019/881. Analýza tejto monitorovacej činnosti je súčasťou monitorovania podľa článku 12 tohto nariadenia.

KAPITOLA VI

RÁMEC KYBERNETICKOBEZPEČNÝCH CVIČENÍ V ODVETVÍ ELEKTRICKEJ ENERGIE

Článok 43

Kybernetickobezpečnostné cvičenia na úrovni subjektu a na úrovni členské štátu

1. Každý subjekt s kritickým vplyvom do 31. decembra roka po informovaní subjektov s kritickým vplyvom a následne každé tri roky vykoná kybernetickobezpečnostné cvičenie vrátane jedného alebo viacerých scenárov s kybernetickými útokmi, ktoré priamo alebo nepriamo ovplyvňujú cezhraničné toky elektriny a súvisia s rizikami identifikovanými v posúdení kybernetickobezpečnostných rizík na úrovni členského štátu a na úrovni subjektu v súlade s článkom 20 a článkom 27.

2. Odchylne od odseku 1 môže príslušný orgán pre pripravenosť na riziká po konzultácii s príslušným orgánom a príslušným orgánom pre riadenie kybernetických kríz určeným alebo zriadeným podľa článku 9 smernice (EÚ) 2022/2555 rozhodnúť, že namiesto vykonania kybernetickobezpečnostného cvičenia na úrovni subjektu zorganizuje kybernetickobezpečnostné cvičenie na úrovni členského štátu, ako sa uvádza v odseku 1. V tejto súvislosti príslušný orgán informuje:

a) všetky subjekty s kritickým vplyvom vo svojom členskom štáte, národné regulačné orgány, jednotky CSIRT a príslušný orgán zodpovedný za kybernetickú bezpečnosť najneskôr do 30. júna roka, ktorý predchádza kybernetickobezpečnostnému cvičeniu na úrovni subjektu;

b) každý subjekt, ktorý sa zúčastní na kybernetickobezpečnostnom cvičení na úrovni členského štátu, najneskôr šesť mesiacov pred jeho uskutočnením.

3. Príslušný orgán pre pripravenosť na riziká s technickou podporou svojich jednotiek CSIRT zorganizuje kybernetickobezpečnostné cvičenie opísané v odseku 2 na úrovni členského štátu nezávisle od iného kybernetickobezpečnostného cvičenia v danom členskom štáte alebo v rámci takéhoto iného cvičenia. Aby bolo možné tieto cvičenia zoskupiť, môže príslušný orgán pre pripravenosť na riziká odložiť kybernetickobezpečnostné cvičenie na úrovni členského štátu uvedené v odseku 1 o jeden rok.

4. Kybernetickobezpečnostné cvičenia na úrovni subjektu a na úrovni členského štátu musia byť v súlade s vnútroštátnymi rámcami krízového riadenia kybernetickej bezpečnosti v súlade s článkom 9 ods. 4 písm. d) smernice (EÚ) 2022/2555.

5. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do 31. decembra 2026 a potom každé tri roky sprístupní vzor scenárov cvičení na vykonávanie kybernetickobezpečnostných cvičení na úrovni subjektu a úrovni členského štátu uvedených v odseku 1. V tomto vzore sa zohľadňujú výsledky najnovších posúdení kybernetickobezpečnostných rizík na úrovni subjektu a úrovni členského štátu a obsahuje kľúčové kritériá úspešnosti. ENTSO pre elektrinu a subjekt PDS EÚ zapoja do vypracovania tohto vzoru agentúru ACER a agentúru ENISA.

Článok 44

Regionálne alebo medziregionálne kybernetickobezpečnostné cvičenia

1. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do 31. decembra 2029 a potom každé tri roky organizuje v každom regióne prevádzky sústavy regionálne kybernetickobezpečnostné cvičenie. Na regionálnom kybernetickobezpečnostnom cvičení sa zúčastňujú subjekty s kritickým vplyvom v regióne prevádzky sústavy. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ môže v rovnakom časovom rámci namiesto regionálneho kybernetickobezpečnostného cvičenia zorganizovať medziregionálne kybernetickobezpečnostné cvičenie vo viac než jednom regióne prevádzky sústavy. Pri tomto cvičení by sa mali zohľadniť ostatné existujúce posúdenia kybernetickobezpečnostných rizík a scenáre vypracované na úrovni Únie.

2. Agentúra ENISA podporuje ENTSO pre elektrinu a subjekt PDS EÚ pri príprave a organizácii kybernetickobezpečnostného cvičenia na regionálnej alebo medziregionálnej úrovni.

3. ENTSO pre elektrinu v koordinácii so subjektom PDS EÚ informuje subjekty s kritickým vplyvom, ktoré sa majú zúčastniť na regionálnom alebo medziregionálnom kybernetickobezpečnostnom cvičení, šesť mesiacov pred jeho uskutočnením.

4. Organizátor pravidelného kybernetickobezpečnostného cvičenia na úrovni Únie podľa článku 7 ods. 5 nariadenia (EÚ) 2019/881 alebo akéhokoľvek povinného kybernetickobezpečnostného cvičenia týkajúceho sa odvetvia elektroenergetiky v rámci tej istej geografickej zóny môže vyzvať na účasť ENTSO pre elektrinu a subjekt PDS EÚ. V takýchto prípadoch sa povinnosť uvedená v odseku 1 neuplatňuje za predpokladu, že na tom istom cvičení sa zúčastnia všetky subjekty s kritickým vplyvom v danom regióne prevádzky sústavy.

5. Ak sa ENTSO pre elektrinu a subjekt PDS EÚ zúčastnia na kybernetickobezpečnostnom cvičení uvedenom v odseku 4, môžu odložiť regionálne alebo medziregionálne kybernetickobezpečnostné cvičenie uvedené v odseku 1 o jeden rok.

6. ENTSO pre elektrinu v koordinácii so subjektom PDS EÚ do 31. decembra 2027 a každé tri roky po tomto dátume sprístupní vzor cvičení na vykonávanie regionálnych a medziregionálnych kybernetickobezpečnostných cvičení. V tomto vzore sa zohľadňujú výsledky najnovších posúdení kybernetickobezpečnostných rizík na regionálnej úrovni a obsahuje kľúčové kritériá úspešnosti. V súvislosti s organizovaním a vykonávaním regionálnych a medziregionálnych kybernetickobezpečnostných cvičení sa ENTSO pre elektrinu radí s Komisiou a môže požiadať o poradenstvo agentúru ACER, agentúru ENISA a Spoločné výskumné centrum.

Článok 45

Výsledky kybernetickobezpečnostných cvičení na úrovni subjektu, členského štátu, regionálnej alebo medziregionálnej úrovni

1. Poskytovatelia kritických služieb sa na žiadosť subjektu s kritickým vplyvom zúčastnia na kybernetickobezpečnostných cvičeniach uvedených v článku 43 ods. 1 a 2 a článku 44 ods. 1, ak subjektu s kritickým vplyvom poskytujú služby v oblasti zodpovedajúcej rozsahu predmetného kybernetickobezpečnostného cvičenia.

2. Organizátori kybernetickobezpečnostných cvičení uvedených v článku 43 ods. 1 a 2 a článku 44 ods. 1 na základe poradenstva od agentúry ENISA, ak oň požiadajú, a v súlade s článkom 7 ods. 5 nariadenia (EÚ) 2019/881 zanalyzujú a dokončia predmetné kybernetickobezpečnostné cvičenie vypracovaním správy obsahujúcej zhrnutie získaných poznatkov, ktorá je určená všetkým účastníkom. Správa musí obsahovať:

a) scenáre cvičení, správy zo stretnutí, hlavné stanoviská, úspechy a získané poznatky na ktorejkoľvek úrovni hodnotového reťazca elektrickej energie;

b) informácie o tom, či boli splnené kľúčové kritériá úspešnosti;

c) zoznam odporúčaní pre subjekty zúčastnené na predmetnom kybernetickobezpečnostnom cvičení týkajúcich sa nápravy, úpravy alebo zmeny krízových kybernetickobezpečnostných procesov, postupov, súvisiacich modelov riadenia a akýchkoľvek existujúcich zmluvných záväzkov s poskytovateľmi kritických služieb.

3. Organizátori kybernetickobezpečnostných cvičení uvedených v článku 43 ods. 1 a 2 a článku 44 ods. 1 poskytnú informácie o výsledku predmetného kybernetickobezpečnostného cvičenia jednotkám CSIRT, skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti alebo sieti EU-CyCLONe, ak o to požiadajú. Organizátori poskytnú každému subjektu zúčastnenému na cvičení informácie uvedené v odseku 2 písm. a) a b) tohto článku. Organizátori poskytnú zoznam odporúčaní uvedených v písmene c) uvedeného odseku výlučne subjektom, ktorým sú odporúčania určené.

4. Organizátori kybernetickobezpečnostných cvičení uvedených v článku 43 ods. 1 a 2 a článku 44 ods. 1 následne pravidelne sledujú, ako subjekty zúčastnené na cvičeniach plnia odporúčania podľa odseku 2 písm. c) tohto článku.

KAPITOLA VII

OCHRANA INFORMÁCIÍ

Článok 46

Zásady ochrany vymieňaných informácií

1. Subjekty uvedené v článku 2 ods. 1 zabezpečia, aby informácie poskytované, získavané, vymieňané alebo zasielané podľa tohto nariadenia boli prístupné len na základe potreby poznať a v súlade s príslušnými pravidlami Únie a vnútroštátnymi pravidlami týkajúcimi sa bezpečnosti informácií.

2. Subjekty uvedené v článku 2 ods. 1 zabezpečia, aby sa s informáciami poskytovanými, získavanými, vymieňanými alebo zasielanými podľa tohto nariadenia primerane zaobchádzalo a aby boli vysledovateľné počas celého životného cyklu daných informácií a aby ich zverejnenie na konci životného cyklu bolo možné len po ich anonymizácii.

3. Subjekty uvedené v článku 2 ods. 1 zabezpečia, aby boli zavedené všetky potrebné ochranné opatrenia organizačnej a technickej povahy na zaistenie a ochranu dôvernosti, integrity, dostupnosti a nepopretia informácií poskytovaných, získavaných, vymieňaných alebo zasielaných podľa tohto nariadenia, a to nezávisle od použitých prostriedkov. Ochranné opatrenia musia:

a) byť primerané;

b) zohľadňovať kybernetickobezpečnostné riziká súvisiace so známymi minulými a vznikajúcimi hrozbami, ktorým môžu byť takéto informácie vystavené v kontexte tohto nariadenia;

c) v čo najväčšej miere vychádzať z vnútroštátnych, európskych alebo medzinárodných noriem a najlepších postupov;

d) byť zdokumentované.

4. Subjekty uvedené v článku 2 ods. 1 zabezpečia, aby každá osoba, ktorej je udelený prístup k informáciám poskytovaným, získavaným, vymieňaným alebo zasielaným podľa tohto nariadenia, bola informovaná o bezpečnostných pravidlách platných na úrovni subjektu a o opatreniach a postupoch týkajúcich sa ochrany informácií. Uvedené subjekty zabezpečia, aby dotknutá osoba uznala zodpovednosť za ochranu informácií podľa pokynov, ktoré dostala na informačnom stretnutí.

5. Subjekty uvedené v článku 2 ods. 1 zabezpečia, aby bol prístup k informáciám poskytovaným, získavaným, vymieňaným alebo zasielaným podľa tohto nariadenia obmedzený len na fyzické osoby:

a) ktoré sú oprávnené na prístup k týmto informáciám na základe svojich funkcií a s obmedzením na vykonávanie pridelených úloh;

b) u ktorých bol subjekt schopný posúdiť etické zásady a zásady bezúhonnosti, ako aj u ktorých neexistuje žiadny dôkaz o negatívnom výsledku previerky osôb s cieľom vyhodnotiť spoľahlivosť danej osoby v súlade s najlepšími postupmi a štandardnými bezpečnostnými požiadavkami subjektu a v prípade potreby s vnútroštátnymi zákonmi a inými právnymi predpismi.

6. Subjekty uvedené v článku 2 ods. 1 musia mať písomný súhlas fyzickej alebo právnickej osoby, ktorá informácie pôvodne vytvorila alebo poskytla, predtým, ako tieto informácie poskytnú tretej strane, ktorá nepatrí do rozsahu pôsobnosti tohto nariadenia.

7. Subjekt uvedený v článku 2 ods. 1 môže zvážiť, že pri výmene týchto informácií sa nebudú dodržiavať odseky 1 a 4 tohto článku, s cieľom predísť súbežnej kríze dodávok elektriny, ktorej hlavná príčina súvisí s kybernetickou bezpečnosťou, alebo akejkoľvek cezhraničnej kríze v rámci Únie v inom odvetví. V takomto prípade musí:

a) konzultovať s príslušným orgánom a mať od neho povolenie na výmenu takýchto informácií;

b) anonymizovať takéto informácie bez toho, aby sa stratili prvky potrebné na informovanie verejnosti o bezprostrednom a závažnom riziku pre cezhraničné toky elektriny a o možných zmierňujúcich opatreniach;

c) chrániť totožnosť pôvodcu a subjektov, ktoré spracúvajú takéto informácie podľa tohto nariadenia.

8. Odchylne od odseku 6 tohto článku môžu príslušné orgány poskytnúť informácie poskytované, získavané, vymieňané alebo zasielané podľa tohto nariadenia tretej strane, ktorá nie je uvedená v článku 2 ods. 1, bez predchádzajúceho písomného súhlasu pôvodcu informácií, ale informujú ho o tom v čo najkratšom čase. Pred sprístupnením akýchkoľvek informácií poskytovaných, získavaných, vymieňaných alebo zasielaných podľa tohto nariadenia tretej strane, ktorá nie je uvedená v článku 2 ods. 1, dotknutý príslušný orgán musí primerane zabezpečiť, aby dotknutá tretia strana poznala platné bezpečnostné pravidlá, a získať primerané uistenie, že dotknutá tretia strana dokáže chrániť získané informácie v súlade s odsekmi 1 až 5 tohto článku. Príslušný orgán anonymizuje takéto informácie bez toho, aby sa stratili prvky potrebné na informovanie verejnosti o bezprostrednom a závažnom riziku pre cezhraničné toky elektriny a o možných zmierňujúcich opatreniach a na ochranu totožnosti pôvodcu informácií. V tomto prípade tretia strana, ktorá nie je uvedená v článku 2 ods. 1, chráni získané informácie v súlade s ustanoveniami, ktoré už platia na úrovni subjektu, alebo ak to nie je možné, v súlade s ustanoveniami a pokynmi, ktoré poskytol relevantný príslušný orgán.

9. Tento článok sa nevzťahuje na subjekty, ktoré nie sú uvedené v článku 2 ods. 1 a ktorým sa poskytujú informácie podľa odseku 6 tohto článku. V tomto prípade sa uplatňuje odsek 7 tohto článku alebo príslušný orgán môže danému subjektu poskytnúť písomné ustanovenia, ktoré sa majú uplatňovať v prípadoch získania informácií podľa tohto nariadenia.

Článok 47

Dôvernosť informácií

1. Na všetky informácie poskytované, získavané, vymieňané alebo zasielané podľa tohto nariadenia sa vzťahujú podmienky služobného tajomstva stanovené v odsekoch 2 až 5 tohto článku tohto nariadenia a požiadavky stanovené v článku 65 nariadenia (EÚ) 2019/943. Všetky informácie poskytované, získavané, vymieňané alebo zasielané medzi subjektmi uvedenými v článku 2 tohto nariadenia na účely vykonávania tohto nariadenia sú chránené s ohľadom na úroveň dôvernosti informácií, ktorú uplatňuje pôvodca.

2. Povinnosť služobného tajomstva sa vzťahuje na subjekty uvedené v článku 2.

3. Príslušné orgány zodpovedné za kybernetickú bezpečnosť, národné regulačné orgány, príslušné orgány pre pripravenosť na riziká a jednotky CSIRT si vymieňajú všetky informácie potrebné na plnenie svojich úloh.

4. Všetky informácie získavané, vymieňané alebo zasielané medzi subjektmi uvedenými v článku 2 ods. 1 na účely vykonávania článku 23 musia byť anonymizované a agregované.

5. Informácie, ktoré získa akýkoľvek subjekt alebo orgán podľa tohto nariadenia pri plnení svojich povinností, sa nesmú poskytovať žiadnemu inému subjektu ani orgánu, čím nie sú dotknuté prípady, na ktoré sa vzťahujú vnútroštátne právne predpisy, iné ustanovenia tohto nariadenia alebo iné príslušné právne predpisy Únie.

6. Bez toho, aby boli dotknuté vnútroštátne právne predpisy alebo právne predpisy Únie, orgán, subjekt alebo fyzická osoba, ktorá získa informácie podľa tohto nariadenia, ich nesmie použiť na iný účel než na plnenie svojich povinností podľa tohto nariadenia.

7. Agentúra ACER po konzultácii s agentúrou ENISA, so všetkými príslušnými orgánmi, s ENTSO pre elektrinu a so subjektom PDS EÚ vydá do 13. júna 2025 usmernenia týkajúce sa mechanizmov výmeny informácií medzi všetkými subjektmi uvedenými v článku 2 ods. 1, a najmä predpokladaných komunikačných tokov a metód anonymizácie a agregovania informácií na účely vykonávania tohto článku.

8. Informácie, ktoré sú dôverné podľa pravidiel Únie a vnútroštátnych pravidiel, sa vymieňajú s Komisiou a inými relevantnými orgánmi len vtedy, ak je táto výmena potrebná na uplatňovanie tohto nariadenia. Vymieňané informácie sa obmedzujú na tie informácie, ktoré sú nevyhnutné a primerané účelu tejto výmeny. Pri výmene informácií sa zachováva dôvernosť týchto informácií a chránia sa bezpečnostné a obchodné záujmy subjektov s kritickým alebo veľkým vplyvom.

KAPITOLA VIII

ZÁVEREČNÉ USTANOVENIA

Článok 48

Dočasné ustanovenia

1. Kým nebudú schválené podmienky alebo metodiky uvedené v článku 6 ods. 2, alebo plány uvedené v článku 6 ods. 3, ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ vypracuje nezáväzné usmernenia týkajúce sa týchto záležitostí:

a) predbežného indexu vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy (ďalej len „ECII“) podľa odseku 2 tohto článku;

b) predbežného zoznamu procesov s veľkým a kritickým vplyvom na celú Úniu podľa odseku 4 tohto článku a

c) predbežného zoznamu európskych a medzinárodných noriem a kontrol, ktoré sa vyžadujú vo vnútroštátnych právnych predpisoch a ktoré sú relevantné pre aspekty kybernetickej bezpečnosti cezhraničných tokov elektriny podľa odseku 6 tohto článku.

2. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do 13. októbra 2024 vypracuje odporúčanie k predbežnému ECII. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ oznámi odporúčaný predbežný ECII príslušným orgánom.

3. Príslušné orgány na základe odporúčaného ECII do štyroch mesiacov od doručenia odporúčaného predbežného ECII alebo najneskôr do 13. februára 2025 identifikujú kandidátske subjekty s veľkým a kritickým vplyvom vo svojom členskom štáte a vypracujú predbežný zoznam subjektov s veľkým a kritickým vplyvom. Subjekty s veľkým a kritickým vplyvom identifikované v predbežnom zozname môžu dobrovoľne plniť svoje povinnosti stanovené v tomto nariadení na základe zásady predbežnej opatrnosti. Príslušné orgány do 13. marca 2025 informujú subjekty identifikované v predbežnom zozname, že boli identifikované ako subjekty s veľkým, resp. kritickým vplyvom.

4. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do 13. decembra 2024 vypracuje predbežný zoznam procesov s veľkým a kritickým vplyvom na celú Úniu. Subjekty informované podľa odseku 3, ktoré sa dobrovoľne rozhodnú plniť svoje povinnosti stanovené v tomto nariadení na základe zásady predbežnej opatrnosti, použijú predbežný zoznam procesov s veľkým a kritickým vplyvom, aby určili predbežné zóny veľkého vplyvu a kritického vplyvu a aby určili aktíva, ktoré sa majú zahrnúť do prvého posúdenia kybernetickobezpečnostných rizík na úrovni subjektu.

5. Každý príslušný orgán podľa článku 4 ods. 1 do 13. septembra 2024 poskytne ENTSO pre elektrinu a subjektu PDS EÚ zoznam svojich vnútroštátnych právnych predpisov, ktoré sú relevantné pre aspekty kybernetickej bezpečnosti cezhraničných tokov elektriny.

6. ENTSO pre elektrinu v spolupráci so subjektom PDS EÚ do 13. júna 2025 pripraví predbežný zoznam európskych a medzinárodných noriem a kontrol požadovaných vo vnútroštátnych právnych predpisoch, ktoré sú relevantné pre aspekty kybernetickej bezpečnosti cezhraničných tokov elektriny, pričom zohľadní informácie poskytnuté príslušnými orgánmi.

7. Predbežný zoznam európskych a medzinárodných noriem a kontrol obsahuje:

a) európske a medzinárodné normy a vnútroštátne právne predpisy, v ktorých sa poskytujú usmernenia k metodikám riadenia kybernetickobezpečnostných rizík na úrovni subjektu, a

b) kontroly kybernetickej bezpečnosti rovnocenné s kontrolami, ktoré majú byť súčasťou minimálnych a pokročilých kontrol kybernetickej bezpečnosti.

8. ENTSO pre elektrinu a subjekt PDS EÚ pri finalizácii predbežného zoznamu noriem zohľadnia stanoviská, ktoré poskytla agentúra ENISA a agentúra ACER. ENTSO pre elektrinu a subjekt PDS EÚ zverejnia prechodný zoznam európskych a medzinárodných noriem a kontrol na svojich webových sídlach.

9. ENTSO pre elektrinu a subjekt PDS EÚ konzultujú návrhy nezáväzných usmernení vypracovaných podľa odseku 1 s agentúrou ENISA a agentúrou ACER.

10. Do vypracovania minimálnych a pokročilých kontrol kybernetickej bezpečnosti podľa článku 29 a ich prijatia podľa článku 8 sa všetky subjekty uvedené v článku 2 ods. 1 usilujú postupne uplatňovať nezáväzné usmernenia vypracované podľa odseku 1.

Článok 49

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 11. marca 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN