2024/1366

24.5.2024

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2024/1366

ze dne 11. března 2024,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2019/943 zavedením kodexu sítě pro odvětvová pravidla pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou ([1]), zejména na čl. 59 odst. 2 písm. e) uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Řízení kybernetických bezpečnostních rizik má zásadní význam pro zachování bezpečnosti dodávek elektřiny a pro zajištění vysoké úrovně kybernetické bezpečnosti v odvětví elektroenergetiky.

(2) Digitalizace a kybernetická bezpečnost jsou rozhodující pro poskytování základních služeb, a mají proto strategický význam pro kritickou energetickou infrastrukturu.

(3) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([2]) stanoví opatření pro vysokou společnou úroveň kybernetické bezpečnosti v Unii. Nařízení Evropského parlamentu a Rady (EU) 2019/941 ([3]) doplňuje směrnici (EU) 2022/2555 tím, že zajišťuje, aby kybernetické bezpečnostní incidenty v odvětví elektroenergetiky byly náležitě označeny za riziko a aby opatření přijatá k jejich řešení byla náležitě zohledněna v plánech rizikové připravenosti. Nařízení (EU) 2019/943 doplňuje směrnici (EU) 2022/2555 a nařízení (EU) 2019/941 stanovením zvláštních pravidel pro odvětví elektřiny na úrovni Unie. Toto nařízení v přenesené pravomoci dále doplňuje ustanovení směrnice (EU) 2022/2555 týkající se odvětví energetiky, pokud jde o přeshraniční toky elektřiny.

(4) V kontextu vzájemně propojených digitalizovaných elektroenergetických systémů nelze předcházení elektroenergetických krizí souvisejících s kybernetickými útoky a řízení takových krizí považovat za výlučně vnitrostátní úkol. Měla by být plně rozvinuta efektivnější a méně nákladná opatření prostřednictvím spolupráce na regionální úrovni a na úrovni Unie. Proto je zapotřebí společný rámec pravidel a lépe koordinované postupy, aby bylo zajištěno, že členské státy a další subjekty budou moci účinně přeshraničně spolupracovat v duchu větší transparentnosti, důvěry a solidarity mezi členskými státy a příslušnými orgány odpovědnými za elektroenergetiku a kybernetickou bezpečnost.

(5) Řízení kybernetických bezpečnostních rizik v oblasti působnosti tohoto nařízení vyžaduje strukturovaný proces zahrnující mimo jiné určení rizik pro přeshraniční toky elektřiny plynoucích z kybernetických útoků, související provozní procesy a perimetry, odpovídající kontroly v oblasti kybernetické bezpečnosti a ověřovací mechanismy. Ačkoli je celý proces časově rozložen do několika let, každý jeho krok by měl přispět k vysoké společné úrovni kybernetické bezpečnosti v tomto odvětví a ke zmírnění kybernetických bezpečnostních rizik. Všichni účastníci procesu by měli vynaložit maximální úsilí, aby metodiky vypracovali a schválili co nejdříve bez zbytečného odkladu, nejpozději však ve lhůtách stanovených v tomto nařízení.

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

([2]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

([3]) Nařízení Evropského parlamentu a Rady (EU) 2019/941 ze dne 5. června 2019 o rizikové připravenosti v odvětví elektroenergetiky a o zrušení směrnice 2005/89/ES (Úř. věst. L 158, 14.6.2019, s. 1).

(6) Posouzení kybernetických bezpečnostních rizik pro celou Unii, členských států, regionů a subjektů v tomto nařízení může být omezeno na rizika vyplývající z kybernetických útoků, jak jsou definovány v nařízení Evropského parlamentu a Rady (EU) 2022/2554 ([4]), a tudíž jsou vyloučeny například fyzické útoky, přírodní katastrofy a výpadky v důsledku ztráty zařízení nebo lidských zdrojů. Na rizika v oblasti elektroenergetiky související s fyzickými útoky nebo přírodními katastrofami v rámci celé Unie nebo v rámci regionů se již vztahují jiné stávající právní předpisy Unie, včetně článku 5 nařízení (EU) 2019/941 nebo nařízení Komise (EU) 2017/1485 ([5]), kterým se stanoví rámcový pokyn pro provoz elektroenergetických přenosových soustav. Podobně i směrnice (EU) 2022/2557 ([6]) o odolnosti kritických subjektů má za cíl snížit zranitelnost a posílit fyzickou odolnost kritických subjektů a zahrnuje všechna příslušná přírodní rizika a rizika způsobená člověkem, která mohou ovlivnit poskytování základních služeb, včetně havárií, přírodních katastrof, mimořádných událostí v oblasti veřejného zdraví, jako jsou pandemie, a hybridních hrozeb nebo jiných antagonistických hrozeb, včetně teroristických trestných činů, pronikání trestné činnosti a sabotáže.

(7) Pojem „subjekty s vysokým dopadem a subjekty s kritickým dopadem“ v tomto nařízení má zásadní význam pro vymezení okruhu subjektů, na které se budou povinnosti popsané v tomto nařízení vztahovat. Cílem přístupu založeného na posouzení rizik, který je popsán v jednotlivých ustanoveních, je určit procesy, podpůrná aktiva a subjekty, které je provozují, které ovlivňují přeshraniční toky elektřiny. Tyto subjekty lze považovat za „subjekty s vysokým dopadem“ nebo „subjekty s kritickým dopadem“ podle míry dopadu možných kybernetických útoků na jejich provoz přeshraničních toků elektřiny. Článek 3 směrnice (EU) 2022/2555 stanoví pojmy základních a důležitých subjektů a kritéria pro určení subjektů těchto kategorií. Ačkoli mnohé z nich budou považovány a označeny současně za „základní“ subjekty ve smyslu článku 3 směrnice (EU) 2022/2555 a za subjekty s vysokým dopadem nebo subjekty s kritickým dopadem podle článku 24 tohoto nařízení, kritéria stanovená v tomto nařízení se týkají pouze jejich úlohy a dopadu v elektroenergetických procesech ovlivňujících přeshraniční toky bez ohledu na kritéria vymezená v článku 3 směrnice (EU) 2022/2555.

(8) Subjekty v oblasti působnosti tohoto nařízení, které jsou považovány za subjekty s vysokým dopadem nebo subjekty s kritickým dopadem podle článku 24 tohoto nařízení a podléhají povinnostem v něm stanoveným, jsou především ty subjekty, které mají přímý dopad na přeshraniční toky elektřiny v EU.

(9) Toto nařízení využívá stávající mechanismy a nástroje, které již byly zavedeny v jiných právních předpisech, s cílem zajistit efektivitu a zabránit zdvojování při dosahování cílů.

(10) Při uplatňování tohoto nařízení by členské státy, příslušné orgány a provozovatelé systémů měli brát v úvahu schválené evropské normy a technické specifikace evropských normalizačních organizací a jednat v souladu s právními předpisy Unie týkajícími se uvádění výrobků, na které se tyto právní předpisy Unie vztahují, na trh nebo do provozu.

([4]) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1).

([5]) Nařízení Komise (EU) 2017/1485 ze dne 2. srpna 2017, kterým se stanoví rámcový pokyn pro provoz elektroenergetických přenosových soustav (Úř. věst. L 220, 25.8.2017, s. 1).

([6]) Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L 333, 27.12.2022, s. 164).

(11) Aby se zmírnila kybernetická bezpečnostní rizika, je nezbytné stanovit podrobný soubor pravidel, kterými se budou řídit činnosti a spolupráce příslušných zainteresovaných subjektů, jejichž činnost se týká aspektů kybernetické bezpečnosti přeshraničních toků elektřiny, s cílem zajistit bezpečnost soustavy. Tato organizační a technická pravidla by měla zajistit, aby většina elektroenergetických incidentů, jež mají příčiny v oblasti kybernetické bezpečnosti, byla účinně řešena na provozní úrovni. Je nezbytné stanovit, co by měly příslušné zainteresované subjekty učinit, aby takovým krizím předcházely, a jaká opatření mohou přijmout, pokud by samotná pravidla provozování soustavy již nestačila. Proto je nutné stanovit společný rámec pravidel, jak předcházet souběžným elektroenergetickým krizím, jež mají příčiny v oblasti kybernetické bezpečnosti, připravovat se na tyto krize a řešit je. To přináší větší transparentnost v přípravné fázi a během souběžné elektroenergetické krize a zajišťuje, že opatření jsou spolu s příslušnými orgány pro kybernetickou bezpečnost v členských státech přijímána koordinovaně a účinně. Členské státy a příslušné subjekty by měly být povinny spolupracovat na regionální úrovni a případně na dvoustranné úrovni v duchu solidarity. Cílem této spolupráce a pravidel je dosáhnout lepší připravenosti na kybernetická bezpečnostní rizika při nižších nákladech, což je rovněž v souladu s cíli směrnice (EU) 2022/2555. Je rovněž zřejmé, že je nezbytné posílit vnitřní trh s elektřinou zvýšením důvěry mezi členskými státy, a zejména zmírněním rizika nepatřičného omezení přeshraničních toků elektřiny, čímž se sníží riziko negativních vedlejších účinků na sousední členské státy.

(12) Bezpečnost dodávek elektřiny vyžaduje účinnou spolupráci mezi členskými státy, orgány, institucemi a jinými subjekty Unie a příslušnými zainteresovanými subjekty. Klíčovou úlohu při zajišťování bezpečné, spolehlivé a účinné elektrizační soustavy v souladu s články 31 a 40 směrnice Evropského parlamentu a Rady (EU) 2019/944 ([7]) hrají provozovatelé distribučních soustav a provozovatelé přenosových soustav. Důležitou úlohu při zajišťování a sledování kybernetické bezpečnosti v rámci dodávek elektřiny mají také různé regulační orgány a další příslušné vnitrostátní orgány, a to v rámci svých úkolů, které jim ukládají směrnice (EU) 2019/944 a (EU) 2022/2555. Členské státy by měly určit stávající nebo nový subjekt jako svůj příslušný vnitrostátní orgán pro provádění tohoto nařízení s cílem zajistit transparentní a inkluzivní účast všech zúčastněných subjektů, efektivní přípravu a řádné provádění tohoto nařízení, spolupráci mezi různými příslušnými zainteresovanými subjekty a příslušnými orgány v oblasti elektroenergetiky a kybernetické bezpečnosti, jakož i usnadnit prevenci a následné hodnocení elektroenergetických krizí, jež mají příčiny v oblasti kybernetické bezpečnosti, a výměnu informací v souvislosti s těmito krizemi.

(13) Pokud subjekt s vysokým dopadem nebo subjekt s kritickým dopadem poskytuje služby v jednom nebo více členských státech nebo má sídlo či jinou provozovnu nebo zástupce v členském státě, ale jeho síť a informační systémy se nacházejí v jednom nebo více jiných členských státech, měly by tyto členské státy vyzvat své příslušné orgány, aby v případě potřeby vyvinuly co největší úsilí o vzájemnou spolupráci a pomoc.

(14) Členské státy by měly zajistit, aby příslušné orgány měly ve vztahu k subjektům s vysokým dopadem a k subjektům s kritickým dopadem nezbytné pravomoci k prosazování dodržování tohoto nařízení. Tyto pravomoci by měly příslušným orgánům umožnit provádět kontroly na místě a dohled na dálku. Může jít o namátkové kontroly, provádění pravidelných auditů, cílené bezpečnostní audity na základě posouzení rizik nebo dostupných informací souvisejících s riziky a bezpečnostní prověrky založené na objektivních, nediskriminačních, spravedlivých a transparentních kritériích pro posouzení rizik, které zahrnují vyžádání informací nezbytných k posouzení opatření kybernetické bezpečnosti přijatých daným subjektem. Tyto informace by měly zahrnovat zdokumentované zásady kybernetické bezpečnosti, přístupové údaje, dokumenty nebo veškeré informace nezbytné pro plnění jejich úkolů v oblasti dohledu a důkazy o provádění politik kybernetické bezpečnosti, například výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podklady.

([7]) Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU (Úř. věst. L 158, 14.6.2019, s. 125).

(15) Aby se předešlo mezerám mezi povinnostmi v oblasti řízení kybernetických bezpečnostních rizik uloženými subjektům s vysokým dopadem a subjektům s kritickým dopadem nebo jejich zdvojování, měly by vnitrostátní orgány podle směrnice (EU) 2022/2555 a příslušné orgány podle tohoto nařízení spolupracovat v souvislosti s prováděním opatření k řízení kybernetických bezpečnostních rizik a dohledem nad dodržováním těchto opatření na vnitrostátní úrovni. Splnění požadavků na řízení kybernetických bezpečnostních rizik, jež stanoví toto nařízení, ze strany subjektu by mohly příslušné orgány podle směrnice (EU) 2022/2555 považovat za zajištění souladu s odpovídajícími požadavky stanovenými v uvedené směrnici, a naopak.

(16) Společný přístup k prevenci a řízení souběžných elektroenergetických krizí vyžaduje, aby členské státy společně chápaly, co je souběžná elektroenergetická krize a kdy je kybernetický útok jejím důležitým faktorem. Zejména by měla být usnadněna koordinace mezi členskými státy a příslušnými subjekty za účelem řešení situace, kdy existuje nebo bezprostředně hrozí potenciální riziko významného nedostatku elektřiny nebo nemožnosti dodávat elektřinu zákazníkům, a to v důsledku kybernetického útoku.

(17) V 1. bodě odůvodnění nařízení Evropského parlamentu a Rady (EU) 2019/881 ([8]) se uznává zásadní úloha sítí a informačních systémů a sítí a služeb elektronických komunikací při udržování v chodu ekonomiky v klíčových odvětvích, jako je energetika, a ve 44. bodě odůvodnění se vysvětluje, že Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) by měla spolupracovat s Agenturou Evropské unie pro spolupráci energetických regulačních orgánů (dále jen „ACER“).

(18) Nařízení (EU) 2019/943 ukládá provozovatelům přenosových soustav a provozovatelům distribučních soustav konkrétní povinnosti v oblasti kybernetické bezpečnosti. Jejich evropská sdružení, konkrétně Evropská síť provozovatelů elektroenergetických přenosových soustav (dále jen „ENTSO pro elektřinu“) a Evropský subjekt pro provozovatele distribučních soustav (dále jen „subjekt EU DSO“), podporují podle článků 30 a 55 uvedeného nařízení kybernetickou bezpečnost ve spolupráci s příslušnými orgány a regulovanými subjekty.

(19) Společný přístup k prevenci a řízení souběžných elektroenergetických krizí, jež mají příčiny v oblasti kybernetické bezpečnosti, rovněž vyžaduje, aby všechny příslušné zainteresované subjekty používaly harmonizované metody a definice pro určení rizik souvisejících s kybernetickou bezpečností dodávek elektřiny. Vyžaduje rovněž, aby bylo možné účinně porovnávat, jak dobře si v této oblasti vedou ony a jejich sousedé. Proto je nezbytné stanovit procesy a úlohy a povinnosti pro vypracování a aktualizaci metodik řízení rizik, stupnic klasifikace incidentů a opatření kybernetické bezpečnosti přizpůsobených kybernetickým bezpečnostním rizikům, jež mají dopad na přeshraniční toky elektřiny.

(20) Členské státy prostřednictvím příslušného orgánu určeného pro účely tohoto nařízení odpovídají za určení subjektů, které splňují kritéria pro zařazení do kategorie subjektů s vysokým dopadem a subjektů s kritickým dopadem. Aby se v tomto ohledu odstranily rozdíly mezi členskými státy a zajistila se právní jistota, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti všech příslušných subjektů, měl by být stanoven soubor kritérií, který určí subjekty spadající do oblasti působnosti tohoto nařízení. Tento soubor kritérií by měl být vymezen a pravidelně aktualizován prostřednictvím procesu vypracování a přijetí podmínek a metodik stanovených v tomto nařízení.

(21) Ustanoveními tohoto nařízení by nemělo být dotčeno právo Unie, které stanoví zvláštní pravidla pro certifikaci produktů informačních a komunikačních technologií (dále jen „IKT“), služeb IKT a procesů IKT, a zejména by jimi nemělo být dotčeno nařízení (EU) 2019/881, pokud jde o rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti. V souvislosti s tímto nařízením by produkty IKT měly zahrnovat také technická zařízení a software, které umožňují přímou interakci s elektrotechnickou sítí, zejména průmyslové řídicí systémy, které lze použít pro přenos, distribuci a výrobu energie, jakož i pro sběr a předávání souvisejících informací. Tato ustanovení by měla zajistit, aby produkty IKT, služby IKT a procesy IKT, na něž mají být zadávány zakázky, splňovaly příslušné bezpečnostní cíle uvedené v článku 51 nařízení (EU) 2019/881.

([8]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

(22) Nedávné kybernetické útoky ukazují, že subjekty se stále častěji stávají terčem útoků na dodavatelský řetězec. Takové útoky na dodavatelský řetězec mají dopad nejen na jednotlivé subjekty v této oblasti působnosti, ale mohou mít také kaskádový účinek v rámci rozsáhlejších útoků na subjekty, s nimiž jsou v elektrické síti propojeny. Proto byla doplněna ustanovení a doporučení, která mají pomoci zmírnit kybernetická bezpečnostní rizika spojená s procesy souvisejícími s dodavatelským řetězcem, zejména se zadáváním zakázek, s dopadem na přeshraniční toky elektřiny.

(23) Vzhledem k tomu, že zneužití zranitelnosti v síti a v informačních systémech může způsobit významné narušení dodávek energie a škody hospodářství a spotřebitelům, měla by být tato zranitelnost rychle zjištěna a odstraněna, aby se snížila rizika. V zájmu usnadnění účinného provádění tohoto nařízení by příslušné subjekty a příslušné orgány měly spolupracovat při cvičeních a testovacích činnostech, které jsou pro tento účel považovány za vhodné, včetně výměny informací o kybernetických hrozbách, kybernetických útocích, zranitelnosti, nástrojích a metodách, taktice, technikách a postupech, připravenosti na řízení kybernetických bezpečnostních krizí a dalších cvičeních. Vzhledem k tomu, že se technologie neustále vyvíjejí a digitalizace odvětví elektroenergetiky rychle postupuje, nemělo by provádění přijatých ustanovení bránit inovacím a představovat překážku pro přístup na trh s elektřinou a následné využívání inovativních řešení, jež přispívají k účinnosti a udržitelnosti elektrizační soustavy.

(24) Informace shromážděné pro účely sledování provádění tohoto nařízení by měly být přiměřeně omezeny podle zásady „vědět jen to nejnutnější“. Zainteresovaným subjektům by měly být poskytnuty dosažitelné a účinné lhůty pro předložení těchto informací. Je třeba se vyhnout dvojímu oznamování.

(25) Ochrana kybernetické bezpečnosti nekončí na hranicích Unie. Bezpečný systém vyžaduje zapojení sousedních třetích zemí. Unie a její členské státy by měly usilovat o podporu sousedních třetích zemí, jejichž elektroenergetická infrastruktura je připojena k evropské síti, při uplatňování obdobných pravidel kybernetické bezpečnosti, jaká jsou stanovena v tomto nařízení.

(26) V zájmu včasného zlepšení koordinace bezpečnosti a testování budoucích závazných podmínek a metodik by ENTSO pro elektřinu, subjekt EU DSO a příslušné orgány měly začít vypracovávat nezávazné pokyny ihned po vstupu tohoto nařízení v platnost. Tyto pokyny budou sloužit jako základ pro vypracování budoucích podmínek a metodik. Současně by příslušné orgány měly určit subjekty, které připadají v úvahu pro zařazení do kategorie subjektů s vysokým dopadem a subjektů s kritickým dopadem, aby začaly dobrovolně plnit příslušné povinnosti.

(27) Toto nařízení bylo vypracováno v úzké spolupráci s ACER, ENISA, ENTSO pro elektřinu, subjektem EU DSO a dalšími zainteresovanými subjekty s cílem přijmout transparentním a participativním způsobem účinná, vyvážená a přiměřená pravidla.

(28) Toto nařízení doplňuje a posiluje opatření k řízení krizí stanovená v rámci EU pro reakci na kybernetické bezpečnostní krize, která jsou uvedena v doporučení Komise (EU) 2017/1584 ([9]). Kybernetický útok by také mohl způsobit elektroenergetickou krizi, jak je definována v čl. 2 bodě 9 nařízení (EU) 2019/941, přispět k ní nebo se s ní časově shodovat, a ovlivnit tak přeshraniční toky elektřiny. Tato elektroenergetická krize by mohla vést k souběžné elektroenergetické krizi ve smyslu čl. 2 odst. 10 nařízení (EU) 2019/941. Takový incident by mohl mít dopad i na další odvětví závislá na bezpečnosti dodávek elektřiny. Pokud by takový incident přerostl v rozsáhlý kybernetický bezpečnostní incident ve smyslu článku 16 směrnice (EU) 2022/2555, měla by se uplatnit ustanovení uvedeného článku, kterým se zřizuje síť Evropská síť styčných organizací pro řešení kybernetických krizí (dále jen „EU-CyCLONe“). Pokud jde o řízení krizí na úrovni Unie, měly by příslušné strany vycházet z integrovaných opatření EU pro politickou reakci na krize (dále jen „opatření IPCR EU“) podle prováděcího rozhodnutí Rady (EU) 2018/1993 ([10]).

(29) Tímto nařízením není dotčena pravomoc členských států přijímat opatření nezbytná k zajištění ochrany základních zájmů jejich bezpečnosti, k ochraně politiky a veřejné bezpečnosti a k umožnění vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 Smlouvy o fungování EU není žádný členský stát povinen poskytovat informace, jejichž zveřejnění je podle jeho názoru v rozporu se základními zájmy jeho bezpečnosti.

([9]) Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

([10]) Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize (Úř. věst. L 320, 17.12.2018, s. 28).

(30) Ačkoli se toto nařízení v zásadě vztahuje na subjekty, které vykonávají činnosti v oblasti výroby elektřiny z jaderných elektráren, některé z těchto činností mohou souviset s národní bezpečností.

(31) Na zpracování osobních údajů podle tohoto nařízení by se mělo uplatnit právo Unie v oblasti ochrany údajů a právo Unie v oblasti ochrany soukromí. Tímto nařízením není dotčeno zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 ([11]), směrnice Evropského parlamentu a Rady 2002/58/ES ([12]) a nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([13]). Tímto nařízením by proto neměly být mimo jiné dotčeny úkoly a pravomoci orgánů příslušných ke sledování souladu s platným právem Unie v oblasti ochrany údajů a právem Unie v oblasti ochrany soukromí.

(32) S ohledem na význam mezinárodní spolupráce na poli kybernetické bezpečnosti by příslušné orgány odpovědné za plnění úkolů, které jim byly svěřeny podle tohoto nařízení, a určené členskými státy měly mít možnost účastnit se sítí pro mezinárodní spolupráci. Příslušné orgány by proto pro účely plnění svých úkolů měly mít možnost vyměňovat si informace, včetně osobních údajů, s příslušnými orgány třetích zemí, pokud jsou splněny podmínky pro předávání osobních údajů do třetích zemí podle práva Unie v oblasti ochrany údajů, mimo jiné podmínky stanovené v článku 49 nařízení (EU) 2016/679.

(33) Zpracování osobních údajů v rozsahu nutném a přiměřeném pro zajištění bezpečnosti aktiv ze strany subjektů s vysokým dopadem nebo subjektů s kritickým dopadem by mohlo být považováno za zákonné na základě toho, že takové zpracování splňuje právní povinnost, která se vztahuje na správce, v souladu s požadavky čl. 6 odst. 1 písm. c) a čl. 6 odst. 3 nařízení (EU) 2016/679. Zpracování osobních údajů může být rovněž nezbytné pro oprávněné zájmy subjektů s vysokým dopadem nebo subjektů s kritickým dopadem, jakož i poskytovatelů bezpečnostních technologií a služeb jednajících jménem těchto subjektů podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679, včetně případů, kdy je takové zpracování nezbytné pro ujednání o sdílení informací o kybernetické bezpečnosti nebo dobrovolné oznamování příslušných informací v souladu s tímto nařízením. Opatření týkající se prevence, odhalování, identifikace, zamezení šíření, analýzy kybernetických útoků a reakce na kybernetické útoky, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměny informací v rámci nápravy zranitelnosti a jejího koordinovaného zveřejňování a také dobrovolné výměny informací o těchto kybernetických útocích a kybernetických hrozbách a zranitelnosti, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích může vyžadovat zpracovávání určitých kategorií osobních údajů, například IP adres, jednotných adres zdroje (URL), jmen domén, e-mailových adres a, odhalují-li osobní údaje, časových razítek. Zpracování osobních údajů příslušnými orgány, jednotnými kontaktními místy a týmy CSIRT může představovat právní povinnost nebo může být považováno za nezbytné pro plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce údajů podle čl. 6 odst. 1 písm. c) nebo e) a čl. 6 odst. 3 nařízení (EU) 2016/679, nebo pro sledování oprávněného zájmu subjektů s vysokým dopadem nebo subjektů s kritickým dopadem, jak je uvedeno v čl. 6 odst. 1 písm. f) uvedeného nařízení. Kromě toho může vnitrostátní právo stanovit pravidla, která příslušným orgánům, jednotným kontaktním místům a týmům CSIRT v rozsahu, který je nezbytný a přiměřený pro účely zajištění bezpečnosti sítí a informačních systémů subjektů s vysokým dopadem nebo subjektů s kritickým dopadem, umožní zpracovávat zvláštní kategorie osobních údajů v souladu s článkem 9 nařízení (EU) 2016/679, zejména stanovením vhodných a konkrétních opatření na ochranu základních práv a zájmů fyzických osob, včetně technických omezení opakovaného použití těchto údajů a používání nejmodernějších bezpečnostních opatření a opatření na ochranu soukromí, jako je pseudonymizace nebo šifrování, pokud může anonymizace mít významný vliv na sledovaný účel.

([11]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

([12]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. Věst. L 201, 31.7.2002, s. 37).

([13]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

(34) V důsledku kybernetických útoků je v mnoha případech ohrožena ochrana osobních údajů. V této souvislosti by příslušné orgány měly spolupracovat a vyměňovat si informace o všech relevantních záležitostech s orgány uvedenými v nařízení (EU) 2016/679 a směrnici 2002/58/ES.

(35) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 a dne 17. listopadu 2023 vydal své stanovisko,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Toto nařízení zavádí kodex sítě, který stanoví odvětvová pravidla pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny, včetně pravidel pro společné minimální požadavky, plánování, monitorování, podávání zpráv a řízení krizí.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na aspekty kybernetické bezpečnosti přeshraničních toků elektřiny při činnostech následujících subjektů, pokud jsou v souladu s článkem 24 označeny za subjekty s vysokým dopadem nebo subjekty s kritickým dopadem:

a) elektroenergetické podniky ve smyslu čl. 2 bodu 57 směrnice (EU) 2019/944;

b) nominovaní organizátoři trhu s elektřinou ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/943;

c) organizovaná tržní místa nebo „organizované trhy“ ve smyslu čl. 2 bodu 4 prováděcího nařízení Komise (EU) č. 1348/2014 ([14]), které sjednávají transakce s produkty relevantními pro přeshraniční toky elektřiny;

d) poskytovatelé kritických služeb IKT podle čl. 3 bodu 9 tohoto nařízení;

e) ENTSO pro elektřinu zřízená podle článku 28 nařízení (EU) 2019/943;

f) subjekt EU DSO zřízený podle článku 52 nařízení (EU) 2019/943;

g) subjekty zúčtování ve smyslu čl. 2 bodu 14 nařízení (EU) 2019/943;

h) provozovatelé dobíjecích bodů ve smyslu přílohy I směrnice (EU) 2022/2555;

i) regionální koordinační centra zřízená podle článku 35 nařízení (EU) 2019/943;

j) poskytovatelé řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555;

k) jakýkoli jiný subjekt nebo třetí strana, jež byly pověřeny plněním povinností podle tohoto nařízení nebo jimž bylo plnění těchto povinností svěřeno.

2. Za plnění úkolů stanovených v tomto nařízení jsou v rámci svých stávajících mandátů odpovědné tyto orgány:

a) Agentura Evropské unie pro spolupráci energetických regulačních orgánů (dále jen „ACER“) zřízená nařízením Evropského parlamentu a Rady (EU) 2019/942 ([15]);

b) příslušné vnitrostátní orgány odpovědné za plnění úkolů, které jim byly svěřeny podle tohoto nařízení a které členské státy určily podle článku 4, nebo „příslušný orgán“;

c) národní regulační orgány určené jednotlivými členskými státy podle čl. 57 odst. 1 směrnice (EU) 2019/944;

([14]) Prováděcí nařízení Komise (EU) č. 1348/2014 ze dne 17. prosince 2014 o oznamování údajů za účelem provedení čl. 8 odst. 2 a 6 nařízení Evropského parlamentu a Rady (EU) č. 1227/2011 o integritě a transparentnosti velkoobchodního trhu s energií (Úř. věst. L 363, 18.12.2014, s. 121).

([15]) Nařízení Evropského parlamentu a Rady (EU) 2019/942 ze dne 5. června 2019, kterým se zřizuje Agentura Evropské unie pro spolupráci energetických regulačních orgánů (Úř. věst. L 158, 14.6.2019, s. 22).

d) příslušné orgány pro rizikovou připravenost zřízené podle článku 3 nařízení (EU) 2019/941;

e) týmy pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) určené nebo zřízené podle článku 10 směrnice (EU) 2022/2555;

f) příslušné orgány odpovědné za kybernetickou bezpečnost určené nebo zřízené podle článku 8 směrnice (EU) 2022/2555;

g) Agentura Evropské unie pro kybernetickou bezpečnost zřízená podle nařízení (EU) 2019/881;

h) jakékoli jiné orgány nebo třetí strana, jež byly pověřeny plněním povinností podle tohoto nařízení nebo jimž bylo plnění těchto povinností svěřeno podle čl. 4 odst. 3.

3. Toto nařízení se rovněž vztahuje na všechny subjekty, které nejsou usazeny v Unii, ale poskytují služby subjektům v Unii, pokud je příslušné orgány v souladu s čl. 24 odst. 2 označily za subjekty s vysokým dopadem nebo subjekty s kritickým dopadem.

4. Tímto nařízením není dotčena odpovědnost členských států za ochranu národní bezpečnosti a jejich pravomoc chránit další základní funkce státu, včetně zajištění územní celistvosti státu a udržování veřejného pořádku.

5. Tímto nařízením není dotčena odpovědnost členských států za ochranu národní bezpečnosti, pokud jde o činnosti při výrobě elektřiny z jaderných elektráren, včetně činností v rámci jaderného hodnotového řetězce, v souladu se Smlouvami.

6. Subjekty, příslušné orgány, jednotná kontaktní místa na úrovni subjektů a týmy CSIRT zpracovávají osobní údaje v rozsahu nezbytném pro účely tohoto nařízení a v souladu s nařízením (EU) 2016/679; takové zpracování je založeno zejména na článku 6 uvedeného nařízení.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „aktivem“ jakékoli informace, software nebo hardware v síti a informačních systémech, ať už hmotné nebo nehmotné, které mají hodnotu pro jednotlivce, organizaci nebo vládu;

2) „příslušným orgánem pro rizikovou připravenost“ příslušný orgán určený podle článku 3 nařízení (EU) 2019/941;

3) „týmem pro reakce na počítačové bezpečnostní incidenty“ tým odpovědný za zvládání rizik a řešení incidentů v souladu s článkem 10 směrnice (EU) 2022/2555;

4) „aktivem s kritickým dopadem“ aktivum, které je nezbytné k provádění procesu s kritickým dopadem;

5) „subjektem s kritickým dopadem“ subjekt, který provádí proces s kritickým dopadem a který byl určen příslušnými orgány v souladu s článkem 24;

6) „perimetrem kritického dopadu“ perimetr vymezený subjektem uvedeným v čl. 2 odst. 1, který obsahuje všechna aktiva s kritickým dopadem, na němž lze kontrolovat přístup k těmto aktivům a který vymezuje oblast, v níž se uplatňují pokročilé kontroly v oblasti kybernetické bezpečnosti;

7) „procesem s kritickým dopadem“ obchodní proces prováděný subjektem, u něhož jsou indexy dopadu na kybernetickou bezpečnost elektřiny vyšší než práh kritického dopadu;

8) „prahem kritického dopadu“ hodnoty indexů dopadu na kybernetickou bezpečnost elektřiny uvedené v čl. 19 odst. 3 písm. b), při jejichž překročení způsobí kybernetický útok na obchodní proces kritické narušení přeshraničních toků elektřiny;

9) „poskytovatelem kritických služeb IKT“ subjekt, který poskytuje službu IKT nebo proces IKT, který je nezbytný pro proces s kritickým dopadem nebo proces s vysokým dopadem ovlivňující aspekty kybernetické bezpečnosti přeshraničních toků elektřiny a který v případě narušení může způsobit kybernetický útok s dopadem vyšším než práh kritického dopadu nebo práh vysokého dopadu;

10) „přeshraničním tokem elektřiny“ přeshraniční tok ve smyslu čl. 2 bodu 3 nařízení (EU) 2019/943;

11) „kybernetickým útokem“ incident ve smyslu v čl. 3 bodu 14 nařízení (EU) 2022/2554;

12) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 2 bodu 1 nařízení (EU) 2019/881;

13) „kontrolou v oblasti kybernetické bezpečnosti“ opatření nebo postupy prováděné za účelem prevence, odhalování, potírání nebo minimalizace kybernetických bezpečnostních rizik;

14) „kybernetickým bezpečnostním incidentem“ incident ve smyslu čl. 6 bodu 6 směrnice (EU) 2022/2555;

15) „systémem řízení kybernetické bezpečnosti“ zásady, postupy, pokyny a související zdroje a činnosti, které subjekt společně řídí s cílem chránit svá informační aktiva před kybernetickými hrozbami systematickým zaváděním, prováděním, provozováním, sledováním, přezkoumáváním, udržováním a zlepšováním bezpečnosti sítí a informačních systémů organizace;

16) „operačním střediskem kybernetické bezpečnosti“ specializované středisko, v němž technický tým složený z jednoho nebo více odborníků s podporou informačních systémů kybernetické bezpečnosti plní úkoly související s bezpečností (služby operačního střediska kybernetické bezpečnosti), jako je zvládání kybernetických útoků a řešení chyb v bezpečnostní konfiguraci, sledování bezpečnosti, analýza protokolů a odhalování kybernetických útoků;

17) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/881;

18) „řízením zranitelnosti v oblasti kybernetické bezpečnosti“ postup zjišťování a řešení zranitelnosti;

19) „subjektem“ subjekt ve smyslu čl. 6 bodu 38 směrnice (EU) 2022/2555;

20) „včasným varováním“ informace nezbytné k určení, zda existuje podezření, že závažný incident byl způsoben protiprávním nebo zlovolným jednáním nebo zda by mohl mít přeshraniční dopad;

21) „indexem dopadu na kybernetickou bezpečnost elektřiny“ (dále jen „ECII“) index nebo klasifikační stupnice, která hodnotí možné důsledky kybernetických útoků na obchodní procesy zapojené do přeshraničních toků elektřiny;

22) „evropským systémem certifikace kybernetické bezpečnosti“ systém ve smyslu definice v čl. 2 bodu 9 nařízení (EU) 2019/881;

23) „subjektem s vysokým dopadem“ subjekt, který provádí proces s vysokým dopadem a který byl určen příslušnými orgány v souladu s článkem 24;

24) „procesem s vysokým dopadem“ jakýkoli obchodní proces prováděný subjektem, u něhož jsou indexy dopadu na kybernetickou bezpečnost elektřiny vyšší než práh vysokého dopadu;

25) „aktivem s vysokým dopadem“ aktivum, které je nezbytné k provedení procesu s vysokým dopadem;

26) „prahem vysokého dopadu“ hodnoty indexů dopadu na kybernetickou bezpečnost elektřiny uvedené v čl. 19 odst. 3 písm. b), při jejichž překročení způsobí úspěšný kybernetický útok na proces vysokou míru narušení přeshraničních toků elektřiny;

27) „perimetrem vysokého dopadu“ perimetr vymezený jakýmkoli subjektem uvedeným v čl. 2 odst. 1, který obsahuje všechna aktiva s vysokým dopadem, na němž lze kontrolovat přístup k těmto aktivům a který vymezuje oblast, v níž se uplatňují minimální kontroly v oblasti kybernetické bezpečnosti;

28) „produktem IKT“ produkt IKT ve smyslu čl. 2 bodu 12 nařízení (EU) 2019/881;

29) „službou IKT“ služba IKT ve smyslu čl. 2 bodu 13 nařízení (EU) 2019/881;

30) „procesem IKT“ proces IKT ve smyslu čl. 2 bodu 14 nařízení (EU) 2019/881;

31) „původním systémem“ původní systém IKT ve smyslu čl. 3 bodu 3 nařízení (EU) 2022/2554;

32) „národním jednotným kontaktním místem“ jednotné kontaktní místo určené nebo zřízené každým členským státem podle čl. 8 odst. 3 směrnice (EU) 2022/2555;

33) „orgány pro řízení kybernetických krizí ovlivňujících bezpečnost sítí a informací“ orgány určené nebo zřízené podle čl. 9 odst. 1 směrnice (EU) 2022/2555;

34) „původcem“ subjekt, který iniciuje výměnu informací, sdílení informací nebo ukládání informací;

35) „specifikacemi pro zadávání zakázek“ specifikace, které subjekty stanoví pro zadávání zakázek na nové nebo aktualizované produkty IKT, procesy IKT nebo služby IKT;

36) „zástupcem“ fyzická nebo právnická osoba usazená v Unii, která je výslovně určena k jednání jménem subjektu s vysokým dopadem nebo subjektu s kritickým dopadem, který není usazen v Unii, ale poskytuje služby subjektům v Unii, a na kterou se může příslušný orgán nebo tým CSIRT obracet místo na samotný subjekt s vysokým dopadem nebo subjekt s kritickým dopadem, pokud jde o povinnosti tohoto subjektu podle tohoto nařízení;

37) „rizikem“ riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555;

38) „maticí dopadu rizik“ matice používaná při posuzování rizik k určení výsledné úrovně dopadu rizik pro každé posuzované riziko;

39) „souběžnou elektroenergetickou krizí“ elektroenergetická krize podle definice v čl. 2 bodě 10 nařízení (EU) 2019/941;

40) „jednotným kontaktním místem na úrovni subjektu“ jednotné kontaktní místo na úrovni subjektu určené podle čl. 38 odst. 1 písm. c);

41) „zainteresovaným subjektem“ jakákoli strana, která má zájem na úspěchu a trvalém fungování organizace nebo procesu, jako jsou zaměstnanci, ředitelé, akcionáři, regulační orgány, sdružení, dodavatelé a zákazníci;

42) „normou“ norma ve smyslu čl. 2 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([16]);

43) „regionem pro provoz soustavy“ regiony pro provoz soustavy vymezené v příloze I rozhodnutí ACER č. 05/2022 o vymezení regionů pro provoz soustavy, stanovené v souladu s článkem 36 nařízení (EU) 2019/943;

44) „provozovateli soustav“ provozovatel distribuční soustavy a provozovatel přenosové soustavy ve smyslu čl. 2 bodu 29 a čl. 2 bodu 35 směrnice (EU) 2019/944;

45) „procesem s kritickým dopadem na celou Unii“ jakýkoli proces v odvětví elektroenergetiky, který může zahrnovat více subjektů a u něhož lze při provádění posouzení kybernetického bezpečnostního rizika pro celou Unii považovat možný dopad kybernetického útoku za kritický;

46) „procesem s vysokým dopadem na celou Unii“ jakýkoli proces v odvětví elektroenergetiky, který může zahrnovat více subjektů a u něhož lze při provádění posouzení kybernetického bezpečnostního rizika na rizika pro celou Unii považovat možný dopad kybernetického útoku za vysoký;

47) „neopravenou aktivně zneužívanou zranitelností“ zranitelnost, která dosud nebyla zveřejněna a opravena a u níž existují spolehlivé důkazy, že aktér v soustavě provedl spuštění škodlivého kódu bez souhlasu vlastníka soustavy;

48) „zranitelností“ zranitelnost ve smyslu čl. 6 bodu 15 směrnice (EU) 2022/2555.

Článek 4

Příslušný orgán

1. Každý členský stát určí co nejdříve, nejpozději však 13. prosince 2024 národní vládní nebo regulační orgán odpovědný za plnění úkolů, jimiž je pověřen v tomto nařízení (dále jen „příslušný orgán“). Dokud není příslušný orgán pověřen plněním úkolů podle tohoto nařízení, plní úkoly příslušného orgánu v souladu s tímto nařízením regulační orgán určený každým členským státem podle čl. 57 odst. 1 směrnice (EU) 2019/944.

2. Členské státy neprodleně oznámí Komisi, ACER, ENISA, skupině pro spolupráci v oblasti bezpečnosti sítí a informací zřízené podle článku 14 směrnice (EU) 2022/2555 a Koordinační skupině pro otázky elektrické energie zřízené podle článku 1 rozhodnutí Komise ze dne 15. listopadu 2012 ([17]) název a kontaktní údaje svého příslušného orgánu určeného podle odstavce 1 tohoto článku a jejich případné následné změny.

([16]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského 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 kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

([17]) Rozhodnutí Komise ze dne 15. listopadu 2012, kterým se zřizuje Koordinační skupina pro otázky elektrické energie (2012/C353/02) (Úř. věst. C 353, 17.11.2012, s. 2).

3. Členské státy mohou příslušnému orgánu povolit, aby úkoly, které mu byly svěřeny tímto nařízením, s výjimkou úkolů uvedených v článku 5, přenesl na jiné vnitrostátní orgány, Každý příslušný orgán sleduje, jak orgány, na něž úkoly přenesl, uplatňují toto nařízení. Příslušný orgán sdělí Komisi, ACER, Koordinační skupině pro otázky elektrické energie, ENISA a skupině pro spolupráci v oblasti bezpečnosti sítí a informací název, kontaktní údaje a přidělené úkoly orgánů, na které na které byly úkoly přeneseny, a jejich veškeré následné změny.

Článek 5

Spolupráce mezi příslušnými orgány a subjekty na vnitrostátní úrovni

Příslušné orgány koordinují a zajišťují vhodnou spolupráci mezi příslušnými orgány odpovědnými za kybernetickou bezpečnost, orgány příslušnými k řízení kybernetických krizí, národními regulačními orgány, příslušnými orgány pro rizikovou připravenost a týmy CSIRT za účelem plnění příslušných povinností stanovených v tomto nařízení. Příslušné orgány rovněž koordinují svou činnost s dalšími subjekty nebo orgány, které určí každý členský stát, k zajištění účinných postupů a zabránění zdvojování úkolů a povinností. Příslušné orgány mohou vydat příslušným národním regulačním orgánům pokyn, aby požádaly ACER o stanovisko podle čl. 8 odst. 3.

Článek 6

Podmínky nebo metodiky či plány

1. Provozovatelé přenosových soustav vypracují ve spolupráci se subjektem EU DSO návrhy podmínek nebo metodik podle odstavce 2 nebo plánů podle odstavce 3.

2. Následující podmínky nebo metodiky a jejich změny podléhají schválení všemi příslušnými orgány:

a) metodiky pro hodnocení kybernetických bezpečnostních rizik podle čl. 18 odst. 1;

b) zpráva o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny podle článku 23;

c) minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti podle článku 29, mapování kontrol v oblasti kybernetické bezpečnosti elektřiny podle norem podle článku 34, včetně minimálních a pokročilých kontrol kybernetické bezpečnosti v dodavatelském řetězci v souladu s článkem 33;

d) doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti podle článku 35;

e) metodiku stupnice pro klasifikaci kybernetických útoků podle čl. 37 odst. 8.

3. Návrhy regionálních plánů pro zmírnění kybernetických bezpečnostních rizik podle článku 22 podléhají schválení všemi příslušnými orgány dotčeného regionu pro provoz soustavy.

4. Návrhy podmínek a metodik uvedených v odstavci 2 nebo plánů uvedených v odstavci 3 musí obsahovat návrh harmonogramu jejich zavádění a popis jejich předpokládaného dopadu na cíle tohoto nařízení.

5. Subjekt EU DSO může dotčeným provozovatelům přenosových soustav poskytnout odůvodněné stanovisko do tří týdnů před uplynutím lhůty pro předložení návrhu podmínek nebo metodik či plánů příslušným orgánům. Provozovatelé přenosových soustav odpovědní za návrh podmínek nebo metodik či plánů zohlední odůvodněné stanovisko subjektu EU DSO před předložením návrhu příslušným orgánům ke schválení. Pokud stanovisko subjektu EU DSO není zohledněno, provozovatelé přenosových soustav pro to poskytnou odůvodnění.

6. Při společném vypracovávání podmínek a metodik nebo plánů zúčastnění provozovatelé přenosových soustav úzce spolupracují. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO pravidelně informují příslušné orgány a ACER o pokroku při vypracovávání podmínek nebo metodik či plánů.

Článek 7

Pravidla hlasování u provozovatelů přenosových soustav

1. Pokud provozovatelé přenosových soustav, kteří rozhodují o návrzích podmínek nebo metodik, nedokážou dosáhnout dohody, rozhodnou na základě hlasování kvalifikovanou většinou. Kvalifikovaná většina pro tyto návrhy se vypočítá takto:

a) provozovatelé přenosových soustav, kteří zastupují nejméně 55 % dotčených členských států a

b) provozovatelé přenosových soustav zastupující členské státy, které představují nejméně 65 % obyvatelstva Unie.

2. U rozhodnutí o návrzích podmínek nebo metodik uvedených v čl. 6 odst. 2 tvoří blokační menšinu provozovatelé přenosových soustav, kteří zastupují nejméně čtyři členské státy, jinak se kvalifikovaná většina považuje za dosaženou.

3. Pokud provozovatelé přenosových soustav z regionů pro provoz soustavy, kteří rozhodují o návrzích plánů uvedených v čl. 6 odst. 2, nedokážou dosáhnout dohody a pokud se daný region pro provoz soustavy skládá z více než pěti členských států, rozhodují provozovatelé přenosových soustav na základě hlasování kvalifikovanou většinou. Kvalifikovaná většina pro návrhy uvedené v čl. 6 odst. 2 vyžaduje tuto většinu:

a) provozovatelé přenosových soustav, kteří zastupují nejméně 72 % dotčených členských států; a

b) provozovatelé přenosových soustav zastupující členské státy, které představují nejméně 65 % obyvatelstva dotčené oblasti.

4. U rozhodnutí o návrzích plánů musí blokační menšinu tvořit alespoň minimální počet provozovatelů přenosových soustav zastupujících více než 35 % obyvatelstva zúčastněných členských států a navíc provozovatelé přenosových soustav zastupující nejméně jeden další dotčený členský stát, jinak se kvalifikovaná většina považuje za dosaženou.

5. Při rozhodování provozovatelů přenosových soustav o návrzích podmínek nebo metodik podle čl. 6 odst. 2 je každému členskému státu přidělen jeden hlas. Působí-li na území členského státu více provozovatelů přenosových soustav, rozdělí mezi ně členský stát hlasovací práva.

6. Nepředloží-li provozovatelé přenosových soustav ve spolupráci se subjektem EU DSO prvotní nebo pozměněný návrh podmínek nebo metodik nebo plánů příslušným orgánům ve lhůtách stanovených v tomto nařízení, poskytnou příslušným orgánům a ACER příslušné pracovní verze podmínek nebo metodik nebo plánů. Vysvětlí, co bránilo dosažení dohody. Příslušné orgány společně přijmou vhodné kroky k přijetí požadovaných podmínek nebo metodik nebo požadovaných plánů. To lze provést například vyžádáním změn pracovních verzí předložených podle tohoto odstavce, revizí a doplněním těchto pracovních verzí, nebo pokud žádné pracovní verze nebyly předloženy, vymezením a schválením požadovaných podmínek nebo metodik či plánů.

Článek 8

Předkládání návrhů příslušným orgánům

1. Provozovatelé přenosových soustav předloží návrhy podmínek nebo metodik či plánů příslušným orgánům ke schválení v příslušných lhůtách stanovených v článcích 18, 23, 29, 33, 34, 35 a 37. Příslušné orgány mohou tyto lhůty za výjimečných okolností společně prodloužit, zejména v případech, kdy není možné lhůtu dodržet vzhledem k okolnostem mimo sféru působnosti provozovatelů přenosových soustav nebo subjektu EU DSO.

2. Návrhy podmínek a metodik nebo plánů podle odstavce 1 se současně s jejich předložením příslušným orgánům předkládají ACER k informaci.

3. Na společnou žádost národních regulačních orgánů vydá ACER stanovisko k návrhu podmínek nebo metodik či plánů do šesti měsíců od obdržení návrhů podmínek nebo metodik či plánů a toto stanovisko oznámí národním regulačním orgánům a příslušným orgánům. Národní regulační orgány, příslušné orgány odpovědné za kybernetickou bezpečnost a všechny ostatní orgány určené jako příslušné orgány se vzájemně koordinují předtím, než národní regulační orgány požádají ACER o stanovisko. ACER může do tohoto stanoviska zahrnout doporučení. Před vydáním stanoviska k návrhům uvedeným v čl. 6 odst. 2 konzultuje ACER agenturu ENISA.

4. Příslušné orgány se navzájem konzultují, úzce spolupracují a koordinují svou činnost s cílem dosáhnout dohody o navrhovaných podmínkách, metodikách nebo plánech. Před schválením podmínek nebo metodik či plánů své návrhy, v případě potřeby po konzultaci s ENTSO pro elektřinu a subjektem EU DSO, revidují a doplní, aby zajistily, že návrhy jsou v souladu s tímto nařízením a přispívají k vysoké společné úrovni kybernetické bezpečnosti v Unii.

5. O podmínkách nebo metodikách nebo o plánech rozhodnou příslušné orgány do šesti měsíců poté, co je příslušný orgán nebo případně poslední příslušný orgán, kterého se to týká, obdrží.

6. Vydá-li ACER stanovisko, příslušné orgány toto stanovisko zohlední a do šesti měsíců od jeho obdržení přijmou svá rozhodnutí.

7. Pokud příslušné orgány společně požadují změnu navrhovaných podmínek nebo metodik či plánů za účelem jejich schválení, vypracují provozovatelé přenosových soustav ve spolupráci se subjektem EU DSO návrh takové změny podmínek nebo metodik či plánů. Pozměněný návrh provozovatelé přenosových soustav předloží ke schválení do dvou měsíců od žádosti příslušných orgánů. Příslušné orgány rozhodnou o změněných podmínkách nebo metodikách či plánech do dvou měsíců od jejich předložení.

8. Nedokážou-li příslušné orgány dosáhnout dohody ve lhůtě uvedené v odstavci 5 nebo 7, informují o tom Komisi. Komise může přijmout vhodné kroky, aby umožnila přijetí požadovaných podmínek nebo metodik či plánů.

9. Po schválení příslušnými orgány provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a subjekt EU DSO zveřejní podmínky nebo metodiky či plány na svých internetových stránkách s výjimkou případů, kdy jsou tyto informace v souladu s článkem 47 považovány za důvěrné.

10. Příslušné orgány mohou společně požádat provozovatele přenosových soustav a subjekt EU DSO o návrhy změn schválených podmínek nebo metodik nebo schválených plánů a stanovit lhůtu pro předložení těchto návrhů. Provozovatelé přenosových soustav mohou ve spolupráci se subjektem EU DSO navrhovat příslušným orgánům změny i z vlastního podnětu. Návrhy na změnu podmínek nebo metodik nebo na změny plánů se vypracovávají a schvalují postupem podle tohoto článku.

11. Nejméně každé tři roky po prvním přijetí příslušných podmínek nebo metodik nebo příslušných přijatých plánů provozovatelé přenosových soustav ve spolupráci se subjektem EU DSO přezkoumají účinnost přijatých podmínek nebo metodik nebo přijatých plánů a o výsledcích přezkumu bez zbytečného odkladu podají zprávu příslušným orgánům a ACER.

Článek 9

Konzultace

1. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO konzultují se zainteresovanými subjekty, včetně ACER, ENISA a příslušného orgánu každého členského státu, o návrzích podmínek nebo metodik uvedených v čl. 6 odst. 2 a o plánech uvedených v čl. 6 odst. 3. Konzultace musí trvat nejméně jeden měsíc.

2. Návrhy podmínek nebo metodik uvedených v čl. 6 odst. 2, které předkládají provozovatelé přenosových soustav ve spolupráci se subjektem EU DSO, se zveřejňují a předkládají ke konzultaci na úrovni Unie. Návrhy plánů uvedených v čl. 6 odst. 3, které předkládají příslušní provozovatelé přenosových soustav ve spolupráci se subjektem EU DSO na regionální úrovni, se předkládají ke konzultaci přinejmenším na regionální úrovni.

3. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a subjekt EU DSO odpovědný za návrh podmínek nebo metodik či plánů před jeho předložením regulačním orgánům ke schválení řádně zohlední názory zainteresovaných subjektů vyplývající z konzultací provedených v souladu s odstavcem 1. Ve všech případech musí být předloženo řádné odůvodnění, proč názory vzešlé z konzultací byly či nebyly do návrhu zahrnuty; toto odůvodnění se přiloží k návrhu předkládanému ke schválení a zároveň se toto odůvodnění včas zveřejní, a to před předložením návrhu podmínek nebo metodik nebo současně s ním.

Článek 10

Zapojení zainteresovaných subjektů

ACER v úzké spolupráci s ENTSO pro elektřinu a subjektem EU DSO organizuje zapojení zainteresovaných subjektů, včetně pravidelných schůzek se zainteresovanými subjekty s cílem určit problémy a navrhnout zlepšení týkající se provádění tohoto nařízení.

Článek 11

Úhrada nákladů

1. Náklady, které nesou provozovatelé přenosových soustav a provozovatelé distribučních soustav podléhající regulaci síťových tarifů a které vyplývají z povinností stanovených v tomto nařízení, včetně nákladů nesených ENTSO pro elektřinu a subjektem EU DSO, posuzuje příslušný národní regulační orgán každého členského státu.

2. Náklady, jež budou posouzeny jako rozumné, účinné a přiměřené se uhradí prostřednictvím síťových tarifů nebo jiných vhodných mechanismů, jež určí příslušný národní regulační orgán.

3. Na žádost příslušných národních regulačních orgánů jsou provozovatelé přenosových soustav a provozovatelé distribučních soustav podle odstavce 1 v přiměřené lhůtě stanovené národním regulačním orgánem povinni předložit informace potřebné pro účely posouzení vzniklých nákladů.

Článek 12

Sledování

1. ACER sleduje provádění tohoto nařízení v souladu s čl. 32 odst. 1 nařízení (EU) 2019/943 a čl. 4 odst. 2 nařízení (EU) 2019/942. Při provádění tohoto sledování může ACER spolupracovat s ENISA a požádat o podporu ENTSO pro elektřinu a subjekt EU DSO. O provádění tohoto nařízení ACER pravidelně informuje Koordinační skupinu pro otázky elektrické energie a skupinu pro spolupráci v oblasti bezpečnosti sítí a informací.

2. Nejméně každé tři roky od vstupu tohoto nařízení v platnost ACER zveřejní zprávu s cílem

a) přezkoumat stav provádění příslušných opatření pro řízení kybernetických bezpečnostních rizik se zřetelem na subjekty s vysokým dopadem a subjekty s kritickým dopadem;

b) zjistit, zda je třeba stanovit další pravidla týkající se společných požadavků, plánování, sledování, podávání zpráv a krizového řízení, aby se předešlo rizikům pro odvětví elektroenergetiky; a

c) určit oblasti, které je třeba zlepšit při revizi tohoto nařízení, nebo určit oblasti, které v něm nejsou zohledněny, a nové priority, které se mohou objevit v důsledku technického rozvoje.

3. Do 13. června 2025 může ACER ve spolupráci s ENISA a po konzultaci s ENTSO pro elektřinu a subjektem EU DSO vydat pokyny ohledně příslušných informací, které mají být sdělovány ACER pro účely sledování, a ohledně postupu a četnosti jejich shromažďování, a to na základě ukazatelů výkonnosti stanovených v souladu s odstavcem 5.

4. Příslušné orgány mohou mít přístup k příslušným informacím, které má ACER k dispozici a které shromáždila v souladu s tímto článkem.

5. ACER ve spolupráci s ENISA a s podporou ENTSO pro elektřinu a subjektu EU DSO vydá nezávazné ukazatele výkonnosti pro hodnocení provozní spolehlivosti, které se týkají aspektů kybernetické bezpečnosti přeshraničních toků elektřiny.

6. Subjekty uvedené v čl. 2 odst. 1 tohoto nařízení předkládají ACER informace potřebné k tomu, aby mohla ACER plnit úkoly uvedené v odstavci 2.

Článek 13

Srovnávací hodnocení

1. Do 13. června 2025 ACER ve spolupráci s ENISA vypracuje nezávaznou příručku pro srovnávací hodnocení kybernetické bezpečnosti. Příručka vysvětlí národním regulačním orgánům zásady srovnávacího hodnocení kontrol prováděných v oblasti kybernetické bezpečnosti podle odstavce 2 tohoto článku, přičemž zohlední náklady na provádění kontrol a účinnost funkce procesů, produktů, služeb, systémů a řešení používaných při provádění těchto kontrol. Při vypracovávání nezávazné příručky pro srovnávací hodnocení kybernetické bezpečnosti ACER zohlední stávající zprávy o srovnávacím hodnocení. Nezávaznou příručku pro srovnávací hodnocení kybernetické bezpečnosti předloží ACER pro informaci národním regulačním orgánům.

2. Do dvanácti měsíců od vytvoření příručky pro srovnávací hodnocení podle odstavce 1 provedou národní regulační orgány srovnávací analýzu s cílem posoudit, zda současné investice do kybernetické bezpečnosti:

a) zmírňují rizika, jež mají dopad na přeshraniční toky elektřiny;

b) přinášejí požadované výsledky a zvyšují efektivitu rozvoje elektrizačních soustav;

c) jsou účinné a integrované do celkového zadávání zakázek na aktiva a služby.

3. Při srovnávací analýze mohou národní regulační orgány zohlednit nezávaznou příručku pro srovnávací hodnocení kybernetické bezpečnosti, kterou vypracovala ACER, a posoudí zejména:

a) průměrné výdaje týkající se kybernetické bezpečnosti na zmírnění rizik, jež mají dopad na přeshraniční toky elektřiny, zejména pokud jde o subjekty s vysokým dopadem a subjekty s kritickým dopadem;

b) ve spolupráci s ENTSO pro elektřinu a subjektem EU DSO průměrné ceny služeb, systémů a produktů kybernetické bezpečnosti, které ve velké míře přispívají k posílení a zachování opatření pro řízení kybernetických bezpečnostních rizik v jednotlivých regionech pro provoz soustavy;

c) existenci a úroveň srovnatelnosti nákladů a funkcí služeb, systémů a řešení v oblasti kybernetické bezpečnosti vhodných pro provádění tohoto nařízení, přičemž určí možná opatření nezbytná pro podporu efektivity výdajů, zejména v případech, kdy mohou být zapotřebí investice do technologií v oblasti kybernetické bezpečnosti.

4. S veškerými informace týkajícími se srovnávací analýzy se zachází a zpracovávají se v souladu s požadavky na klasifikaci údajů podle tohoto nařízení, minimálními kontrolami v oblasti kybernetické bezpečnosti a zprávou o posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny. Srovnávací analýza uvedená v odstavcích 2 a 3 se nezveřejňuje.

5. Aniž jsou dotčeny požadavky na důvěrnost uvedené v článku 47 a potřeba chránit bezpečnost subjektů, na které se vztahují ustanovení tohoto nařízení, sdílí se srovnávací analýza uvedená v odstavcích 2 a 3 tohoto článku se všemi národními regulačními orgány, všemi příslušnými orgány, ACER, ENISA a Komisí.

Článek 14

Dohody s provozovateli přenosových soustav mimo Unii

1. Provozovatelé přenosových soustav z regionu pro provoz soustavy, který sousedí se třetí zemí, usilují, aby do 18 měsíců od vstupu tohoto nařízení v platnost uzavřeli dohody s provozovateli přenosových soustav ze sousední třetí země, které jsou v souladu s příslušnými právními předpisy Unie a které stanoví základ pro spolupráci v oblasti ochrany kybernetické bezpečnosti, a ujednání o spolupráci v oblasti kybernetické bezpečnosti s těmito provozovateli přenosových soustav.

2. O dohodách uzavřených podle odstavce 1 provozovatelé přenosových soustav informují příslušný orgán.

Článek 15

Právní zástupci

1. Subjekty, které nemají provozovnu v Unii, ale poskytují služby subjektům v Unii a byly v souladu s čl. 24 odst. 6 oznámeny jako subjekty s vysokým dopadem nebo subjekty s kritickým dopadem, do tří měsíců od oznámení písemně určí svého zástupce v Unii a informují o tom příslušný oznamující orgán.

2. Na tohoto zástupce se bude moci obracet jakýkoli příslušný orgán nebo tým CSIRT v Unii, a to dodatečně k subjektu s vysokým dopadem nebo subjektu s kritickým dopadem nebo namísto nich, pokud jde o povinnosti subjektu podle tohoto nařízení. Subjekt s vysokým dopadem nebo subjekt s kritickým dopadem musí svému právnímu zástupci poskytnout nezbytné pravomoci a dostatečné zdroje, aby byla zaručena jeho účinná a včasná spolupráce s příslušnými orgány nebo týmy CSIRT.

3. Zástupce musí být usazen v jednom z členských států, kde subjekt nabízí své služby. Má se za to, že subjekt spadá pod jurisdikci členského státu, v němž je zástupce usazen. Subjekty s vysokých dopadem nebo subjekty s kritickým dopadem oznámí jméno, poštovní adresu, e-mailovou adresu a telefonní číslo svého právního zástupce příslušnému orgánu v členském státě, ve kterém má tento právní zástupce bydliště nebo je usazen.

4. Určený právní zástupce může nést odpovědnost za neplnění povinností podle tohoto nařízení, aniž je dotčena odpovědnost a právní kroky, které by mohly být zahájeny proti samotnému subjektu s vysokým dopadem nebo subjektu s kritickým dopadem.

5. Pokud zástupce v Unii určený podle tohoto článku neexistuje, může kterýkoli členský stát, v němž subjekt poskytuje služby, podniknout právní kroky proti subjektu za neplnění povinností podle tohoto nařízení.

6. Určení právního zástupce v Unii podle odstavce 1 nepředstavuje usazení v Unii.

Článek 16

Spolupráce mezi ENTSO pro elektřinu a subjektem EU DSO

1. ENTSO pro elektřinu a subjekt EU DSO spolupracují při provádění posouzení kybernetických bezpečnostních rizik podle článků 19 a 21, a zejména při plnění těchto úkolů:

a) vývoj metodiky pro hodnocení kybernetických bezpečnostních rizik podle čl. 18 odst. 1;

b) vypracování zprávy o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny podle článku 23;

c) vypracování společného rámce kybernetické bezpečnosti elektřiny podle kapitoly III;

d) vypracování doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti podle článku 35;

e) vývoj metodiky stupnice pro klasifikaci kybernetických útoků podle čl. 37 odst. 8;

f) vypracování předběžného indexu dopadu na kybernetickou bezpečnost elektřiny (dále jen „ECII“) podle čl. 48 odst. 1 písm. a);

g) vypracování konsolidovaného předběžného seznamu subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 48 odst. 3;

h) vypracování předběžného seznamu procesů s vysokým dopadem na celou Unii a procesů s kritickým dopadem na celou Unii podle čl. 48 odst. 4;

i) vypracování prozatímního seznamu evropských a mezinárodních norem a kontrol podle čl. 48 odst. 6;

j) provádění posouzení kybernetických bezpečnostních rizik na celou Unii podle článku 19;

k) provádění posouzení kybernetických bezpečnostních rizik na úrovni regionů podle článku 21;

l) vymezení regionálních plánů ke zmírnění kybernetických bezpečnostních rizik podle článku 22;

m) vypracování pokynů týkajících se evropských systémů certifikace kybernetické bezpečnosti pro produkty IKT, služby IKT a procesy IKT v souladu s článkem 36;

n) vypracování pokynů pro provádění tohoto nařízení po konzultaci s ACER a ENISA.

2. Spolupráce mezi ENTSO pro elektřinu a subjektem EU DSO může mít podobu pracovní skupiny pro kybernetická bezpečnostní rizika.

3. ENTSO pro elektřinu a subjekt EU DSO pravidelně informují ACER, ENISA, skupinu pro spolupráci v oblasti bezpečnosti sítí a informací a Koordinační skupinu pro otázky elektrické energie o pokroku při provádění posouzení kybernetických bezpečnostních rizik na celou Unii a na úrovni regionů podle článků 19 a 21.

Článek 17

Spolupráce mezi ACER a příslušnými orgány

ACER ve spolupráci s každým příslušným orgánem:

1) sleduje provádění opatření k řízení kybernetických bezpečnostních rizik podle čl. 12 odst. 2 písm. a) a plnění oznamovacích povinností podle článků 27 a 39 a

2) sleduje proces přijímání a provádění podmínek, metodik nebo plánů podle čl. 6 odst. 2 a 3. Spolupráce mezi ACER, ENISA a jednotlivými příslušnými orgány může mít podobu subjektu pro sledování kybernetických bezpečnostních rizik.

KAPITOLA II

POSOUZENÍ RIZIK A URČENÍ PŘÍSLUŠNÝCH KYBERNETICKÝCH BEZPEČNOSTNÍCH RIZIK

Článek 18

Metodiky pro posuzování kybernetických bezpečnostních rizik

1. Do 13. března 2025 předloží provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu ve spolupráci se subjektem EU DSO a po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací návrh metodik pro posuzování kybernetických bezpečnostních rizik pro celou Unii, na regionální úrovni a na úrovni členských států.

2. Metodiky pro posuzování kybernetických bezpečnostních rizik na úrovni Unie, na regionální úrovni a na úrovni členských států zahrnují:

a) seznam kybernetických hrozeb, které je třeba zvážit, včetně minimálně těchto následujících hrozeb pro dodavatelský řetězec:

   i) závažné a neočekávané narušení dodavatelského řetězce;

   ii) nedostupnost produktů IKT, služeb IKT nebo procesů IKT z dodavatelského řetězce;

iii) kybernetické útoky iniciované aktéry v dodavatelském řetězci;

iv) únik citlivých informací v dodavatelském řetězci, včetně sledování dodavatelského řetězce;

v) zavedení slabých míst nebo „zadních vrátek“ do produktů ICT, služeb ICT nebo procesů ICT prostřednictvím aktérů v dodavatelském řetězci;

b) kritéria pro hodnocení dopadu kybernetických bezpečnostních rizik jako vysokých nebo kritických s využitím vymezených prahových hodnot pro důsledky a pravděpodobnost;

c) přístup k analýze kybernetických bezpečnostních rizik vyplývajících z původních systémů, kaskádových účinků kybernetických útoků a povahy systémů provozujících rozvodnou síť v reálném čase;

d) přístup k analýze kybernetických bezpečnostních rizik vyplývajících ze závislosti na jediném dodavateli produktů IKT, služeb IKT nebo procesů IKT.

3. Metodiky pro posuzování kybernetických bezpečnostních rizik na úrovni Unie, na regionální úrovni a na úrovni členských států posuzují kybernetická bezpečnostní rizika pomocí stejné matice dopadu rizik. Matice dopadu rizik:

a) měří důsledky kybernetických útoků na základě následujících kritérií:

i) ztráta zatížení;

ii) snížení výroby energie;

iii) ztráta kapacity v primární frekvenční rezervě;

iv) ztráta kapacity pro obnovení provozu elektrické sítě bez závislosti na vnější přenosové síti po úplném nebo částečném vypnutí (nazývaném také „start ze tmy“);

v) očekávaná doba trvání výpadku elektřiny, který ovlivní zákazníky, v kombinaci s rozsahem výpadku v počtu zákazníků a

vi) jakákoli jiná kvantitativní nebo kvalitativní kritéria, která by mohla přiměřeně sloužit jako ukazatel dopadu kybernetického útoku na přeshraniční toky elektřiny;

b) měří pravděpodobnost incidentu jako četnost kybernetických útoků za rok.

4. Metodiky pro posuzování kybernetických bezpečnostních rizik na úrovni Unie popisují, jak budou vymezeny hodnoty indexu ECII pro práh vysokého dopadu a práh kritického dopadu. Index ECII umožní subjektům odhadnout s pomocí kritérií uvedených v odst. 2 písm. a) dopad těchto rizik na jejich obchodní proces během posouzení obchodního dopadu, které provádějí podle čl. 26 odst. 4 písm. c) bodu i).

5. ENTSO pro elektřinu v koordinaci se subjektem EU DSO informuje Koordinační skupinu pro otázky elektrické energie o návrzích metodik posuzování kybernetických bezpečnostních rizik, které byly vypracovány podle odstavce 1.

Článek 19

Posouzení kybernetických bezpečnostních rizik pro celou Unii

1. Do devíti měsíců od schválení metodik pro hodnocení kybernetických bezpečnostních rizik podle článku 8 a poté každé tři roky provede ENTSO pro elektřinu ve spolupráci se subjektem EU DSO a po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, aniž je dotčen článek 22 směrnice (EU) 2022/2555, posouzení kybernetických bezpečnostních rizik pro celou Unii a vypracuje návrh zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii. Za tímto účelem použijí metodiky vypracované podle článku 18 a schválené podle článku 8, aby zjistily, analyzovaly a vyhodnotily možné důsledky kybernetických útoků, jež ovlivňují provozní bezpečnost elektrizační soustavy a narušují přeshraniční toky elektřiny. Při posouzení kybernetických bezpečnostních rizik pro celou Unii se nezvažuje právní a finanční újma ani újma na dobré pověsti způsobená kybernetickými útoky.

2. Zpráva o posouzení kybernetických bezpečnostních rizik pro celou Unie obsahuje tyto prvky:

a) procesy s vysokým dopadem na celou Unii a procesy s kritickým dopadem na celou Unii;

b) matice dopadu rizik, kterou subjekty a příslušné orgány použijí k posouzení kybernetického bezpečnostního rizika zjištěného při posouzení kybernetických bezpečnostních rizik na úrovni členských států provedeného podle článku 20 a při posouzení kybernetických bezpečnostních rizik na úrovni subjektů podle čl. 26 odst. 2 písm. b).

3. Pokud jde o procesy s vysokým dopadem na celou Unii a procesy s kritickým dopadem na celou Unii, zpráva o posouzení kybernetických bezpečnostních rizik pro celou Unii obsahuje:

a) posouzení možných důsledků kybernetického útoku s použitím metrik definovaných v metodice pro posuzování kybernetických bezpečnostních rizik vypracované podle čl. 18 odst. 2, 3 a 4 a schválené podle článku 8;

b) index ECII a prahy vysokého dopadu a kritického dopadu, které příslušné orgány použijí podle čl. 24 odst. 1 a 2 k určení subjektů s vysokým dopadem a subjektů s kritickým dopadem zapojených do procesů s vysokým dopadem na celou Unii a do procesů s kritickým dopadem na celou Unii.

4. Návrh zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii s výsledky posouzení kybernetických bezpečnostních rizik pro celou Unii předloží ENTSO pro elektřinu ve spolupráci se subjektem EU DSO ACER k vyjádření stanoviska. K návrhu zprávy vydá ACER stanovisko do tří měsíců od jejího obdržení. ENTSO pro elektřinu a subjekt EU DSO při dokončování této zprávy stanovisko ACER zohlední v nejvyšší míře.

5. Do tří měsíců od obdržení stanoviska ACER ENTSO pro elektřinu ve spolupráci se subjektem EU DSO předloží ACER, Komisi, ENISA a příslušným orgánům konečnou zprávu o posouzení kybernetických bezpečnostních rizik pro celou Unii.

Článek 20

Posouzení kybernetických bezpečnostních rizik na úrovni členských států

1. Každý příslušný orgán provede posouzení kybernetických bezpečnostních rizik na úrovni členského státu u všech subjektů s vysokým dopadem a subjektů s kritickým dopadem ve svém členském státě za použití metodik vypracovaných podle článku 18 a schválených podle článku 8. Posouzení kybernetických bezpečnostních rizik na úrovni členského státu určí a analyzuje rizika kybernetických útoků ovlivňujících provozní bezpečnost elektrizační soustavy a narušujících přeshraniční toky elektřiny. Při posouzení kybernetických bezpečnostních rizik na úrovni členského státu se nezvažuje právní a finanční újma ani újma na dobré pověsti způsobená kybernetickými útoky.

2. Každý příslušný orgán s podporou týmu CSIRT a po konzultaci s příslušným orgánem odpovědným za kybernetickou bezpečnost v elektroenergetice do 21 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6 a každé tři roky po tomto datu předloží ENTSO pro elektřinu a subjektu EU DSO zprávu o posouzení kybernetických bezpečnostních rizik na úrovni členského státu, která obsahuje tyto informace ohledně každého obchodního procesu s vysokým dopadem a procesu s kritickým dopadem:

a) stav provádění minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti podle článku 29;

b) seznam všech kybernetických útoků nahlášených v předchozích třech letech podle čl. 38 odst. 3;

c) souhrn informací o kybernetických hrozbách oznámených v předchozích třech letech podle čl. 38 odst. 6;

d) pro každý proces s vysokým dopadem na celou Unii nebo proces s kritickým dopadem na celou Unii odhad rizik ohrožení důvěrnosti, integrity a dostupnosti informací a příslušných aktiv;

e) v případě potřeby seznam dalších subjektů, které byly určeny jako subjekty s vysokým dopadem nebo subjekty s kritickým dopadem podle čl. 24 odst. 1, 2, 3 a 5.

3. Zpráva o posouzení kybernetických bezpečnostních rizik na úrovni členského státu zohlední plán rizikové připravenosti členského státu vypracovaný podle článku 10 nařízení (EU) 2019/941.

4. Informace obsažené ve zprávě o posouzení kybernetických bezpečnostních rizik na úrovni členského státu podle odst. 2 písm. a) až d) nesouvisí s konkrétními subjekty nebo aktivy. Zpráva o posouzení kybernetických bezpečnostních rizik na úrovni členského státu rovněž zahrnuje posouzení rizik vyplývajících z dočasných výjimek vydaných příslušnými orgány členských států podle článku 30.

5. ENTSO pro elektřinu a subjekt EU DSO si mohou od příslušných orgánů vyžádat další informace týkající se úkolů stanovených v odst. 2 písm. a) a c).

6. Příslušné orgány zajistí, aby informace, které poskytují, byly přesné a správné.

Článek 21

Posouzení kybernetických bezpečnostních rizik na úrovni regionů

1. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO a po konzultaci s příslušným regionálním koordinačním centrem provede posouzení kybernetických bezpečnostních rizik na úrovni regionů pro každý region pro provoz soustavy za použití metodik vypracovaných podle článku 19 a schválených podle článku 8 s cílem určit, analyzovat a vyhodnotit rizika kybernetických útoků ovlivňujících provozní bezpečnost elektrizační soustavy a narušujících přeshraniční toky elektřiny. Při posouzení kybernetických bezpečnostních rizik na úrovni regionů se nezvažuje právní a finanční újma ani újma na dobré pověsti způsobená kybernetickými útoky.

2. Do 30 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6 a poté každé tři roky vypracuje ENTSO pro elektřinu ve spolupráci se subjektem EU DSO a po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací zprávu o posouzení kybernetických bezpečnostních rizik na úrovni regionu pro každý region pro provoz soustavy.

3. Zpráva o posouzení kybernetických bezpečnostních rizik na úrovni regionu musí zohlednit příslušné informace obsažené ve zprávách o posouzení kybernetických bezpečnostních rizik pro celou Unii a ve zprávách o posouzení kybernetických bezpečnostních rizik na úrovni členských států.

4. Posouzení kybernetických bezpečnostních rizik na úrovni regionu musí zohlednit regionální scénáře elektroenergetických krizí související s kybernetickou bezpečností zjištěné podle článku 6 nařízení (EU) 2019/941.

Článek 22

Regionální plány ke zmírnění kybernetických bezpečnostních rizik

1. Do 36 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6, nejpozději však do 13. června 2031, a každé tři roky po tomto datu vypracují provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu, ve spolupráci se subjektem EU DSO a po konzultaci s regionálními koordinačními centry a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací regionální plán ke zmírnění kybernetických bezpečnostních rizik pro každý region pro provoz soustavy.

2. Regionální plány ke zmírnění kybernetických bezpečnostních rizik zahrnují:

a) minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti, které musí subjekty s vysokým dopadem a subjekty s kritickým dopadem uplatňovat v daném regionu pro provoz soustavy;

b) zbytková kybernetická bezpečnostní rizika v regionech pro provoz soustavy po uplatnění kontrol uvedených v písmeni a).

3. ENTSO pro elektřinu předloží regionální plány ke zmírnění rizik příslušným provozovatelům přenosových soustav, příslušným orgánům a Koordinační skupině pro otázky elektrické energie. Koordinační skupina pro otázky elektrické energie může doporučit změny.

4. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu, ve spolupráci se subjektem EU DSO a po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací aktualizují regionální plány ke zmírnění rizik každé tři roky, pokud okolnosti nevyžadují častější aktualizace.

Článek 23

Zpráva o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny

1. Do 40 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6 a poté každé tři roky provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu, ve spolupráci se subjektem EU DSO a po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací předloží Koordinační skupině pro otázky elektrické energie zprávu o výsledku posouzení kybernetických bezpečnostních rizik s ohledem na přeshraniční toky elektřiny (dále jen „zpráva o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny“).

2. Zpráva o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny vychází ze zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii, zpráv o posouzení kybernetických bezpečnostních rizik na úrovni členských států a zpráv o posouzení kybernetických bezpečnostních rizik na úrovni regionů a obsahuje tyto informace:

a) seznam procesů s vysokým dopadem na celou Unii a procesů s kritickým dopadem na celou Unii zjištěných ve zprávě o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 2 písm. a), včetně odhadu pravděpodobnosti a dopadu kybernetických bezpečnostních rizik vyhodnocených při vypracování zpráv o posouzení kybernetických bezpečnostních rizik na regionální úrovni čl. 21 odst. 2 a čl. 19 odst. 3 písm. a);

b) aktuální kybernetické hrozby, se zvláštním zaměřením na vznikající hrozby a rizika pro elektrizační soustavu;

c) kybernetické útoky za předchozí období na úrovni Unie, s poskytnutím kritického přehledu o tom, jaký dopad mohly mít tyto kybernetické útoky na přeshraniční toky elektřiny;

d) celkový stav provádění opatření v oblasti kybernetické bezpečnosti;

e) stav provádění informačních toků podle článků 37 a 38;

f) seznam informací nebo zvláštních kritérií pro klasifikaci informací podle článku 46;

g) zjištěná a zvýrazněná rizika, která mohou vyplývat z nezabezpečeného řízení dodavatelského řetězce;

h) výsledky a získané poznatky z regionálních a meziregionálních cvičení v oblasti kybernetické bezpečnosti pořádaných podle článku 44;

i) analýza vývoje celkových přeshraničních kybernetických bezpečnostních rizik v odvětví elektroenergetiky od posledního posouzení kybernetických bezpečnostních rizik na úrovni regionů;

j) jakékoli další informace, které mohou být užitečné pro určení možných zlepšení tohoto nařízení nebo potřeby revize tohoto nařízení nebo některého z jeho nástrojů; a

k) souhrnné a anonymizované informace o výjimkách udělených podle čl. 30 odst. 3.

3. Subjekty uvedené v čl. 2 odst. 1 mohou přispívat k vypracování zprávy o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny, přičemž musí respektovat důvěrnost informací v souladu s článkem 47. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO konzultují tyto subjekty již od počáteční fáze.

4. Na zprávu o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny se vztahují pravidla o ochraně výměny informací podle článku 46. Aniž jsou dotčena ustanovení čl. 10 odst. 4 a čl. 47 odst. 4, ENTSO pro elektřinu a subjekt EU DSO zveřejní veřejné znění této zprávy, které nesmí obsahovat informace, jež mohou způsobit újmu subjektům uvedeným v čl. 2 odst. 1. Veřejné znění této zprávy bude zveřejněno pouze se souhlasem skupiny pro spolupráci v oblasti bezpečnosti sítí a informací a Koordinační skupiny pro otázky elektrické energie. Za sestavení a zveřejnění veřejného znění zprávy odpovídá ENTSO pro elektřinu v koordinaci se subjektem EU DSO.

Článek 24

Určení subjektů s vysokým dopadem a subjektů s kritickým dopadem

1. Každý příslušný orgán určí pomocí indexu ECII a prahů vysokého dopadu a prahů kritického dopadu uvedených ve zprávě o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 3 písm. b) subjekty s vysokým dopadem a subjekty s kritickým dopadem ve svém členském státě, které jsou zapojeny do procesů s vysokým dopadem na celou Unii a do procesů s kritickým dopadem na celou Unii. Příslušné orgány si mohou vyžádat informace od subjektu ve svém členském státě, aby mohly určit hodnoty indexu ECII pro tento subjekt. Pokud je zjištěná hodnota indexu ECII u subjektu vyšší než práh vysokého dopadu nebo práh kritického dopadu, uvede se určený subjekt ve zprávě o posouzení kybernetických bezpečnostních rizik na úrovni členského státu podle čl. 20 odst. 2.

2. Každý příslušný orgán určí pomocí indexu ECII a prahu vysokého dopadu a prahu kritického dopadu obsažených ve zprávě o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 3 písm. b) subjekty s vysokým dopadem a subjekty s kritickým dopadem, které nejsou usazeny v Unii, pokud působí v Unii. Příslušný orgán si může vyžádat informace od subjektu, který není usazen v Unii, za účelem stanovení hodnot indexu ECII pro tento subjekt.

3. Každý příslušný orgán může ve svém členském státě určit další subjekty jako subjekty s vysokým dopadem nebo subjekty s kritickým dopadem, jsou-li splněna tato kritéria:

a) subjekt je součástí skupiny subjektů, u nichž existuje významné riziko, že budou kybernetickým útokem zasaženy současně;

b) hodnota indexu ECII agregovaná za skupinu subjektů je vyšší než práh vysokého dopadu nebo práh kritického dopadu.

4. Určí-li příslušný orgán další subjekty v souladu s odstavcem 3, považují se všechny procesy v těchto subjektech, u nichž jsou hodnoty indexu ECII agregované za skupinu vyšší než práh vysokého dopadu, za procesy s vysokým dopadem a všechny procesy v těchto subjektech, u nichž jsou hodnoty indexu ECII agregované za skupinu vyšší než prahy kritického dopadu, se považují za procesy s kritickým dopadem.

5. Určí-li příslušný orgán subjekty uvedené v odst. 3 písm. a) ve více než jednom členském státě, informuje o tom ostatní příslušné orgány, ENTSO pro elektřinu a subjekt EU DSO. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO na základě informací obdržených od všech příslušných orgánů poskytne příslušným orgánům analýzu agregace subjektů ve více než jednom členském státě, která může způsobit distribuované narušení přeshraničních toků elektřiny a může vést ke kybernetickému útoku. Je-li skupina subjektů v několika členských státech určena jako agregace, jejíž index ECII je vyšší než práh vysokého dopadu nebo práh kritického dopadu, všechny dotčené příslušné orgány určí subjekty v této skupině jako subjekty s vysokým dopadem nebo subjekty s kritickým dopadem pro svůj příslušný členský stát na základě agregovaného indexu ECII pro skupinu subjektů a určené subjekty se uvedou ve zprávě o posouzení kybernetických bezpečnostních rizik pro celou Unii.

6. Každý příslušný orgán do devíti měsíců poté, co mu ENTSO pro elektřinu a subjekt EU DSO oznámí zprávu o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 5, nejpozději však do 13. června 2028, oznámí subjektům uvedeným na seznamu, že byly v jeho členském státě určeny jako subjekty s vysokým nebo subjekty s kritickým dopadem.

7. Je-li poskytovatel služeb oznámen příslušnému orgánu jako poskytovatel kritických služeb IKT podle čl. 27 písm. c), oznámí to tento příslušný orgán příslušným orgánům členských států, na jejichž území má tento poskytovatel služeb sídlo nebo zástupce. Posledně uvedený příslušný orgán oznámí poskytovateli služeb, že byl označen za poskytovatele kritických služeb.

Článek 25

Vnitrostátní systémy ověřování

1. Příslušné orgány mohou zavést vnitrostátní systém ověřování k ověření toho, že subjekty s kritickým dopadem určené podle čl. 24 odst. 1 zavedly vnitrostátní legislativní rámec, který je obsažen v mapovací matici uvedené v článku 34. Vnitrostátní systém ověřování může být založen na inspekci prováděné příslušným orgánem, nezávislých bezpečnostních auditech nebo vzájemných hodnoceních prováděných subjekty s kritickým dopadem ve stejném členském státě, ve kterém příslušný orgán vykonává dohled.

2. Rozhodne-li se příslušný orgán zavést vnitrostátní systém ověřování, zajistí, aby ověřování bylo prováděno v souladu s následujícími požadavky:

a) každá strana provádějící vzájemné hodnocení, audit nebo inspekci musí být nezávislá na ověřovaném subjektu s kritickým dopadem a nesmí být ve střetu zájmů;

b) pracovníci provádějící vzájemné hodnocení, audit nebo inspekci musí mít prokazatelné znalosti o:

   i) kybernetické bezpečnosti v odvětví elektrické energie;

   ii) systémech řízení kybernetické bezpečnosti;

   iii) zásadách provádění auditů;

   iv) posuzování kybernetických bezpečnostních rizik;

   v) společném rámci kybernetické bezpečnosti elektřiny;

   vi) vnitrostátním legislativním a regulačním rámci a evropských a mezinárodních normách v oblasti působnosti ověřování;

   vii) procesech s kritickým dopadem v oblasti působnosti ověřování;

c) strana provádějící vzájemné hodnocení, audit nebo inspekci musí mít na tyto činnosti dostatek času;

d) strana provádějící vzájemné hodnocení, audit nebo inspekci přijme vhodná opatření k ochraně informací, které shromáždí během ověřování, v souladu s úrovní jejich důvěrnosti; a

e) vzájemná hodnocení, audity nebo inspekce se provádějí nejméně jednou ročně a nejméně jednou za tři roky musí zahrnovat ověření v celém rozsahu.

3. Rozhodne-li se příslušný orgán zavést vnitrostátní systém ověřování, podává každoročně agentuře ACER zprávu o četnosti kontrol provedených v rámci tohoto systému.

Článek 26

Řízení kybernetických bezpečnostních rizik na úrovni subjektů

1. Každý subjekt s vysokým dopadem a každý subjekt s kritickým dopadem určený příslušnými orgány podle čl. 24 odst. 1 provádí řízení kybernetických bezpečnostních rizik pro všechna svá aktiva v perimetru vysokého dopadu a perimetru kritického dopadu. Každý subjekt s vysokým dopadem a subjekt s kritickým dopadem provádí každé tři roky řízení rizik, jež obsahuje fáze uvedené v odstavci 2.

2. Každý subjekt s vysokým dopadem a subjekt s kritickým dopadem musí při řízení kybernetických bezpečnostních rizik vycházet z přístupu, jehož cílem je chránit jeho síť a informační systémy a který zahrnuje tyto fáze:

a) stanovení kontextu;

b) posouzení kybernetických bezpečnostních rizik na úrovni subjektu;

c) řešení kybernetických bezpečnostních rizik;

d) přijetí kybernetických bezpečnostních rizik.

3. Ve fázi stanovení kontextu každý subjekt s vysokým dopadem a každý subjekt kritickým dopadem:

a) vymezí rozsah posouzení rizik kybernetické bezpečnosti, včetně procesů s vysokým dopadem a procesů s kritickým dopadem, které určil ENTSO pro elektřinu a subjekt EU DSO, a dalších procesů, které mohou být cílem kybernetických útoků s vysokým nebo kritickým dopadem na přeshraniční toky elektřiny; a

b) vymezí kritéria pro hodnocení rizik a pro přijetí rizik v souladu s maticí dopadu rizik, kterou subjekty a příslušné orgány používají k posuzování kybernetických bezpečnostních rizik v rámci metodik posuzování kybernetických bezpečnostních rizik na úrovni Unie, na regionální úrovni a na úrovni členských států, které vypracovaly ENTSO pro elektřinu a subjekt EU DSO v souladu s čl. 19 odst. 2.

4. Ve fázi posuzování kybernetických bezpečnostních rizik každý subjekt s vysokým dopadem a subjekt s kritickým dopadem:

a) určí kybernetická bezpečnostní rizika se zohledněním:

   i) všech aktiv, která podporují procesy s vysokým dopadem na celou Unii a procesy s kritickým dopadem na celou Unii, s posouzením možného dopadu na přeshraniční toky elektřiny v případě, že by tato aktiva byla ohrožena;

   ii) možných kybernetických hrozeb se zohledněním kybernetických hrozeb určených v nejnovější zprávě o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny uvedené v článku 23 a hrozeb pro dodavatelský řetězec;

   iii) zranitelnosti, včetně zranitelnosti v původních systémech;

   iv) možných scénářů kybernetických útoků, včetně kybernetických útoků ovlivňujících provozní bezpečnost elektrizační soustavy a narušujících přeshraniční toky elektřiny;

   v) příslušných hodnocení a posouzení rizik prováděných na úrovni Unie, včetně koordinovaných posouzení rizik kritických dodavatelských řetězců v souladu s článkem 22 směrnice (EU) 2022/2555; a

   vi) stávajících zavedených kontrol;

b) analyzují pravděpodobnost a důsledky kybernetických bezpečnostních rizik určených v písmeni a) a určí úroveň kybernetických bezpečnostních rizik za použití matice dopadu rizik používané k posuzování kybernetických bezpečnostních rizik v rámci metodik posuzování kybernetických bezpečnostních rizik na úrovni Unie, na regionální úrovni a na úrovni členských států, které vypracovali provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO v souladu s čl. 19 odst. 2;

c) klasifikují aktiva podle možných důsledků při narušení kybernetické bezpečnosti a určí perimetr vysokého dopadu a perimetr kritického dopadu pomocí těchto kroků:

   i) u všech procesů, na které se vztahuje posouzení kybernetických bezpečnostních rizik, se provede posouzení obchodních dopad za použití indexu ECII;

   ii) proces se klasifikuje jako proces s vysokým dopadem nebo proces s kritickým dopadem, pokud je jeho index ECII vyšší než práh vysokého dopadu, respektive práh kritického dopadu;

   iii) všechna aktiva s vysokým dopadem a aktiva s kritickým dopadem se určí jako aktiva potřebná pro procesy s vysokým dopadem, respektive pro procesy s kritickým dopadem;

   iv) vymezí se perimetr vysokého dopadu a perimetr kritického dopadu, který obsahuje všechna aktiva s vysokým dopadem, respektive aktiva s kritickým dopadem tak, aby bylo možné kontrolovat přístup k perimetru;

d) vyhodnotí kybernetická bezpečnostní rizika stanovením jejich priority prostřednictvím kritérií pro hodnocení rizik a kritérií pro přijetí rizik uvedených v odst. 3 písm. b).

5. Během fáze řešení kybernetických bezpečnostních rizik každý subjekt s vysokým dopadem a subjekt s kritickým dopadem vypracuje plán ke zmírnění rizik na úrovni subjektu tím, že zvolí možnosti řešení rizik vhodné pro řízení rizik a určení zbytkových rizik.

6. Ve fázi přijetí kybernetického bezpečnostního rizika se každý subjekt s vysokým dopadem a subjekt s kritickým dopadem rozhodne, zda přijme zbytkové riziko na základě kritérií pro přijetí rizik stanovených v odst. 3 písm. b).

7. Každý subjekt s vysokým dopadem a subjekt s kritickým dopadem zaeviduje aktiva určená v odstavci 1 v seznamu aktiv. Tento seznam aktiv není součástí zprávy o posouzení rizik.

8. Aktiva v seznamu může příslušný orgán zkontrolovat při kontrolách.

Článek 27

Podávání zpráv o posouzení rizik na úrovni subjektu

Každý subjekt s vysokým dopadem a subjekt s kritickým dopadem do 12 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6 a poté každé tři roky předloží příslušnému orgánu zprávu obsahující tyto informace:

1) seznam kontrol vybraných pro plán ke zmírnění rizik na úrovni subjektu podle čl. 26 odst. 5 s aktuálním stavem provádění každé kontroly;

2) pro každý proces s vysokým dopadem na celou Unii nebo proces s kritickým dopadem na celou Unii odhad rizika ohrožení důvěrnosti, integrity a dostupnosti informací a příslušných aktiv. Odhad tohoto rizika se uvede v souladu s maticí dopadu rizik uvedenou v čl. 19 odst. 2;

3) seznam poskytovatelů kritických služeb IKT pro jejich procesy s kritickým dopadem.

KAPITOLA III

SPOLEČNÝ RÁMEC KYBERNETICKÉ BEZPEČNOSTI ELEKTŘINY

Článek 28

Složení, fungování a přezkum společného rámce kybernetické bezpečnosti elektřiny

1. Společný rámec kybernetické bezpečnosti elektřiny se skládá z následujících kontrolních mechanismů a systému řízení kybernetické bezpečnosti:

a) minimální kontroly v oblasti kybernetické bezpečnosti vypracované v souladu s článkem 29;

b) minimální kontroly v oblasti kybernetické bezpečnosti vypracované v souladu s článkem 29;

c) mapovací matice vypracované v souladu s článkem 34, která mapuje kontroly uvedené v písmenech a) a b) podle vybraných evropských a mezinárodních norem a vnitrostátních právních nebo regulačních rámců;

d) systém řízení kybernetické bezpečnosti zavedený podle článku 32.

2. Všechny subjekty s vysokým dopadem uplatňují minimální kontroly v oblasti kybernetické bezpečnosti podle odst. 1 písm. a) v rámci svého perimetru vysokého dopadu.

3. Všechny subjekty s kritickým dopadem uplatňují pokročilé kontroly v oblasti kybernetické bezpečnosti podle odst. 1 písm. b) v rámci svého perimetru kritického dopadu.

4. Do sedmi měsíců od předložení prvního návrhu zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 4 se společný rámec kybernetické bezpečnosti elektřiny uvedený v odstavci 1 doplní o minimální a pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci vypracované podle článku 33.

Článek 29

Minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti

1. Do sedmi měsíců od předložení prvního návrhu zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 4 vypracují provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO návrh minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti.

2. Do šesti měsíců od vypracování každé zprávy o posouzení kybernetických bezpečnostních rizik na úrovni regionu podle čl. 21 odst. 2 provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO navrhnou příslušnému orgánu změnu minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti. Návrh bude proveden v souladu s čl. 8 odst. 10 a zohlední rizika zjištěná při posouzení rizik na úrovni regionu.

3. Minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti jsou ověřitelné účastí ve vnitrostátním systému ověřování v souladu s postupem stanoveným v článku 31 nebo absolvováním nezávislých bezpečnostních auditů prováděných třetí stranou v souladu s požadavky uvedenými v čl. 25 odst. 2.

4. Počáteční minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti vypracované podle odstavce 1 vycházejí z rizik, která byla zjištěna ve zprávě o posouzení kybernetických bezpečnostních rizik pro celou Unii uvedené v čl. 19 odst. 5. Pozměněné minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti vypracované podle odstavce 2 vycházejí ze zprávy o posouzení kybernetických bezpečnostních rizik na úrovni regionu uvedené v čl. 21 odst. 2.

5. Minimální kontroly v oblasti kybernetické bezpečnosti zahrnují kontroly na ochranu informací vyměňovaných podle článku 46.

6. Do 12 měsíců od schválení minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti podle čl. 8 odst. 5 nebo po každé aktualizaci podle čl. 8 odst. 10 uplatní subjekty uvedené v čl. 2 odst. 1 a označené jako subjekty s kritickým dopadem a subjekty s vysokým dopadem podle článku 24 během zavádění plánu ke snižování rizik na úrovni subjektu podle čl. 26 odst. 5 minimální kontroly v oblasti kybernetické bezpečnosti v perimetru vysokého dopadu a pokročilé kontroly v oblasti kybernetické bezpečnosti v perimetru kritického dopadu.

Článek 30

Odchylky od minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti

1. Subjekty uvedené v čl. 2 odst. 1 mohou požádat příslušný orgán o udělení výjimky z povinnosti uplatňovat minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti uvedené v čl. 29 odst. 6. Příslušný orgán může tuto výjimku udělit z jednoho z těchto důvodů:

a) ve výjimečných případech, kdy subjekt prokáže, že náklady na zavedení příslušných kontrol v oblasti kybernetické bezpečnosti výrazně převyšují přínosy. ACER a ENTSO pro elektřinu mohou ve spolupráci se subjektem DSO společně vypracovat pokyny pro odhad nákladů na kontroly v oblasti kybernetické bezpečnosti, které subjektům pomohou;

b) pokud subjekt předloží plán řešení rizik na úrovni subjektu, který zmírňuje kybernetická bezpečnostní rizika pomocí alternativních kontrolních mechanismů na úroveň, která je přijatelná v souladu s kritérii pro přijetí rizik uvedenými v čl. 26 odst. 3 písm. b).

2. Do tří měsíců od obdržení žádosti uvedené v odstavci 1 každý příslušný orgán rozhodne, zda výjimka z minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti má být udělena. Odchylky od minimálních nebo pokročilých kontrol v oblasti kybernetické bezpečnosti se udělují na dobu nejvýše tří let s možností prodloužení.

3. Souhrnné a anonymizované informace o udělených výjimkách se připojí jako příloha ke zprávě o komplexním posouzení kybernetických bezpečnostních rizik pro přeshraniční toky elektřiny uvedené v článku 23. ENTSO pro elektřinu a subjekt EU DSO tento seznam v případě potřeby společně aktualizují.

Článek 31

Ověření společného rámce kybernetické bezpečnosti elektřiny

1. Nejpozději 24 měsíců od přijetí kontrol uvedených v čl. 28 odst. 1 písm. a), b) a c) a zavedení systému řízení kybernetické bezpečnosti uvedeného v čl. 28 odst. 1 písm. d) musí být každý subjekt s kritickým dopadem určený v souladu s čl. 24 odst. 1 schopen na žádost příslušného orgánu prokázat, že dodržuje systém řízení kybernetické bezpečnosti a minimální nebo pokročilé kontroly v oblasti kybernetické bezpečnosti.

2. Každý subjekt s kritickým dopadem splní povinnost uvedenou v odstavci 1 buď absolvováním nezávislého bezpečnostního auditu provedeného třetí stranou v souladu s požadavky uvedenými v čl. 25 odst. 2, nebo účastní ve vnitrostátním systému ověřování v souladu s čl. 25 odst. 1.

3. Ověření, zda subjekt s kritickým dopadem dodržuje systém řízení kybernetické bezpečnosti a minimální nebo pokročilé kontroly v oblasti kybernetické bezpečnosti, se vztahuje na všechna aktiva v perimetru subjektu s kritickým dopadem.

4. Ověření, zda subjekt s kritickým dopadem dodržuje systém řízení kybernetické bezpečnosti a minimální nebo pokročilé kontroly v oblasti kybernetické bezpečnosti, se pravidelně opakuje nejpozději 36 měsíců od skončení prvního ověření a poté každé tři roky.

5. Každý subjekt s kritickým dopadem určený v souladu s článkem 24 prokáže soulad s kontrolami uvedenými v čl. 28 odst. 1 písm. a), b) a c) a zavedení systému řízení kybernetické bezpečnosti uvedeného v čl. 28 odst. 1 písm. d) tím, že podá příslušnému orgánu zprávu o výsledku ověření souladu.

Článek 32

Systém řízení kybernetické bezpečnosti

1. Do 24 měsíců poté, co jim příslušný orgán oznámil, že byly určeny jako subjekt s vysokým dopadem nebo subjekt s kritickým dopadem v souladu s čl. 24 odst. 6, zavede každý subjekt s vysokým dopadem a subjekt s kritickým dopadem systém řízení kybernetické bezpečnosti a následně jej každé tři roky přezkoumá s cílem:

a) určit oblast působnosti systému řízení kybernetické bezpečnosti s ohledem na rozhraní a závislosti s jinými subjekty;

b) zajistit, aby byli všichni jeho vedoucí pracovníci informováni o příslušných právních povinnostech a aktivně přispívali k zavádění systému řízení kybernetické bezpečnosti prostřednictvím včasných rozhodnutí a pohotových reakcí;

c) zajistit, aby byly pro systém řízení kybernetické bezpečnosti k dispozici potřebné zdroje;

d) stanovit zásady kybernetické bezpečnosti, které musí být zdokumentovány a sděleny v rámci subjektu a stranám, jichž se bezpečnostní rizika týkají;

e) přidělit a sdělovat odpovědnost za úlohy související s kybernetickou bezpečností;

f) provádět řízení kybernetických bezpečnostních rizik na úrovni subjektu vymezených v článku 26;

g) určit a zajistit zdroje potřebné pro zavedení, údržbu a neustálé zlepšování systému řízení kybernetické bezpečnosti s ohledem na potřebné kompetence a povědomí o zdrojích kybernetické bezpečnosti;

h) určit interní a externí komunikaci, která se týká kybernetické bezpečnosti;

i) vytvářet, aktualizovat a kontrolovat zdokumentované informace týkající se systému řízení kybernetické bezpečnosti;

j) vyhodnotit výkonnost a účinnost systému řízení kybernetické bezpečnosti;

k) v plánovaných intervalech provádět interní audity, aby se zajistilo, že systém řízení kybernetické bezpečnosti je účinně zaveden a udržován;

l) v plánovaných intervalech přezkoumávat zavedený systém řízení kybernetické bezpečnosti a kontrolovat a napravovat nesoulad zdrojů a činností se zásadami, postupy a pokyny v systému řízení kybernetické bezpečnosti.

2. Oblast působnosti systému řízení kybernetické bezpečnosti musí zahrnovat všechna aktiva v perimetru vysokého dopadu a v perimetru kritického dopadu subjektu s vysokým dopadem a subjektu s kritickým dopadem.

3. Příslušné orgány podporují používání evropských nebo mezinárodních norem a specifikací týkajících se systémů řízení a souvisejících s bezpečností sítí a informačních systémů, aniž by vnucovaly nebo diskriminovaly používání určitého druhu technologie.

Článek 33

Minimální a pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci

1. Do sedmi měsíců od předložení prvního návrhu zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 4 provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO vypracují návrh minimálních a pokročilých kontrol kybernetické bezpečnosti v dodavatelském řetězci, které zmírňují rizika dodavatelského řetězce zjištěná při posouzení kybernetických bezpečnostních rizik pro celou Unii a které doplňují minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti vypracované podle článku 29. Minimální a pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci se vypracovávají spolu s minimálními a pokročilými kontrolami v oblasti kybernetické bezpečnosti podle článku 29. Minimální a pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci musí zahrnovat celý životní cyklus všech produktů IKT, služeb IKT a procesů IKT uvnitř perimetru vysokého dopadu nebo perimetru kritického dopadu subjektu s vysokým dosahem nebo subjektu s kritickým dopadem. Při vypracování návrhu minimálních a pokročilých kontrol kybernetické bezpečnosti v dodavatelském řetězci se konzultuje skupina pro spolupráci v oblasti bezpečnosti sítí a informací.

2. Minimální kontroly kybernetické bezpečnosti v dodavatelském řetězci se skládají z kontrol pro subjekty s vysokým dopadem a subjekty s kritickým dopadem, které:

a) zahrnují doporučení pro zadávání zakázek na produkty IKT, služby IKT a procesy IKT, která se týkají specifikací kybernetické bezpečnosti a zahrnují alespoň:

   i) ověřování spolehlivosti zaměstnanců dodavatele zapojených do dodavatelského řetězce, kteří nakládají s citlivými informacemi nebo mají přístup k aktivům s vysokým dopadem nebo aktivům s kritickým dopadem. Ověřování spolehlivosti může zahrnovat ověření totožnosti a biografických údajů zaměstnanců nebo smluvních partnerů subjektu v souladu s vnitrostátním právem a postupy a s příslušným a použitelným právem Unie, včetně nařízení (EU) 2016/679 a směrnice Evropského parlamentu a Rady (EU) 2016/680 ([18]). Ověřování spolehlivosti musí být přiměřené a přísně omezeno na to, co je nezbytné. Provádí se výhradně za účelem vyhodnocení potenciálního bezpečnostního rizika pro dotčený subjekt. Musí být úměrné obchodním požadavkům, stupni utajení informací, k nimž má být poskytnut přístup, a vnímaným rizikům a mohou být prováděny subjektem samotným, externí společností provádějící prověrky nebo prostřednictvím vládní prověrky;

   ii) procesy bezpečného a kontrolovaného návrhu, vývoje a výroby produktů IKT, služeb IKT a procesů IKT, podporu návrhu a vývoje produktů IKT, služeb IKT a procesů IKT, které zahrnují vhodná technická opatření k zajištění kybernetické bezpečnosti;

   iii) návrh sítí a informačních systémů, v nichž zařízení nejsou důvěryhodná, i když se nacházejí v zabezpečeném perimetru, vyžadují ověření všech přijatých požadavků a uplatňují zásadu minimálních práv;

   iv) přístup dodavatele k aktivům subjektu;

([18]) Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

v) smluvní povinnost dodavatele chránit citlivé informace subjektu a omezit k nim přístup;

vi) specifikace podkladů pro zadávání zakázek v oblasti kybernetické bezpečnosti subdodavatelům dodavatele;

vii) sledovatelnost uplatňování specifikací kybernetické bezpečnosti od vývoje přes výrobu až po dodání produktů IKT, služeb IKT nebo procesů IKT;

viii) podporu bezpečnostních aktualizací po celou dobu životnosti produktů IKT, služeb IKT nebo procesů IKT;

ix) právo kontrolovat kybernetickou bezpečnost v procesu návrhu, vývoje a výroby u dodavatele a

x) posouzení rizikového profilu dodavatele;

b) vyžadují, aby tyto subjekty při uzavírání smluv s dodavateli, spolupracujícími partnery a dalšími stranami v dodavatelském řetězci zohledňovaly doporučení pro zadávání zakázek uvedená v písmeni a), která se týkají běžných dodávek produktů IKT, služeb IKT a procesů IKT, jakož i nevyžádaných událostí a okolností, jako je ukončení a převod smluv v případech nedbalosti smluvního partnera;

c) vyžadují, aby tyto subjekty zohlednily výsledky příslušných koordinovaných posouzení bezpečnostních rizik kritických dodavatelských řetězců provedených v souladu s čl. 22 odst. 1 směrnice (EU) 2022/2555;

d) zahrnují kritéria pro výběr dodavatelů a uzavírání smluv s dodavateli, kteří mohou splnit specifikace kybernetické bezpečnosti uvedené v písmenu a) a kteří mají úroveň kybernetické bezpečnosti odpovídající kybernetickým bezpečnostním rizikům produktu IKT, služby IKT nebo procesů IKT, které dodavatel dodává;

e) zahrnují kritéria pro diverzifikaci zdrojů dodávek produktů IKT, služeb IKT a procesů IKT a omezují riziko proprietárního uzamčení;

f) zahrnují kritéria pro pravidelné sledování, přezkum nebo audit specifikací kybernetické bezpečnosti interních provozních procesů dodavatele v průběhu celého životního cyklu každého produktu IKT, služby IKT a procesu IKT.

3. Pro specifikace kybernetické bezpečnosti v doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti uvedeném v odst. 2 písm. a) použijí subjekty s vysokým dopadem nebo subjekty s kritickým dopadem zásady zadávání veřejných zakázek podle směrnice Evropského parlamentu a Rady (ES) 2014/24/EU ([19]) v souladu s čl. 35 odst. 4, nebo stanoví vlastní specifikace na základě výsledků posouzení kybernetických bezpečnostních rizik na úrovni subjektu.

4. Pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci zahrnují kontroly u subjektů s kritickým dopadem s cílem ověřit během zadávání zakázek, že produkty IKT, služby IKT a procesy IKT, které budou používány jako aktiva s kritickým dopadem, splňují specifikace kybernetické bezpečnosti. Produkt IKT, služba IKT nebo proces IKT musí být ověřeny buď prostřednictvím evropského systému certifikace kybernetické bezpečnosti uvedeného v článku 31, nebo prostřednictvím ověřovacích činností, které si subjekt zvolí a zorganizuje. Hloubka a rozsah ověřovacích činností musí být dostatečné, aby poskytly jistotu, že produkt IKT, službu IKT nebo proces IKT lze použít ke zmírnění rizik zjištěných při posouzení rizik na úrovni subjektu. Subjekt s kritickým dopadem kroky přijaté k omezení zjištěných rizik zdokumentuje.

5. Minimální a pokročilé kontroly kybernetické bezpečnosti v dodavatelském řetězci se vztahují na zadávání zakázek na příslušné produkty IKT, služby IKT a procesy IKT. Minimální a pokročilé kontroly kybernetické bezpečnosti dodavatelského řetězce se budou vztahovat na procesy zadávání zakázek v rámci subjektů označených jako subjekty s kritickým dopadem a subjekty s vysokým dopadem podle článku 24, které budou zahájeny šest měsíců po přijetí nebo aktualizaci minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti uvedených v článku 29.

([19]) Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

6. Do šesti měsíců od vypracování každé zprávy o posouzení kybernetických bezpečnostních rizik na úrovni regionů podle čl. 21 odst. 2 navrhnou provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO příslušnému orgánu změnu minimálních a pokročilých kontrol kybernetické bezpečnosti v dodavatelském řetězci. Návrh bude proveden v souladu s čl. 8 odst. 10 a zohlední rizika zjištěná při posouzení rizik na úrovni regionu.

Článek 34

Mapovací matice pro kontroly kybernetické bezpečnosti elektřiny na základě norem

1. Do sedmi měsíců od předložení prvního návrhu zprávy o posouzení kybernetických bezpečnostních rizik pro celou Unii podle čl. 19 odst. 4 vypracují provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO a po konzultaci s ENISA návrh matice pro mapování kontrol uvedených v čl. 28 odst. 1 písm. a) a b) podle vybraných evropských a mezinárodních norem, jakož i podle příslušných technických specifikací (dále jen „mapovací matice“). ENTSO pro elektřinu a subjekt EU DSO zdokumentují rovnocennost různých kontrol s kontrolami uvedenými v čl. 28 odst. 1 písm. a) a b).

2. Příslušné orgány mohou poskytnout ENTSO pro elektřinu a subjektu EU DSO zmapování kontrol uvedených v čl. 28 odst. 1 písm. a) a b) s odkazem na související vnitrostátní právní nebo regulační rámce, včetně příslušných vnitrostátních norem členských států podle článku 25 směrnice (EU) 2022/2555. Pokud příslušný orgán členského státu takové zmapování poskytne, ENTSO pro elektřinu a subjekt EU DSO toto vnitrostátní zmapování zahrnou do mapovací matice.

3. Do šesti měsíců od vypracování každé zprávy o posouzení kybernetických bezpečnostních rizik na úrovni regionu podle čl. 21 odst. 2 navrhnou provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO a po konzultaci s ENISA příslušnému orgánu změnu mapovací matice. Návrh bude proveden v souladu s čl. 8 odst. 10 a zohlední rizika zjištěná při posouzení rizik na úrovni regionu.

KAPITOLA IV

DOPORUČENÍ PRO ZADÁVÁNÍ ZAKÁZEK V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Článek 35

Doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti

1. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO vypracují v rámci pracovního programu, který bude stanoven a aktualizován pokaždé, když bude přijata zpráva o posouzení kybernetických bezpečnostních rizik na úrovni regionu, soubory nezávazných doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti, které mohou subjekty s vysokým dopadem a subjekty s kritickým dopadem použít jako základ pro zadávání zakázek na produkty IKT, služby IKT a procesy IKT v perimetru vysokého dopadu a v perimetru kritického dopadu. Tento pracovní program zahrnuje:

a) popis a klasifikaci druhů produktů IKT, služeb IKT a procesů IKT používaných subjekty s vysokým dopadem a subjekty s kritickým dopadem v perimetru vysokého dopadu a v perimetru kritického dopadu;

b) seznam druhů produktů IKT, služeb IKT a procesů IKT, pro které bude vypracován soubor nezávazných doporučení v oblasti kybernetické bezpečnosti na základě příslušných zpráv o posouzení kybernetických bezpečnostních rizik na úrovni regionů a na základě priorit subjektů s vysokým dopadem a subjektů s kritickým dopadem;

2. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO do šesti měsíců od přijetí nebo aktualizace zprávy o posouzení kybernetických bezpečnostních rizik poskytne ACER shrnutí tohoto pracovního programu.

3. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO usilují o to, aby nezávazná doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti vypracovaná na základě příslušného posouzení kybernetických bezpečnostních rizik na úrovni regionu byla podobná nebo srovnatelná ve všech regionech pro provoz soustavy. Soubory doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti zahrnují alespoň specifikace uvedené v čl. 33 odst. 2 písm. a). Specifikace se pokud možno vybírají z evropských a mezinárodních norem.

4. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO zajistí, aby soubory doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti:

a) byly v souladu se zásadami zadávání veřejných zakázek podle směrnice 2014/24/EU a

b) byly slučitelné s nejnovějšími dostupnými evropskými systémy certifikace kybernetické bezpečnosti, které se vztahují k produktu IKT, službě IKT nebo procesu IKT, a zohledňovaly tyto systémy.

Článek 36

Pokyny k používání evropských systémů certifikace kybernetické bezpečnosti při zadávání zakázek na produkty IKT, služby IKT a procesy IKT

1. Nezávazná doporučení pro zadávání zakázek v oblasti kybernetické bezpečnosti vypracovaná podle článku 35 mohou zahrnovat odvětvové pokyny týkající se používání evropských systémů certifikace kybernetické bezpečnosti, kdykoli je k dispozici vhodný systém pro určitý druh produktu IKT, služby IKT nebo procesu IKT používaný subjekty s kritickým dopadem, aniž je dotčen rámec pro zřizování evropských systémů certifikace kybernetické bezpečnosti podle článku 46 nařízení (EU) 2019/881.

2. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO úzce spolupracují s ENISA při poskytování odvětvových pokynů obsažených v nezávazných doporučeních pro zadávání zakázek v oblasti kybernetické bezpečnosti podle odstavce 1.

KAPITOLA V

INFORMAČNÍ TOKY, KYBERNETICKÉ ÚTOKY A ŘÍZENÍ KRIZÍ

Článek 37

Pravidla pro sdílení informací

1. Pokud příslušný orgán obdrží informace týkající se kybernetického útoku podléhajícího hlášení, tento příslušný orgán:

a) posoudí úroveň důvěrnosti těchto informací a o výsledku svého posouzení informuje subjekt bez zbytečného odkladu, nejpozději však do 24 hodin od obdržení informací;

b) se pokusí zjistit jakýkoli jiný podobný kybernetický útok v Unii, který byl nahlášen jiným příslušným orgánům, s cílem porovnat informace získané v souvislosti s kybernetickým útokem, který je předmětem hlášení, s informacemi poskytnutými v souvislosti s jinými kybernetickými útoky a obohatit stávající informace, posílit a koordinovat reakce v oblasti kybernetické bezpečnosti;

c) odpovídá za odstranění obchodních tajemství a anonymizaci informací v souladu s příslušnými vnitrostátními předpisy a předpisy Unie;

d) bez zbytečného odkladu, nejpozději však do 24 hodin od přijetí informace o kybernetickém útoku podléhajícím hlášení, sdílí tyto informace s národními jednotnými kontaktními místy, týmy CSIRT a všemi příslušnými orgány určenými podle článku 4 v jiných členských státech a pravidelně těmto orgánům nebo subjektům poskytuje aktualizované informace;

e) po anonymizaci a odstranění obchodních tajemství podle odst. 1 písm. c) a bez zbytečného odkladu, nejpozději však do 24 hodin od obdržení informací podle odst. 1 písm. a), předá informace o kybernetickém útoku subjektům s kritickým dopadem a subjektům s vysokým dopadem ve svém členském státě a pravidelně jim poskytuje aktualizované informace, které těmto subjektům umožní účinně organizovat obranu;

f) může požádat ohlašující subjekt s vysokým dopadem nebo subjekt s kritickým dopadem, aby informace o kybernetickém útoku podléhajícím hlášení dále bezpečným způsobem šířil mezi další subjekty, které mohou být zasaženy, s cílem vytvořit v rámci odvětví elektroenergetiky povědomí o situaci a zabránit naplnění rizika, které může eskalovat v přeshraniční kybernetický bezpečnostní incident v elektroenergetice;

g) po anonymizaci a odstranění obchodních tajemství předloží ENISA souhrnnou zprávu s informacemi o kybernetickém útoku.

2. Pokud se tým CSIRT dozví o neopravené aktivně zneužívané zranitelnosti, musí:

a) toto neprodleně sdělit ENISA prostřednictvím vhodného zabezpečeného kanálu pro výměnu informací, není-li v jiných právních předpisech Unie stanoveno jinak;

b) podpořit dotčený subjekt, aby od výrobce nebo poskytovatele obdržel účinnou, koordinovanou a rychlou správu neopravené aktivně zneužívané zranitelnosti nebo účinná a efektivní opatření k jejímu zmírnění;

c) sdílet dostupné informace s dodavatelem a požádat výrobce nebo poskytovatele, aby pokud možno určil seznam týmů CSIRT v členských státech, kterých se neopravená aktivně zneužívaná zranitelnost týká, a které je nutné informovat;

d) sdílet dostupné informace s týmy CSIRT uvedenými v předchozím písmeni na základě zásady „vědět jen to nejnutnější“;

e) sdílet strategie a opatření ke zmírnění nahlášené neopravené aktivně zneužívané zranitelnosti, pokud takové strategie a opatření existují.

3. Pokud se příslušný orgán dozví o neopravené aktivně zneužívané zranitelnosti, musí:

a) v koordinaci s týmy SCIRT sdílet strategie a opatření ke zmírnění nahlášené neopravené a aktivně zneužívané zranitelnosti, pokud takové strategie a opatření existují v jeho členském státě;

b) sdílet informace s týmem CSIRT v členském státě, kde byla neopravená aktivně zneužívaná zranitelnost nahlášena.

4. Pokud se příslušný orgán dozví o neopravené zranitelnosti, aniž by bylo prokázáno, že je dosud aktivně zneužívána, bez zbytečného odkladu koordinuje svou činnost s týmem CSIRT za účelem koordinovaného zveřejnění zranitelnosti, jak je stanoveno v čl. 12 odst. 1 směrnice (EU) 2022/2555.

5. Pokud tým CSIRT obdrží od jednoho nebo více subjektů s vysokým dopadem nebo subjektů s kritickým dopadem informace týkající se kybernetických hrozeb podle čl. 38 odst. 6, bez zbytečného odkladu, nejpozději však do čtyř hodin od obdržení informací předá tyto informace nebo jakékoli jiné informace důležité pro prevenci a odhalení souvisejícího rizika, reakci na ně a jeho zmírnění subjektům s kritickým dopadem a subjektům s vysokým dopadem ve svém členském státě a v příslušných případech všem dotčeným týmům CSIRT a svému národnímu jednotnému kontaktnímu místu.

6. Pokud se příslušný orgán dozví od jednoho nebo více subjektů s vysokým dopadem nebo subjektů s kritickým dopadem informace týkající se kybernetických hrozeb, předá tyto informace týmu CSIRT pro účely uvedené v odstavci 5.

7. Příslušné orgány mohou po dohodě mezi dotčenými příslušnými orgány přenést zcela nebo částečně povinnosti podle odstavců 3 a 4 týkající se jednoho nebo více subjektů s vysokým dopadem nebo subjektů s kritickým dopadem, které působí ve více členských státech, na jiný příslušný orgán v jednom z těchto členských států.

8. Provozovatelé přenosových soustav s pomocí ENTSO pro elektřinu a ve spolupráci se subjektem EU DSO vypracují do 13. června 2025 metodiku stupnice pro klasifikaci kybernetických útoků. Provozovatelé přenosových soustav mohou s pomocí ENTSO pro elektřinu a subjektu EU DSO požádat příslušné orgány, aby konzultovaly ENISA a své příslušné orgány odpovědné za kybernetickou bezpečnost o pomoc při vypracování takové klasifikační stupnice. Metodika musí stanovit klasifikaci závažnosti kybernetického útoku podle pěti úrovní, přičemž dvě nejvyšší úrovně jsou „vysoká" a „kritická". Klasifikace je založena na posouzení těchto parametrů:

a) potenciální dopad s ohledem na aktiva a perimetry vystavené útoku, určené v souladu s čl. 26 odst. 4 písm. c); a

b) závažnost kybernetického útoku.

9. Do 13. června 2026 provede ENTSO pro elektřinu ve spolupráci se subjektem EU DSO studii proveditelnosti s cílem posoudit možnosti a finanční náklady nezbytné pro vytvoření společného nástroje, který umožní všem subjektům sdílet informace s příslušnými vnitrostátními orgány.

10. Studie proveditelnosti posoudí možnosti, aby takový nástroj:

a) podporoval subjekty s kritickým dopadem a subjekty s vysokým dopadem relevantními informacemi týkajícími se bezpečnosti provozu přeshraničních toků elektřiny, jako je hlášení kybernetických útoků v téměř reálném čase, včasná upozornění týkající se kybernetické bezpečnosti a nezjištěné zranitelnosti zařízení používaných v elektrizační soustavě;

b) byl uchováván ve vhodném a vysoce důvěryhodném prostředí;

c) umožňoval shromažďování údajů od subjektů s kritickým dopadem a subjektů s vysokým dopadem a usnadnil odstranění důvěrných informací a anonymizaci dat a jejich rychlé šíření mezi subjekty s kritickým dopadem a subjekty s vysokým dopadem.

11. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO:

a) při posuzování proveditelnosti konzultuje s ENISA a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, národní jednotnými kontaktními místy a zástupci hlavních zainteresovaných subjektů;

b) výsledky studie proveditelnosti předloží ACER a skupině pro spolupráci v oblasti bezpečnosti sítí a informací.

12. ENTSO pro elektřinu může ve spolupráci se subjektem EU DSO analyzovat a usnadňovat iniciativy navržené subjekty s kritickým dopadem a subjekty s vysokým dopadem za účelem vyhodnocení a testování těchto nástrojů pro sdílení informací.

Článek 38

Úloha subjektů s vysokým dopadem a subjektů s kritickým dopadem, pokud jde o sdílení informací

1. Každý subjekt s vysokým dopadem a subjekt s kritickým dopadem:

a) pro všechna aktiva v rámci svého perimetru kybernetické bezpečnosti určeného podle čl. 26 odst. 4 písm. c) zajistí, aby operační středisko kybernetické bezpečnosti bylo minimálně schopno:

   i) zajistit, aby příslušné sítě a informační systémy a aplikace poskytovaly bezpečnostní protokoly pro bezpečnostní monitorování, které umožní odhalovat anomálie a shromažďovat informace o kybernetických útocích;

   ii) provádět bezpečnostní sledování, včetně odhalování narušení a posuzování zranitelnosti sítí a informačních systémů;

   iii) provádět analýzy a v případě potřeby přijmout veškerá opatření, která jsou v rámci jeho odpovědnosti a možností nezbytná k ochraně subjektu;

   iv) účastnit se shromažďování a sdílení informací popsaných v tomto článku;

b) má právo pořizovat všechny tyto schopnosti nebo jejich části podle písmene a) prostřednictvím poskytovatelů řízených bezpečnostních služeb. Subjekty s kritickým dopadem a subjekty s vysokým dopadem jsou nadále za poskytovatele řízených bezpečnostních služeb odpovědné a dohlížejí na jejich činnost;

c) určí jednotné kontaktní místo na úrovni subjektu pro účely sdílení informací.

2. ENISA může v rámci úkolu stanoveného v čl. 6 odst. 2 nařízení (EU) 2019/881 vydat nezávazné pokyny týkající se vytváření takových schopností nebo zadávání služeb poskytovatelům řízených bezpečnostních služeb.

3. Každý subjekt s kritickým dopadem a subjekt s vysokým dopadem sdílí příslušné informace týkající se kybernetického útoku podléhajícího hlášení se svými týmy CSIRT a příslušným orgánem bez zbytečného odkladu, nejpozději však do čtyř hodin od okamžiku, kdy se dozví, že incident podléhá hlášení.

4. Informace týkající se kybernetického útoku se považují za podléhající ohlášení, pokud dotčený subjekt vyhodnotí kybernetický útok jako kritický v rozmezí od „vysoké“ do „kritické“ podle metodiky stupnice pro klasifikaci kybernetických útoků podle čl. 37 odst. 8. Klasifikaci incidentu sdělí jednotné kontaktní místo na úrovni subjektu určené podle odst. 1 písm. c).

5. Pokud subjekty s kritickým dopadem a subjekty s vysokým dopadem oznámí týmu CSIRT příslušné informace týkající se neopravené aktivně zneužívané zranitelnosti, může tým CSIRT tyto informace předat svému příslušnému orgánu. S ohledem na úroveň citlivosti oznámených informací může tým CSIRT na základě oprávněných důvodů souvisejících s kybernetickou bezpečností informace dále neposkytnout nebo jejich předání odložit.

6. Každý subjekt s kritickým dopadem a subjekt s vysokým dopadem poskytne bez zbytečného odkladu svým týmům CSIRT veškeré informace týkající se kybernetických hrozeb podléhajících hlášení, které mohou mít přeshraniční dopad. Informace týkající se kybernetické hrozby se považují za podléhající hlášení, je-li splněna alespoň jedna z těchto podmínek:

a) poskytují relevantní informace pro jiné subjekty s kritickým dopadem a subjekty s vysokým dopadem důležité pro prevenci a odhalení rizika, reakci na ně nebo zmírnění jeho dopadu;

b) zjištěné techniky, taktika a postupy použité v rámci útoku vedou k informacím, jako jsou kompromitované adresy URL nebo IP, hashe nebo další atributy užitečné pro kontextualizaci a korelaci útoku;

c) kybernetická hrozba může být dále posouzena a dána do kontextu s dalšími informacemi poskytnutými poskytovateli služeb nebo třetími stranami, na které se toto nařízení nevztahuje.

7. Každý subjekt s kritickým dopadem a subjekt s vysokým dopadem při sdílení informací podle tohoto článku uvede tyto údaje:

a) že informace jsou předkládány v souladu s tímto nařízením;

b) zda se informace týkají:

   i) kybernetického útoku podléhajícího hlášení podle odstavce 3;

   ii) neopravené aktivně zneužívané zranitelnosti, která není veřejně známá, uvedené v odstavci 4;

   iii) kybernetické hrozby podléhající ohlášení uvedené v odstavci 5;

c) v případě kybernetického útoku podléhajícího hlášení, úroveň kybernetického útoku podle metodiky stupnice pro klasifikaci kybernetických útoků uvedené v čl. 37 odst. 8 a informace vedoucí k této klasifikaci, včetně alespoň stupně kritičnosti kybernetického útoku.

8. Pokud subjekt s kritickým dopadem nebo subjekt s vysokým dopadem oznámí významný incident podle článku 23 směrnice (EU) 2022/2555 a oznámení incidentu podle uvedeného článku obsahuje příslušné informace požadované podle odstavce 3 tohoto článku, oznámení subjektu podle čl. 23 odst. 1 uvedené směrnice představuje nahlášení informací podle odstavce 3 tohoto článku.

9. Každý subjekt s kritickým dopadem a subjekt s vysokým dopadem podává zprávy svému příslušnému orgánu nebo týmu CSIRT, přičemž jasně označí konkrétní informace, které mohou být sdíleny pouze s příslušným orgánem nebo týmem CSIRT v případech, kdy by sdílení informací mohlo být zdrojem kybernetického útoku. Každý subjekt s kritickým dopadem a subjekt s vysokým dopadem má právo poskytnout příslušnému týmu CSIRT verzi informací, která nemá důvěrný charakter.

Článek 39

Odhalování kybernetických útoků a nakládání se souvisejícími informacemi

1. Subjekty s kritickým dopadem a subjekty s vysokým dopadem s nezbytnou podporou příslušného orgánu, ENTSO pro elektřinu a subjektu EU DSO vyvinou potřebné schopnosti pro zvládání odhalených kybernetických útoků. Subjekty s kritickým dopadem a subjekty s vysokým dopadem může podporovat tým CSIRT určený v jejich příslušném členském státě, a to v rámci úkolu, který je týmu CSIRT svěřen podle čl. 11 odst. 5 písm. a) směrnice (EU)2022/2555. Subjekty s kritickým dopadem a subjekty s vysokým dopadem zavedou účinné postupy pro určování a klasifikaci kybernetických útoků, které ovlivní nebo mohou ovlivnit přeshraniční toky elektřiny, a pro reakci na tyto útoky, aby se minimalizoval jejich dopad.

2. Pokud má kybernetický útok vliv na přeshraniční toky elektřiny, jednotná kontaktní místa na úrovni subjektů v dotčených subjektech s kritickým dopadem a subjektech s vysokým dopadem spolupracují při vzájemném sdílení informací, které koordinuje příslušný orgán členského státu, v němž byl kybernetický útok nahlášen jako první.

3. Subjekty s kritickým dopadem a subjekty s vysokým dopadem:

a) zajistí, aby jejich vlastní jednotné kontaktní místo na úrovni subjektu mělo přístup k informacím, které obdrželo od vnitrostátního jednotného kontaktního místa prostřednictvím svého příslušného orgánu, na základě zásady „vědět jen to nejnutnější“;

b) pokud tak již neučinily podle čl. 3 odst. 4 směrnice (EU) 2022/2555, oznámí příslušnému orgánu členského státu, v němž jsou usazeny, a vnitrostátnímu jednotnému kontaktnímu místu seznam svých jednotných kontaktních míst na úrovni subjektu pro kybernetickou bezpečnost:

   i) od nichž může příslušný orgán a vnitrostátní jednotné kontaktní místo očekávat, že obdrží informace o kybernetických útocích podléhajících hlášení;

   ii) jimž mohou příslušné orgány a vnitrostátní jednotná kontaktní místa poskytovat informace;

c) stanoví postupy pro zvládání kybernetických útoků, včetně úloh a povinností, úkolů a reakcí na základě pozorovatelného vývoje kybernetického útoku v rámci perimetru kritického dopadu a perimetru vysokého dopadu;

d) nejméně jednou ročně testují celkové postupy zvládání kybernetických útoků prostřednictvím testování alespoň jednoho scénáře, který přímo nebo nepřímo ovlivňuje přeshraniční toky elektřiny. Tento každoroční test mohou subjekty s kritickým dopadem a subjekty s vysokým dopadem provádět během pravidelných cvičení uvedených v článku 43. Jako každoroční test v rámci plánu reakce na kybernetické útoky může posloužit jakákoli činnost v reakci na skutečný kybernetický útok s důsledkem klasifikovaným alespoň na stupni 2 podle metodiky stupnice pro klasifikaci kybernetických útoků uvedené v čl. 37 odst. 8 a s příčinami v oblasti kybernetické bezpečnosti.

4. Úkoly uvedené v odstavci 1 mohou členské státy rovněž přenést na regionální koordinační centra v souladu s čl. 37 odst. 2 nařízení (EU) 2019/943.

Článek 40

Krizové řízení

1. Pokud příslušný orgán zjistí, že elektroenergetická krize souvisí s kybernetickým útokem, který má dopad na více než jeden členský stát, příslušné orgány z dotčených členských států, příslušné orgány odpovědné za kybernetickou bezpečnost, příslušný orgán pro rizikovou připravenost a orgány pro řízení kybernetických krizí ovlivňujících bezpečnost sítí a informací z dotčených členských států společně vytvoří *ad hoc* skupinu pro přeshraniční krizovou koordinaci.

2. *Ad hoc* skupina pro přeshraniční krizovou koordinaci:

a) koordinuje účinné vyhledávání všech relevantních informací o kybernetické bezpečnosti a jejich další šíření mezi subjekty zapojené do procesu řízení krize;

b) organizuje komunikaci mezi všemi subjekty zasaženými krizí a příslušnými orgány s cílem omezit překrývání a zvýšit účinnost analýz a technických reakcí, které mají napravit souběžné elektroenergetické krize, jež mají příčiny v oblasti kybernetické bezpečnosti;

c) ve spolupráci s příslušnými týmy CSIRT poskytuje subjektům, které incident ovlivnil, potřebné odborné znalosti, včetně operativního poradenství týkajícího se provádění možných opatření ke zmírnění následků;

d) informuje Komisi a Koordinační skupinu pro otázky elektrické energie o stavu incidentu v souladu se zásadami ochrany stanovenými v článku 46 a své informace pravidelně aktualizuje;

e) vyžádá si poradenství od příslušných orgánů, agentur nebo subjektů, které by mohly být nápomocny při zmírnění krize v elektroenergetice.

3. Pokud je kybernetický útok označen nebo se očekává, že bude označen jako rozsáhlý kybernetický bezpečnostní incident, *ad hoc* skupina pro přeshraniční krizovou koordinaci o tom v souladu s čl. 9 odst. 1 směrnice (EU) 2022/2555 neprodleně informuje vnitrostátní orgány pro řízení kybernetických krizí v členských státech zasažených incidentem, jakož i Komisi a síť EU CyCLONe. V takové situaci *ad hoc* skupina pro přeshraniční krizovou koordinaci podporuje síť EU CyCLONe, pokud jde o odvětvová specifika.

4. Subjekty s kritickým dopadem a subjekty s vysokým dopadem vyvinou a mají k dispozici kapacity, interní směrnice, plány připravenosti a zaměstnance, kteří se budou podílet na odhalování přeshraničních krizí a zmírňování jejich následků. Subjekt s kritickým dopadem nebo subjekt s vysokým dopadem, který je postižen souběžnou elektroenergetickou krizí, prošetří ve spolupráci se svým příslušným orgánem příčinu takové krize a určí, do jaké míry krize souvisí s kybernetickým útokem.

5. Úkoly uvedené v odstavci 4 mohou členské státy rovněž přenést na regionální koordinační centra v souladu s čl. 37 odst. 2 nařízení (EU) 2019/943.

Článek 41

Plány řízení kybernetických bezpečnostních krizí a reakce na kybernetické bezpečnostní krize

1. Do 24 měsíců poté, co byla ACER oznámena zpráva o posouzení rizik pro celou Unii, ACER v úzké spolupráci s ENISA, ENTSO pro elektřinu, subjektem EU DSO, příslušnými orgány odpovědnými za kybernetickou bezpečnost, příslušnými orgány, příslušnými orgány pro rizikovou připravenost, národními regulačními orgány a orgány pro řízení kybernetických krizí ovlivňujících bezpečnost sítí a informací vypracuje plán řízení kybernetických bezpečnostních krizí v odvětví elektroenergetiky a reakce na tyto krize na úrovni Unie.

2. Do 12 měsíců poté, co ACER vypracuje plán řízení kybernetických bezpečnostních krizí v odvětví elektroenergetiky a reakce na tyto krize na úrovni Unie podle odstavce 1, vypracuje každý příslušný orgán národní plán řízení kybernetických bezpečnostních krizí ovlivňujících přeshraniční toky elektřiny a reakce na tyto krize, přičemž zohlední plán řízení kybernetických bezpečnostních krizí na úrovni Unie a národní plán rizikové připravenosti vypracovaný v souladu s článkem 10 nařízení (EU) 2019/941. Tento plán musí být v souladu s plánem reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize podle čl. 9 odst. 4 směrnice (EU) 2022/2555. Příslušný orgán koordinuje svou činnost se subjekty s kritickým dopadem a se subjekty s vysokým dopadem a s příslušným orgánem pro rizikovou připravenost ve svém členském státě.

3. Národní plán reakce na rozsáhlé kybernetické bezpečnostních incidenty a krize vyžadovaný podle čl. 9 odst. 4 směrnice (EU) 2022/2555 se považuje za národní plán řízení kybernetických bezpečnostních krizí podle tohoto článku, pokud obsahuje ustanovení o řízení krizí ovlivňujících přeshraniční toky elektřiny a reakci na tyto krize.

4. Úkoly uvedené v odstavcích 1 a 2 mohou členské státy rovněž přenést na regionální koordinační centra v souladu s čl. 37 odst. 2 nařízení (EU) 2019/943.

5. Subjekty s kritickým dopadem a subjekty s vysokým dopadem zajistí, aby jejich procesy řízení krizí souvisejících s kybernetickou bezpečností:

a) měly do svých plánů krizového řízení formálně začleněny postupy pro řešení kybernetických bezpečnostních incidentů s přeshraničním dopadem, které jsou slučitelné s postupy vymezenými v čl. 6 bodě 8 směrnice (EU) 2022/2555;

b) byly součástí obecných činností krizového řízení.

6. Do 12 měsíců od oznámení subjektů s vysokým dopadem a subjektů s kritickým dopadem podle čl. 24 odst. 6 a poté každé tři roky vypracují subjekty s kritickým dopadem a subjekty s vysokým dopadem plán krizového řízení na úrovni subjektu pro případ krize související s kybernetickou bezpečností, který bude zahrnut do jejich obecných plánů krizového řízení. Tento plán musí obsahovat alespoň tyto prvky:

a) pravidla pro vyhlášení krize stanovená v čl. 14 odst. 2 a 3 nařízení (EU) 2019/941;

b) jasné úlohy a povinnosti v rámci krizového řízení, včetně úlohy dalších příslušných subjektů s kritickým dopadem a subjektů s vysokým dopadem;

c) aktuální kontaktní informace a pravidla pro komunikaci a sdílení informací během krizové situace, včetně spojení s týmy CSIRT.

7. Opatření krizového řízení podle čl. 21 odst. 2 písm. c) směrnice (EU) 2022/2555 se považují za plán krizového řízení v odvětví elektroenergetiky na úrovni subjektu podle tohoto článku, pokud zahrnují všechny požadavky uvedené v odstavci 6.

8. Plány krizového řízení se testují během cvičení v oblasti kybernetické bezpečnosti uvedených v článcích 43, 44 a 45.

9. Subjekty s kritickým dopadem a subjekty s vysokým dopadem zahrnou své plány krizového řízení na úrovni subjektu do svých plánů kontinuity činností pro procesy s kritickým dopadem a procesy s vysokým dopadem. Plány krizového řízení na úrovni subjektu zahrnují:

a) procesy závisející na dostupnosti, integritě a spolehlivosti služeb IT;

b) všechna místa nezbytná pro zajištění kontinuity činností včetně umístění hardwaru a softwaru;

c) všechny interní úlohy a povinnosti spojené s procesy zajištění kontinuity činností.

10. Subjekty s kritickým dopadem a subjekty s vysokým dopadem aktualizují své plány krizového řízení na úrovni subjektu nejméně jednou za tři roky a kdykoli v případě potřeby.

11. ACER aktualizuje plán řízení kybernetických bezpečnostních krizí v odvětví elektroenergetiky a reakce na tyto krize na úrovni Unie vypracovaný podle odstavce 1 nejméně jednou za tři roky a kdykoli v případě potřeby.

12. Každý příslušný orgán aktualizuje národní plán řízení kybernetických bezpečnostních krizí ovlivňujících přeshraniční toky elektřiny a reakce na tyto krize vypracovaný podle odstavce 2 nejméně jednou za tři roky a kdykoli v případě potřeby.

13. Subjekty s kritickým dopadem a subjekty s vysokým dopadem testují své plány kontinuity činností nejméně jednou za tři roky nebo po významných změnách procesu s kritickým dopadem. Výsledek testů plánu kontinuity činnosti musí být zdokumentován. Subjekty s kritickým dopadem a subjekty s vysokým dopadem mohou test plánu kontinuity činností zahrnout do svých cvičení v oblasti kybernetické bezpečnosti.

14. Subjekty s kritickým dopadem a subjekty s vysokým dopadem aktualizují svůj plán kontinuity činností s ohledem na výsledek testu kdykoli v případě potřeby, nejméně však jednou za tři roky.

15. Zjistí-li test nedostatky v plánu kontinuity činností, subjekt s kritickým dopadem a subjekt s vysokým dopadem do 180 kalendářních dnů od testování tyto nedostatky napraví a provede nový test, aby prokázal, že nápravná opatření jsou účinná.

16. Pokud subjekt s kritickým nebo subjekt s vysokým dopadem nemůže nedostatky napravit do 180 kalendářních dnů, uvede důvody ve zprávě, kterou předloží svému příslušnému orgánu v souladu s článkem 27.

Článek 42

Schopnosti včasného varování v oblasti kybernetické bezpečnosti v odvětví elektroenergetiky

1. Příslušné orgány spolupracují s ENISA na rozvoji schopností včasného varování v oblasti kybernetické bezpečnosti elektřiny (ECEAC) v rámci pomoci členským státům podle čl. 6 odst. 2 a 7 nařízení (EU) 2019/881.

2. Schopnosti včasného varování v oblasti kybernetické bezpečnosti v elektroenergetice umožní ENISA při plnění úkolů uvedených v čl. 7 odst. 7 nařízení (EU) 2019/881:

a) shromažďovat dobrovolně sdílené informace od:

   i) týmů CSIRT a příslušných orgánů;

   ii) subjektů uvedených v článku 2 tohoto nařízení;

   iii) jakéhokoli dalšího subjektu, který chce dobrovolně sdílet příslušné informace;

b) posuzovat a třídit shromážděné informace;

c) posuzovat informace, ke kterým má ENISA přístup, pro účely určení podmínek kybernetického rizika a příslušných ukazatelů pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny;

d) určit podmínky a ukazatele, které často korelují s kybernetickými útoky v odvětví elektroenergetiky;

e) stanovit, zda je třeba provést další analýzu a preventivní opatření prostřednictvím posouzení a určení rizikových faktorů;

f) informovat příslušné orgány o zjištěných rizicích a doporučených preventivních opatřeních specifických pro dotčené subjekty;

g) informovat všechny příslušné subjekty uvedené v článku 2 o výsledcích posouzení informací podle písmen b), c) a d) tohoto odstavce;

h) pravidelně zahrnovat příslušné informace do zprávy o situačním povědomí vydávané v souladu s čl. 7 odst. 6 nařízení (EU) 2019/881;

i) pokud je to možné, odvodit ze shromážděných informací použitelné údaje, které indikují potenciální narušení bezpečnosti nebo kybernetický útok („indikátory narušení“).

3. Týmy CSIRT neprodleně předají informace obdržené od ENISA dotčeným subjektům v rámci svých úkolů vymezených v čl. 11 odst. 3 písm. b) směrnice (EU) 2022/2555.

4. ACER sleduje účinnost schopností včasného varování v oblasti kybernetické bezpečnosti v elektroenergetice. ENISA je ACER nápomocna tím, že jí poskytuje veškeré potřebné informace podle čl. 6 odst. 2 a čl. 7 odst. 1 nařízení (EU) 2019/881. Analýza této sledovací činnosti je součástí sledování podle článku 12 tohoto nařízení.

KAPITOLA VI

RÁMEC PRO CVIČENÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI ELEKTŘINY

Článek 43

Cvičení v oblasti kybernetické bezpečnosti na úrovni subjektů a členských států

1. Do 31. prosince roku následujícího po oznámení subjektů s kritickým dopadem a poté každé tři roky provede každý subjekt s kritickým dopadem cvičení v oblasti kybernetické bezpečnosti zahrnující jeden nebo více scénářů s kybernetickými útoky, které přímo nebo nepřímo ovlivňují přeshraniční toky elektřiny a souvisejí s riziky zjištěnými během posouzení kybernetických bezpečnostních rizik na úrovni členských států a na úrovni subjektů v souladu s článkem 20 a článkem 27.

2. Odchylně od odstavce 1 může příslušný orgán pro rizikovou připravenost po konzultaci s příslušným orgánem a příslušným orgánem pro řízení kybernetických krizí určeným nebo zřízeným podle článku 9 směrnice (EU) 2022/2555 rozhodnout o uspořádání cvičení v oblasti kybernetické bezpečnosti na úrovni členského státu, jak je popsáno v odstavci 1, namísto provedení cvičení v oblasti kybernetické bezpečnosti na úrovni subjektu. Příslušný orgán v tomto ohledu informuje:

a) všechny subjekty s kritickým dopadem svého členského státu, národní regulační orgán, týmy CSIRT a příslušný orgán odpovídající za kybernetickou bezpečnost, a to nejpozději do 30. června roku, který předchází cvičení v oblasti kybernetické bezpečnosti na úrovni subjektu;

b) každý subjekt, který se zúčastní cvičení v oblasti kybernetické bezpečnosti na úrovni členského státu, a to nejpozději 6 měsíců před jeho konáním.

3. Příslušný orgán pro rizikovou připravenost s technickou podporou svých týmů CSIRT zorganizuje cvičení v oblasti kybernetické bezpečnosti na úrovni členského státu popsané v odstavci 2, a to samostatně nebo v rámci jiného cvičení v oblasti kybernetické bezpečnosti v daném členském státě. Aby bylo možné tato cvičení sdružit, může příslušný orgán pro rizikovou připravenost cvičení v oblasti kybernetické bezpečnosti na úrovni členského státu uvedené v odstavci 1 odložit o jeden rok.

4. Cvičení v oblasti kybernetické bezpečnosti na úrovni subjektů a na úrovni členských států musí být v souladu s vnitrostátními rámci pro řízení kybernetických bezpečnostních krizí podle čl. 9 odst. 4 písm. d) směrnice (EU) 2022/2555.

5. Do 31. prosince 2026 a poté každé tři roky zpřístupní ENTSO pro elektřinu ve spolupráci se subjektem EU DSO šablonu scénáře cvičení pro provádění cvičení v oblasti kybernetické bezpečnosti na úrovni subjektů a na úrovni členských států uvedených v odstavci 1. Tato šablona zohledňuje výsledky posledně provedeného posouzení kybernetických bezpečnostních rizik na úrovni subjektu a na úrovni členského státu a obsahuje klíčová kritéria úspěšnosti. ENTSO pro elektřinu a subjekt EU DSO zapojí do vývoje této šablony ACER a ENISA.

Článek 44

Regionální nebo meziregionální cvičení v oblasti kybernetické bezpečnosti

1. Do 31. prosince 2029 a poté každé tři roky uspořádá ENTSO pro elektřinu ve spolupráci se subjektem EU DSO v každém regionu pro provoz soustavy regionální cvičení v oblasti kybernetické bezpečnosti. Regionálního cvičení v oblasti kybernetické bezpečnosti se účastní subjekty s kritickým dopadem v daném regionu pro provoz soustavy. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO může uspořádat namísto regionálního cvičení v oblasti kybernetické bezpečnosti meziregionální cvičení v oblasti kybernetické bezpečnosti ve více než jednom regionu pro provoz soustavy ve stejném časovém rámci. Cvičení by mělo zohlednit i další existující posouzení kybernetických bezpečnostních rizik a scénáře vypracované na úrovni Unie.

2. ENTSO pro elektřinu a subjekt EU DSO při přípravě a organizaci cvičení v oblasti kybernetické bezpečnosti na regionální nebo meziregionální úrovni podporuje ENISA.

3. ENTSO pro elektřinu v koordinaci se subjektem EU DSO informuje subjekty s kritickým dopadem, které se zúčastní regionálního nebo meziregionálního cvičení v oblasti kybernetické bezpečnosti, šest měsíců před jeho konáním.

4. Pořadatel pravidelného cvičení kybernetické bezpečnosti na úrovni Unie podle čl. 7 odst. 5 nařízení (EU) 2019/881 nebo jakéhokoli povinného cvičení v oblasti kybernetické bezpečnosti týkajícího se odvětví elektřiny ve stejném zeměpisném perimetru může k účasti přizvat ENTSO pro elektřinu a subjekt EU DSO. V takových případech se povinnost uvedená v odstavci 1 neuplatní, pokud se téhož cvičení účastní všechny subjekty s kritickým dopadem v daném regionu pro provoz soustavy.

5. Účastní-li se ENTSO pro elektřinu a subjekt EU DSO cvičení v oblasti kybernetické bezpečnosti podle odstavce 4, mohou regionální nebo meziregionální cvičení v oblasti kybernetické bezpečnosti uvedené v odstavci 1 odložit o jeden rok.

6. Do 31. prosince 2027 a každé tři roky po tomto datu zpřístupní ENTSO pro elektřinu v koordinaci se subjektem EU DSO šablonu cvičení pro provádění regionálních a meziregionálních cvičení v oblasti kybernetické bezpečnosti. Tato šablona zohledňuje výsledky posledně provedeného posouzení kybernetických bezpečnostních rizik na regionální úrovni a obsahuje klíčová kritéria úspěšnosti. ENTSO pro elektřinu konzultuje organizaci a provádění regionálních a meziregionálních cvičení v oblasti kybernetické bezpečnosti s Komisí a může si k nim vyžádat poradenství od ACER, ENISA a Společného výzkumného střediska.

Článek 45

Výsledky cvičení v oblasti kybernetické bezpečnosti na úrovni subjektů, členských států, regionů nebo na meziregionální úrovni

1. Poskytovatelé kritických služeb se na žádost subjektu s kritickým dopadem účastní cvičení v oblasti kybernetické bezpečnosti uvedených v čl. 43 odst. 1 a 2 a v čl. 44 odst. 1, pokud poskytují subjektu s kritickým dopadem služby v oblasti odpovídající rozsahu příslušného cvičení v oblasti kybernetické bezpečnosti.

2. Pořadatelé cvičení v oblasti kybernetické bezpečnosti uvedených v čl. 43 odst. 1 a 2 a v čl. 44 odst. 1 provedou s poradenstvím ENISA, pokud o ně požádají, a podle čl. 7 odst. 5 nařízení (EU) 2019/881 analýzu příslušného cvičení v oblasti kybernetické bezpečnosti a uzavřou ho prostřednictvím zprávy shrnující získané poznatky, která je určena všem účastníkům. Zpráva musí obsahovat:

a) scénáře cvičení, zprávy ze schůzek, hlavní stanoviska, úspěchy a získané zkušenosti na všech úrovních hodnotového řetězce elektřiny;

b) informaci, zda byla splněna klíčová kritéria úspěšnosti;

c) seznam doporučení pro subjekty účastnící se příslušného cvičení v oblasti kybernetické bezpečnosti, jejichž účelem je opravit, upravit nebo změnit procesy a postupy řešení kybernetických bezpečnostních krizí, související modely řízení a veškeré stávající smluvní závazky s poskytovateli kritických služeb.

3. Na žádost sítě CSIRT nebo skupiny pro spolupráci v oblasti bezpečnosti sítí a informací nebo sítě EU CyCLONe pořadatelé cvičení v oblasti kybernetické bezpečnosti uvedených v čl. 43 odst. 1 a 2 a v čl. 44 odst. 1 sdílejí výsledky příslušného cvičení v oblasti kybernetické bezpečnosti. Pořadatelé sdílejí s každým subjektem účastnícím se cvičení informace uvedené v odst. 2 písm. a) a b) tohoto článku. Seznam doporučení uvedených v uvedeném odstavci písmenu c) sdílejí pořadatelé výhradně se subjekty, jichž se doporučení týkají.

4. Pořadatelé cvičení v oblasti kybernetické bezpečnosti uvedených v čl. 43 odst. 1 a 2 a v čl. 44 odst. 1 spolu se subjekty, které se cvičení účastní, pravidelně sledují provádění doporučení podle odst. 2 písm. c) tohoto článku.

KAPITOLA VII

OCHRANA INFORMACÍ

Článek 46

Zásady ochrany vyměňovaných informací

1. Subjekty uvedené v čl. 2 odst. 1 zajistí, aby informace poskytované, přijímané, vyměňované nebo předávané podle tohoto nařízení byly přístupné pouze na základě zásady „vědět jen to nejnutnější“ a v souladu s příslušnými předpisy Unie a vnitrostátními předpisy o bezpečnosti informací.

2. Subjekty uvedené v čl. 2 odst. 1 zajistí, aby s informacemi poskytnutými, přijatými, vyměněnými nebo předanými podle tohoto nařízení bylo nakládáno a aby byly sledovány po celou dobu životního cyklu těchto informací a aby mohly být na konci svého životního cyklu zveřejněny pouze po anonymizaci.

3. Subjekty uvedené v čl. 2 odst. 1 zajistí, aby byla zavedena veškerá nezbytná ochranná opatření organizační a technické povahy k zajištění a ochraně důvěrnosti, integrity, dostupnosti a nepopiratelnosti informací poskytovaných, přijímaných, vyměňovaných nebo předávaných podle tohoto nařízení, a to nezávisle na použitých prostředcích. Ochranná opatření musí:

a) být přiměřená;

b) zohlednit kybernetická bezpečnostní rizika související se známými minulými a vznikajícími hrozbami, kterým mohou být tyto informace v souvislosti s tímto nařízením vystaveny;

c) pokud možno vycházet z vnitrostátních, evropských nebo mezinárodních norem a osvědčených postupů;

d) být zdokumentovány.

4. Subjekty uvedené v čl. 2 odst. 1 zajistí, aby každá fyzická osoba, které je umožněn přístup k informacím poskytovaným, přijímaným, vyměňovaným nebo předávaným podle tohoto nařízení, byla poučena o bezpečnostních pravidlech platných na úrovni subjektu a o opatřeních a postupech týkajících se ochrany informací. Tyto subjekty zajistí, aby dotčená fyzická osoba vzala na vědomí odpovědnost za ochranu informací podle pokynů obdržených během instruktáže.

5. Subjekty uvedené v čl. 2 odst. 1 zajistí, aby přístup k informacím poskytovaným, přijímaným, vyměňovaným nebo předávaným podle tohoto nařízení měly pouze fyzické osoby:

a) které jsou oprávněny k přístupu k těmto informacím na základě svých funkcí, jenž je omezen na plnění svěřených úkolů;

b) u nichž byl subjekt schopen posoudit etické zásady a zásady bezúhonnosti a u nichž neexistují žádné důkazy o negativním výsledku prověrky za účelem ověřování spolehlivosti osoby v souladu s osvědčenými postupy a standardními bezpečnostními požadavky subjektu a případně s vnitrostátními právními a správními předpisy.

6. Subjekty uvedené v čl. 2 odst. 1 musí mít písemný souhlas fyzické nebo právnické osoby, která původně informace vytvořila nebo poskytla, před tím, než tyto informace poskytnou třetí straně, která nespadá do oblasti působnosti tohoto nařízení.

7. Subjekt uvedený v čl. 2 odst. 1 může zvážit sdílení těchto informací bez dodržení odstavců 1 a 4 tohoto článku, aby se zabránilo souběžné elektroenergetické krizi s příčinami v oblasti kybernetické bezpečnosti nebo jakékoli přeshraniční krizi v rámci Unie v jiném odvětví. V takovém případě subjekt musí:

a) konzultovat s příslušným orgánem a být jím oprávněn ke sdílení těchto informací;

b) anonymizovat tyto informace, aniž by se ztratily prvky nezbytné pro informování veřejnosti o bezprostředním a vážném riziku pro přeshraniční toky elektřiny a o možných opatřeních k jeho zmírnění;

c) chránit totožnost původce a subjektů, které tyto informace zpracovávají podle tohoto nařízení.

8. Odchylně od odstavce 6 tohoto článku mohou příslušné orgány informace poskytnuté, obdržené, vyměněné nebo předané podle tohoto nařízení poskytnout třetí straně, která není uvedena v čl. 2 odst. 1, bez předchozího písemného souhlasu původce informací, musí jej však o tom co nejdříve informovat. Před zpřístupněním jakýchkoli informací poskytnutých, obdržených, vyměněných nebo předaných podle tohoto nařízení třetí straně, která není uvedena v čl. 2 odst. 1, dotčený příslušný orgán přiměřeně zajistí, aby si dotčená třetí strana byla vědoma platných bezpečnostních pravidel, a získá přiměřenou jistotu, že dotčená třetí strana může chránit obdržené informace v souladu s odstavci 1 až 5 tohoto článku. Příslušný orgán tyto informace anonymizuje, aniž by se ztratily prvky nezbytné k informování veřejnosti o bezprostředním a vážném riziku pro přeshraniční toky elektřiny a o možných opatřeních ke zmírnění rizika a k ochraně totožnosti původce informací. V takovém případě třetí strana, která není uvedena v čl. 2 odst. 1, chrání obdržené informace v souladu s předpisy již platnými na úrovni subjektu, nebo pokud to není možné, v souladu s předpisy a pokyny vydanými příslušným orgánem.

9. Tento článek se nevztahuje na subjekty, které nejsou uvedeny v čl. 2 odst. 1 a kterým jsou poskytovány informace podle odstavce 6 tohoto článku. V takovém případě se použije odstavec 7 tohoto článku nebo může příslušný orgán poskytnout tomuto subjektu písemná ustanovení, která se použijí v případech, kdy jsou informace obdrženy podle tohoto nařízení.

Článek 47

Důvěrnost informací

1. Na veškeré informace poskytnuté, přijaté, vyměněné nebo předané podle tohoto nařízení se vztahují podmínky profesního tajemství stanovené v odstavcích 2 až 5 tohoto článku tohoto nařízení a požadavky stanovené v článku 65 nařízení (EU) 2019/943. Veškeré informace poskytované, přijímané, vyměňované nebo předávané mezi subjekty uvedenými v článku 2 tohoto nařízení pro účely provádění tohoto nařízení jsou chráněny s ohledem na úroveň důvěrnosti informací, kterou uplatňuje původce informací.

2. Povinnost zachovávat profesní tajemství se vztahuje na subjekty uvedené v článku 2.

3. Příslušné orgány odpovědné za kybernetickou bezpečnost, národní regulační orgány, příslušné orgány odpovědné za rizikovou připravenost a týmy CSIRT si vyměňují veškeré informace nezbytné k plnění svých úkolů.

4. Veškeré informace přijaté, vyměňované nebo předávané mezi subjekty uvedenými v čl. 2 odst. 1 pro účely provádění článku 23 musí být anonymizovány a agregovány.

5. Informace, které obdrží jakýkoli subjekt nebo orgán, na který se vztahuje toto nařízení, při plnění svých povinností nesmějí být sděleny žádnému jinému subjektu nebo orgánu, aniž jsou dotčeny případy, na které se vztahuje vnitrostátní právo, jiná ustanovení tohoto nařízení nebo jiné příslušné právní předpisy Unie.

6. Aniž jsou dotčeny vnitrostátní právní předpisy nebo právní předpisy Unie, nesmí orgán, subjekt nebo fyzická osoba, která obdrží informace podle tohoto nařízení, tyto informace použít k jinému účelu než k plnění svých povinností podle tohoto nařízení.

7. ACER po konzultaci s ENISA, všemi příslušnými orgány, ENTSO pro elektřinu a subjektem EU-DSO vydá do 13. června 2025 pokyny týkající se mechanismů pro výměnu informací mezi všemi subjekty uvedenými v čl. 2 odst. 1, a zejména předpokládaných komunikačních toků a metod anonymizace a agregace informací pro účely provádění tohoto článku.

8. Informace, které jsou podle pravidel Unie a vnitrostátních pravidel důvěrné, se vyměňují s Komisí a dalšími příslušnými orgány pouze tehdy, je-li tato výměna nezbytná pro uplatňování tohoto nařízení. Vyměňované informace se omezí na ty, které jsou nezbytné a přiměřené účelu této výměny. Při výměně informací se zachovává důvěrnost těchto informací a chrání se bezpečnostní a obchodní zájmy subjektů s kritickým dopadem nebo subjektů s vysokým dopadem.

KAPITOLA VIII

ZÁVĚREČNÁ USTANOVENÍ

Článek 48

Dočasná ustanovení

1. Do schválení podmínek nebo metodik uvedených v čl. 6 odst. 2 nebo plánů uvedených v čl. 6 odst. 3 vypracuje ENTSO pro elektřinu ve spolupráci se subjektem EU DSO nezávazné pokyny k následujícím otázkám:

a) předběžný index dopadu na kybernetickou bezpečnost elektřiny („ECII“) podle odstavce 2 tohoto článku;

b) předběžný seznam procesů s vysokým dopadem na celou Unii a procesů s kritickým dopadem na celou Unii podle odstavce 4 tohoto článku a

c) předběžný seznam evropských a mezinárodních norem a kontrol vyžadovaných vnitrostátními právními předpisy, které mají význam pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny podle odstavce 6 tohoto článku.

2. Do 13. října 2024 vypracuje ENTSO pro elektřinu ve spolupráci se subjektem EU DSO doporučení pro předběžný index ECII. ENTSO pro elektřinu ve spolupráci se subjektem EU DSO oznámí doporučený předběžný index ECII příslušným orgánům.

3. Čtyři měsíce po obdržení doporučeného předběžného indexu dopadu na energetickou bezpečnost elektřiny, nejpozději však do 13. února 2025 určí příslušné orgány na základě doporučeného indexu dopadu na kybernetickou bezpečnost elektřiny kandidáty na subjekty s vysokým dopadem a subjekty s kritickým dopadem ve svém členském státě a vypracují předběžný seznam subjektů s vysokým dopadem a subjektů s kritickým dopadem. Subjekty s vysokým dopadem a subjekty s kritickým dopadem uvedené na předběžném seznamu mohou dobrovolně plnit své povinnosti stanovené v tomto nařízení na základě zásady předběžné opatrnosti. Do 13. března 2025 oznámí příslušné orgány subjektům uvedeným na předběžném seznamu, že byly určeny jako subjekty s vysokým dopadem nebo subjekty s kritickým dopadem.

4. Do 13. prosince 2024 ENTSO pro elektřinu ve spolupráci se subjektem EU DSO vypracuje předběžný seznam procesů s vysokým dopadem na celou Unii a procesů s kritickým dopadem na celou Unii. Subjekty, jimž bylo zasláno oznámení podle odstavce 3 a které se dobrovolně rozhodnou plnit své povinnosti stanovené v tomto nařízení na základě zásady předběžné opatrnosti, použijí předběžný seznam procesů s vysokým dopadem a procesů s kritickým dopadem k určení předběžných perimetrů vysokého dopadu a perimetrů kritického dopadu a k určení, jaká aktiva mají být zahrnuta do prvního posouzení kybernetických bezpečnostních rizik na úrovni subjektu.

5. Do 13. září 2024 každý příslušný orgán podle čl. 4 odst. 1 poskytne ENTSO pro elektřinu a subjektu EU DSO seznam svých vnitrostátních právních předpisů, které mají význam pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny.

6. Do 13. června 2025 připraví ENTSO pro elektřinu ve spolupráci se subjektem EU DSO předběžný seznam evropských a mezinárodních norem a kontrol vyžadovaných vnitrostátními právními předpisy, které mají význam pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny, přičemž zohlední informace poskytnuté příslušnými orgány.

7. Předběžný seznam evropských a mezinárodních norem a kontrol zahrnuje:

a) evropské a mezinárodní normy a vnitrostátní právní předpisy, které obsahují pokyny týkající se metodik řízení kybernetických bezpečnostních rizik na úrovni subjektů; a

b) kontroly kybernetické bezpečnosti odpovídající kontrolám, které by měly být součástí minimálních a pokročilých kontrol v oblasti kybernetické bezpečnosti.

8. ENTSO pro elektřinu a subjekt EU DSO při dokončování předběžného seznamu norem zohlední stanoviska ENISA a ACER. ENTSO pro elektřinu a subjekt EU DSO zveřejní přechodný seznam evropských a mezinárodních norem a kontrol na svých internetových stránkách.

9. ENTSO pro elektřinu a subjekt EU DSO konzultují s ENISA a ACER návrhy nezávazných pokynů vypracované podle odstavce 1.

10. Dokud nebudou vypracovány minimální a pokročilé kontroly v oblasti kybernetické bezpečnosti podle článku 29 a přijaty podle článku 8, budou všechny subjekty uvedené v čl. 2 odst. 1 usilovat o postupné uplatňování nezávazných pokynů vypracovaných podle odstavce 1.

Článek 49

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 11. března 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN