I

(Uznesenia, odporúčania a stanoviská)

ODPORÚČANIA

EURÓPSKY VÝBOR PRE SYSTÉMOVÉ RIZIKÁ

ODPORÚČANIE EURÓPSKEHO VÝBORU PRE SYSTÉMOVÉ RIZIKÁ

z 2. decembra 2021

o celoeurópskom rámci koordinácie systémových kybernetických incidentov pre príslušné orgány

(ESRB/2021/17)

(2022/C 134/01)

GENERÁLNA RADA EURÓPSKEHO VÝBORU PRE SYSTÉMOVÉ RIZIKÁ,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na Dohodu o Európskom hospodárskom priestore ([1]), a najmä na jej prílohu IX,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 1092/2010 z 24. novembra 2010 o makroprudenciálnom dohľade Európskej únie nad finančným systémom a o zriadení Európskeho výboru pre systémové riziká ([2]), a najmä na jeho článok 3 ods. 2 písm. b) a d) a články 16 a 18,

so zreteľom na rozhodnutie Európskeho výboru pre systémové riziká ESRB/2011/1 z 20. januára 2011, ktorým sa prijíma rokovací poriadok Európskeho výboru pre systémové riziká ([3]), a najmä na jeho články 18 až 20,

keďže:

(1) Ako sa uvádza v odôvodnení 4 odporúčania Európskeho výboru pre systémové riziká ESRB/2013/1 ([4]), konečným cieľom makroprudenciálnej politiky je prispieť k ochrane stability finančného systému ako celku, okrem iného posilňovaním odolnosti finančného systému a obmedzovaním nárastu systémových rizík, a tým zabezpečiť, že finančný sektor bude v udržateľnej miere prispievať k hospodárskemu rastu. Európsky výbor pre systémové riziká (ESRB) zodpovedá za makroprudenciálny dohľad nad finančným systémom v rámci Únie. Pri plnení svojho mandátu by ESRB mal prispievať k prevencii a zmierňovaniu systémových rizík pre finančnú stabilitu vrátane rizík spojených s kybernetickými incidentmi a navrhovať, ako by sa tieto riziká dali zmierniť.

(2) Závažné kybernetické incidenty môžu vzhľadom na svoj potenciál narušiť kritické finančné služby a operácie predstavovať systémové riziko pre finančný systém. Počiatočný šok môže zosilnieť buď vplyvom šírenia prevádzkovej alebo finančnej nákazy, alebo narušením dôvery vo finančný systém. Ak finančný systém tieto šoky nedokáže absorbovať, finančná stabilita bude ohrozená a táto situácia môže viesť k systémovej kybernetickej kríze ([5]).

([1]) Ú. v. ES L 1, 3.1.1994, s. 3.
([2]) Ú. v. EÚ L 331, 15.12.2010, s. 1.
([3]) Ú. v. EÚ C 58, 24.2.2011, s. 4.
([4]) Odporúčanie Európskeho výboru pre systémové riziká ESRB/2013/1 zo 4. apríla 2013 o predbežných cieľoch a nástrojoch makroprudenciálnej politiky (Ú. v. EÚ C 170, 15.6.2013, s. 1).
([5]) Pozri správu *Systemic cyber risk*, ESRB, február 2020, dostupné na webovom sídle ESRB na adrese www.esrb.europa.eu

(3) Neustále sa vyvíjajúce prostredie kybernetických hrozieb a nedávny nárast výskytu závažných kybernetických incidentov sú ukazovateľmi vyššej miery rizika pre finančnú stabilitu v Únii. Pandémia COVID-19 poukázala na to, aké dôležité sú technológie pre fungovanie finančného systému. Príslušné orgány a inštitúcie museli prispôsobiť svoju technickú infraštruktúru a rámce riadenia rizík náhlemu zvýšeniu objemu práce na diaľku, čo zvýšilo celkovú mieru, do akej je finančný systém vystavený kybernetickým hrozbám, a umožnilo páchateľom vymyslieť nové spôsoby, ako páchať trestnú činnosť, a tiež prispôsobiť existujúce tak, aby využili situáciu ([6]). V tejto súvislosti je potrebné uviesť, že sa počet kybernetických incidentov nahlásených bankovému dohľadu ECB v roku 2020 zvýšil o 54 %v porovnaní s rokom 2019 ([7]).

(4) Potenciálny veľký rozsah, rýchlosť a miera šírenia závažných kybernetických incidentov si vyžadujú účinnú reakciu zo strany príslušných orgánov na zmiernenie potenciálnych negatívnych vplyvov na finančnú stabilitu. Rýchla koordinácia a komunikácia medzi príslušnými orgánmi na úrovni Únie môže napomôcť včasnému posúdeniu vplyvu závažných kybernetických incidentov na finančnú stabilitu, zachovaniu dôvery vo finančný systém a obmedzeniu šírenia nákazy do iných finančných inštitúcií, a tak prispieť k zabráneniu tomu, aby sa závažný kybernetický incident stal rizikom pre finančnú stabilitu.

(5) V porovnaní s tradičnými finančnými krízami a krízami likvidity, ktorým príslušné orgány zvyčajne čelia, vzniká východiskový šok novým spôsobom. Okrem finančných aspektov musí celkové hodnotenie rizík zahŕňať rozsah a dosah narušení prevádzky, keďže by mohli ovplyvniť výber makroprudenciálnych nástrojov. Podobne aj finančná stabilita by mohla ovplyvniť výber prostriedkov na zmiernenie prevádzkového rizika zo strany odborníkov na kybernetickú bezpečnosť. To si vyžaduje úzku a rýchlu koordináciu a otvorenú komunikáciu okrem iného s cieľom budovať situačnú informovanosť.

(6) Existuje riziko zlyhania koordinácie orgánov, ktoré treba riešiť. Príslušné orgány v Únii sa budú musieť skoordinovať navzájom aj s inými orgánmi, ako je Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA), s ktorými zvyčajne nemusia spolupracovať. Vzhľadom na to, že veľký počet finančných inštitúcií Únie pôsobí celosvetovo, závažný kybernetický incident sa pravdepodobne nebude týkať len Únie a je tiež možné, že vznikne mimo Únie a môže si vyžadovať koordináciu globálnej reakcie.

(7) Príslušné orgány musia byť na tieto interakcie pripravené. V opačnom prípade by mohlo hroziť, že budú prijímať nejednotné opatrenia, ktoré budú v rozpore s reakciou iných orgánov alebo ohrozia jej dopad. Takéto zlyhanie koordinácie by mohlo posilniť šok pre finančný systém tým, že by viedlo k narušeniu dôvery vo fungovanie finančného systému, čo by v najhoršom prípade predstavovalo riziko pre finančnú stabilitu ([8]). Preto treba prijať potrebné kroky na riešenie rizika ohrozujúceho finančnú stabilitu, ktoré plynie zo zlyhania koordinácie v prípade závažných kybernetických incidentov.

(8) Správa ESRB o *zmierňovaní systémového kybernetického rizika* z roku 2021 ([9]) poukazuje na potrebu vytvoriť celoeurópsky rámec koordinácie systémových kybernetických incidentov (pan-European systemic cyber incident coordination framework – EU-SCICF) pre príslušné orgány v Únii. Cieľom rámca EU-SCICF by bolo zvýšiť mieru pripravenosti príslušných orgánov s cieľom uľahčiť koordinovanú reakciu na potenciálne závažné kybernetické incidenty. Správa ESRB o *zmierňovaní systémového kybernetického rizika* z roku 2021 upravuje hodnotenie ESRB v súvislosti s potrebnými vlastnosťami uvedeného rámca, ktoré by mal mať, aby mohol riešiť riziko zlyhania koordinácie.

(9) Hlavným cieľom tohto odporúčania je nadviazať na jednu z plánovaných úloh európskych orgánov dohľadu podľa návrhu nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora ([10]) (ďalej len „nariadenie o digitálnej prevádzkovej odolnosti“), ktorou je postupne umožniť účinnú koordinovanú reakciu na úrovni Únie v prípade závažného cezhraničného incidentu súvisiaceho s informačnými a komunikačnými technológiami (ďalej len „IKT“) alebo súvisiacej hrozby majúcej systémový vplyv na finančný sektor Únie ako celok. Tento proces povedie k vytvoreniu rámca EU-SCICF pre príslušné orgány.

([6]) Pozri správu *Internet Organised Crime Threat Assessment*, Europol, 2020, dostupné na webovom sídle Europolu na adrese www.europol.europa.eu

([7]) Pozri článok *IT and cyber risk: a constant challenge*, ECB, 2021, dostupné na webovom sídle bankového dohľadu ECB na adrese www.bankingsupervision.europa.eu

([8]) Pozri správu *Systemic cyber risk*, ESRB, február 2020, dostupné na webovom sídle ESRB na adrese www.esrb.europa.eu

([9]) Pozri správu Mitigating systemic cyber risk, ESRB, 2021, (nadchádzajúca).

([10]) COM/2020/595 final.

(10) Cieľom EU-SCICF by nemalo byť nahradiť existujúce rámce, ale preklenúť všetky nedostatky v koordinácii a komunikácii medzi príslušnými orgánmi navzájom, ako aj s inými orgánmi v Únii a inými kľúčovými subjektmi na medzinárodnej úrovni. V tejto súvislosti by sa mala zvážiť pozícia EU-SCICF v prostredí existujúceho rámca pre riešenie finančnej krízy a rámca Únie v oblasti kybernetických incidentov. Pokiaľ ide o vzájomnú koordináciu medzi príslušnými orgánmi, mali by sa popri zapojení agentúry ENISA zvážiť okrem iného úlohy a činnosti skupiny pre spoluprácu v oblasti sietí a informačných systémov (Network and Information Systems – NIS) pre finančné subjekty podľa smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([11]) a koordinačné mechanizmy plánované v rámci založenia spoločnej kybernetickej jednotky.

(11) Návrh na začatie prípravy rámca EU-SCICF má za cieľ najmä podporiť potenciálne úlohy európskych orgánov dohľadu, ako sa predpokladá v návrhu nariadenia o digitálnej prevádzkovej odolnosti. V návrhu nariadenia o digitálnej prevádzkovej odolnosti sa stanovuje, že „európske orgány dohľadu môžu prostredníctvom spoločného výboru a v spolupráci s príslušnými orgánmi, Európskou centrálnou bankou (ECB) a výborom ESRB vytvoriť mechanizmy, ktoré umožnia výmenu účinných postupov vo finančných sektoroch s cieľom zlepšiť situačnú informovanosť a identifikovať spoločné kybernetické zraniteľnosti a riziká naprieč sektormi“ a „môžu vypracovať cvičenia týkajúce sa krízového riadenia, ako aj krízových udalostí zahŕňajúce scenáre kybernetického útoku, aby sa vyvinuli komunikačné kanály a postupne umožnila účinná koordinovaná reakcia na úrovni EÚ v prípade závažného cezhraničného incidentu súvisiaceho s IKT alebo súvisiacej hrozby majúcej systémový vplyv na finančný sektor Únie ako celok“ ([12]). Celoeurópsky rámec, ako je EU-SCICF, zatiaľ neexistuje a mal by sa vytvoriť a vyvinúť v rámci nariadenia o digitálnej prevádzkovej odolnosti.

(12) Vzhľadom na riziko pre finančnú stabilitu v Únii vyplývajúce z kybernetického rizika by sa prípravné práce na postupné vytvorenie rámca EU-SCICF mali v najväčšom možnom rozsahu začať ešte skôr, ako bude právny a politický rámec potrebný na jeho vytvorenie nadobudne v plnom rozsahu uplatniteľný. Tento právny a politický rámec by sa mal v plnom rozsahu dokončiť a sfinalizovať po tom, ako nadobudnú účinnosť príslušné ustanovenia nariadenia o digitálnej prevádzkovej odolnosti a jej delegovaných aktov.

(13) Účinná komunikácia prispieva k situačnej informovanosti medzi príslušnými orgánmi, a preto je počas závažných kybernetických incidentov nevyhnutným predpokladom koordinácie v rámci celej Únie. V tejto súvislosti by sa mala vymedziť komunikačná infraštruktúra potrebná na koordináciu, pokiaľ ide o reakciu na závažný kybernetický incident. Zahŕňalo by to stanovenie druhu informácií, ktoré je potrebné vymieňať, bežné kanály, ktoré sa majú na výmenu týchto informácií používať, a kontaktné miesta, s ktorými by sa informácie mali vymieňať. Výmena informácií musí spĺňať existujúce právne požiadavky. Okrem toho môže byť potrebné, aby príslušné orgány stanovili jasný akčný plán a protokoly, ktoré treba dodržiavať, aby sa zabezpečila náležitá koordinácia medzi orgánmi zapojenými do plánovania koordinovanej reakcie na závažný kybernetický incident.

(14) Systémová kybernetická kríza si vyžiada nadviazanie plnej spolupráce na vnútroštátnej úrovni i na úrovni Únie. Preto by sa v rámci európskych orgánov dohľadu, ECB a príslušných vnútroštátnych orgánov každého členského štátu mohlo uvažovať o určení kontaktných miest, ktoré by sa mali oznámiť európskym orgánom dohľadu, s cieľom stanoviť hlavných účastníkov dialógu v koordinačnej schéme rámca EU-SCICF, ktorých bude potrebné informovať v prípade závažného kybernetického incidentu. Potreba určiť kontaktné miesta by sa mala posúdiť počas vývoja rámca EU-SCICF, pričom treba zohľadniť určené jednotné kontaktné miesto podľa smernice (EÚ) 2016/1148, ktoré členské štáty stanovili pre oblasť bezpečnosti sietí a informačných systémov s cieľom zaistiť cezhraničnú spoluprácu s inými členskými štátmi a so skupinou pre spoluprácu v oblasti NIS ([13]).

(15) Výkon cvičení týkajúcich sa krízového riadenia a krízových udalostí by mohol uľahčiť implementáciu rámca EU-SCICF a umožniť orgánom posúdiť, do akej miery sú pripravené na systémovú kybernetickú krízu na úrovni Únie. Z takýchto cvičení by orgány získali skúsenosti a umožnili by tiež nepretržité zlepšovanie a vývoj rámca EU-SCICF.

([11]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

([12]) Pozri článok 43 návrhu nariadenia o digitálnej prevádzkovej odolnosti.

([13]) Pozri skupinu pre spoluprácu v oblasti NIS, dostupné na webovom sídle Európskej komisie na adrese www.ec.europa.eu

(16) Pre vývoj rámca EU-SCICF je nevyhnutné, aby európske orgány dohľadu spoločne vykonali príslušné prípravné práce s cieľom posúdiť potenciálne kľúčové prvky rámca a zdroje a potreby nevyhnutné pre pokračovanie v jeho vývoji. Potom by európske orgány dohľadu mohli začať pracovať na predbežnej analýze všetkých prekážok, ktoré by im a príslušným orgánom mohli brániť pri vytváraní rámca EU-SCICF a výmene príslušných informácií prostredníctvom komunikačných kanálov v prípade závažných kybernetických incidentov. Takáto analýza by bola dôležitým krokom, od ktorého by sa odvíjal celý ďalší postup, či už kroky legislatívnej povahy, alebo iné podporné iniciatívy, ktoré Európska komisia môže spustiť vo fáze po implementácii nariadenia o digitálnej prevádzkovej odolnosti,

PRIJALA TOTO ODPORÚČANIE:

ODDIEL 1

ODPORÚČANIA

Odporúčanie A – Vytvorenie celoeurópskeho rámca koordinácie systémových kybernetických incidentov (EU-SCICF)

1. Odporúča sa, aby sa európske orgány dohľadu kolektívne prostredníctvom spoločného výboru a spolu s Európskou centrálnou bankou (ECB), Európskym výborom pre systémové riziká (ESRB) a príslušnými vnútroštátnymi orgánmi začali pripravovať na postupné vytvorenie účinnej koordinovanej reakcie na úrovni Únie v prípade závažného cezhraničného incidentu súvisiaceho s IKT alebo súvisiacej hrozby, ktorá by mohla mať systémový vplyv na finančný sektor Únie, ako sa predpokladá v návrhu nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora (ďalej len „nariadenie o digitálnej prevádzkovej odolnosti“), ktorý predložila Komisia. Prípravné práce na zabezpečenie koordinovanej reakcie na úrovni Únie by mali zahŕňať postupné vytvorenie rámca EU-SCICF pre európske orgány dohľadu, ECB, ESRB a príslušné vnútroštátne orgány. Súčasťou by malo byť tiež posúdenie požiadaviek na zdroje pre účinný vývoj rámca EU-SCICF.

2. Odporúča sa, aby európske orgány dohľadu vzhľadom na odporúčanie A bod 1 po konzultácii s ECB a ESRB vykonali mapovanie a následnú analýzu súčasných prekážok, právnych a iných, ktoré by mohli brániť v účinnom vytvorení rámca EU-SCICF.

Odporúčanie B – Určenie kontaktných miest EU-SCICF

Odporúča sa, aby európske orgány dohľadu, ECB a každý členský štát spomedzi svojich príslušných vnútroštátnych orgánov určili hlavné kontaktné miesto, ktoré by sa malo oznámiť európskym orgánom dohľadu. Tento zoznam kontaktov zjednoduší vytváranie rámca EU-SCICF a po jeho zavedení by kontaktné miesta a ESRB mali byť v prípade závažných kybernetických incidentov informované. Malo by sa uvažovať aj o koordinácii EU-SCICF s určeným jednotným kontaktným miestom podľa smernice (EÚ) 2016/1148, ktoré členské štáty stanovili pre oblasť bezpečnosti sietí a informačných systémov s cieľom zaistiť cezhraničnú spoluprácu s inými členskými štátmi a so skupinou pre spoluprácu v oblasti sietí a informačných systémov.

Odporúčanie C – Primerané opatrenia na úrovni Únie

Odporúča sa, aby Komisia na základe výsledkov analýz vykonaných v súlade s odporúčaním A zvážila prijatie primeraných opatrení potrebných na zabezpečenie účinnej koordinácie reakcií na systémové kybernetické incidenty.

ODDIEL 2

IMPLEMENTÁCIA

1. **Vymedzenie pojmov**

Na účely tohto odporúčania sa uplatňuje toto vymedzenie pojmov:

a) „kybernetické“ znamená súvisiace s prepojenou informačnou infraštruktúrou interakcií medzi osobami, procesmi, údajmi a informačnými systémami, v rámci nej alebo prostredníctvom nej ([14]);

([14]) Pozri dokument *Cyber Lexicon*, FSB, 12. november 2018, dostupné na webovom sídle FSB na adrese www.fsb.org

b) „závažný kybernetický incident“ je incident súvisiaci s IKT, ktorý má potenciálne veľký nepriaznivý vplyv na sieť a informačné systémy, ktoré podporujú kritické funkcie finančných subjektov ([15]);

c) „systémová kybernetická kríza“ je závažný kybernetický incident, ktorý spôsobí narušenie finančného systému Únie na úrovni, ktorá môže mať závažné negatívne dôsledky pre plynulé fungovanie vnútorného trhu a fungovanie reálnej ekonomiky. Takáto kríza by mohla vzniknúť v dôsledku závažného kybernetického incidentu, ktorý by spôsobil šoky vo viacerých kanáloch vrátane prevádzkového kanála, kanála dôvery a finančného kanála;

d) „európske orgány dohľadu“ sú Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) zriadený nariadením Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([16]) spolu s Európskym orgánom dohľadu (Európskym orgánom pre poisťovníctvo a dôchodkové poistenie zamestnancov) zriadeným nariadením Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([17]) a s Európskym orgánom dohľadu (Európskym orgánom pre cenné papiere a trhy) zriadeným nariadením Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([18]);

e) „spoločný výbor“ je Spoločný výbor európskych orgánov dohľadu zriadený v článku 54 nariadenia (EÚ) č. 1093/2010, nariadenia (EÚ) č. 1094/2010 a nariadenia (EÚ) č. 1095/2010;

f) „príslušný vnútroštátny orgán“ je:

1. príslušný orgán alebo orgán dohľadu v členskom štáte, ako sa stanovuje v aktoch Únie uvedených v článku 1 ods. 2 nariadenia (EÚ) č. 1093/2010, nariadenia (EÚ) č. 1094/2010 a nariadenia (EÚ) č. 1095/2010, a každý iný príslušný vnútroštátny orgán, ako sa stanovuje v aktoch Únie, ktoré zverujú úlohy európskym orgánom dohľadu;

2. príslušný orgán v členskom štáte určený v súlade s:

i. článkom 4 smernice Európskeho parlamentu a Rady 2013/36/EÚ ([19]) bez toho, aby boli dotknuté osobitné úlohy, ktoré boli ECB udelené nariadením Rady (EÚ) č. 1024/2013 ([20]);

ii. článkom 22 smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 ([21]);

iii. článkom 37 smernice Európskeho parlamentu a Rady 2009/110/ES ([22]);

iv. článkom 4 smernice Európskeho parlamentu a Rady (EÚ) 2019/2034 ([23]);

([15]) Pozri článok 3 bod 7 návrhu nariadenia o digitálnej prevádzkovej odolnosti.

([16]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

([17]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48).

([18]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84).

([19]) Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

([20]) Nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29.10.2013, s. 63).

([21]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35).

([22]) Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES (Ú. v. EÚ L 267, 10.10.2009, s. 7).

([23]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/2034 z 27. novembra 2019 o prudenciálnom dohľade nad investičnými spoločnosťami a o zmene smerníc 2002/87/ES, 2009/65/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/59/EÚ a 2014/65/EÚ (Ú. v. EÚ L 314, 5.12.2019, s. 64).

v. článkom 3 ods. 1 bodom ee) prvou zarážkou návrhu nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937 ([24]);

vi. článkom 11 nariadenia Európskeho parlamentu a Rady (EÚ) č. 909/2014 ([25]);

vii. článkom 22 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 ([26]);

viii. článkom 67 smernice Európskeho parlamentu a Rady 2014/65/EÚ ([27]);

ix. článkom 22 nariadenia (EÚ) č. 648/2012;

x. článkom 44 smernice Európskeho parlamentu a Rady 2011/61/EÚ ([28]);

xi. článkom 97 smernice Európskeho parlamentu a Rady 2009/65/ES ([29]);

xii. článkom 30 smernice Európskeho parlamentu a Rady 2009/138/ES ([30]);

xiii. článkom 12 smernice Európskeho parlamentu a Rady (EÚ) 2016/97 ([31]);

xiv. článkom 47 smernice Európskeho parlamentu a Rady (EÚ) 2016/2341 ([32]);

xv. článkom 22 nariadenia Európskeho parlamentu a Rady (ES) č. 1060/2009 ([33]);

xvi. článkom 3 ods. 2 a článkom 32 smernice Európskeho parlamentu a Rady 2006/43/ES ([34]);

xvii. článkom 40 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/1011 ([35]);

xviii. článkom 29 nariadenia Európskeho parlamentu a Rady (EÚ) 2020/1503 ([36]);

([24]) COM/2020/593 final.

([25]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014, s. 1).

([26]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).

([27]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).

([28]) Smernica Európskeho parlamentu a Rady 2011/61/EU z 8. júna 2011 o správcoch alternatívnych investičných fondov a o zmene a doplnení smerníc 2003/41/ES a 2009/65/ES a nariadení (ES) č. 1060/2009 a (EÚ) č. 1095/2010 (Ú. v. EÚ L 174, 1.7.2011, s. 1).

([29]) Smernica Európskeho parlamentu a Rady 2009/65/ES z 13. júla 2009 o koordinácii zákonov, iných právnych predpisov a správnych opatrení týkajúcich sa podnikov kolektívneho investovania do prevoditeľných cenných papierov (PKIPCP) (Ú. v. EÚ L 302, 17.11.2009, s. 32).

([30]) Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1).

([31]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/97 z 20. januára 2016 o distribúcii poistenia (prepracované znenie) (Ú. v. EÚ L 26, 2.2.2016, s. 19).

([32]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/2341 zo 14. decembra 2016 o činnostiach inštitúcií zamestnaneckého dôchodkového zabezpečenia (IZDZ) a dohľade nad nimi (Ú. v. EÚ L 354, 23.12.2016, s. 37).

([33]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1060/2009 zo 16. septembra 2009 o ratingových agentúrach (Ú. v. EÚ L 302, 17.11.2009, s. 1).

([34]) Smernica Európskeho parlamentu a Rady 2006/43/ES zo 17. mája 2006 o štatutárnom audite ročných účtovných závierok a konsolidovaných účtovných závierok, ktorou sa menia a dopĺňajú smernice Rady 78/660/EHS a 83/349/EHS a ktorou sa zrušuje smernica Rady 84/253/EHS (Ú. v. EÚ L 157, 9.6.2006, s. 87).

([35]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/1011 z 8. júna 2016 o indexoch používaných ako referenčné hodnoty vo finančných nástrojoch a finančných zmluvách alebo na meranie výkonnosti investičných fondov, ktorým sa menia smernice 2008/48/ES a 2014/17/EÚ a nariadenie (EÚ) č. 596/2014 (Ú. v. EÚ L 171, 29.6.2016, s. 1).

([36]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2020/1503 zo 7. októbra 2020 o európskych poskytovateľoch služieb hromadného financovania pre podnikanie a o zmene nariadenia (EÚ) 2017/1129 a smernice (EÚ) 2019/1937 (Ú. v. EÚ L 347, 20.10.2020, s. 1).

3. orgán poverený prijímaním a/alebo aktiváciou opatrení makroprudenciálnej politiky alebo inými úlohami, ktoré sa týkajú finančnej stability, ako je napríklad príslušná podporná analýza, okrem iného vrátane:

   i. určeného orgánu podľa hlavy VII kapitoly 4 smernice 2013/36/EÚ alebo podľa článku 458 ods. 1 nariadenia Európskeho parlamentu a Rady ([37]) (EÚ) č. 575/2013;

   ii. makroprudenciálneho orgánu s cieľmi, opatreniami, úlohami, právomocami, nástrojmi, požiadavkami na zodpovednosť a inými charakteristickými znakmi stanovenými v odporúčaní Európskeho výboru pre systémové riziká ESRB/2011/3 ([38]);

g) „príslušný orgán“ je:

   1. európsky orgán dohľadu;

   2. ECB, pokiaľ ide o úlohy, ktorými bola poverená v súlade s článkom 4 ods. 1 a 2 a článkom 5 ods. 2 nariadenia (EÚ) č. 1024/2013;

   3. príslušný vnútroštátny orgán.

2. **Kritériá implementácie**

Na implementáciu tohto odporúčania sa uplatňujú nasledujúce kritériá:

a) mala by sa venovať náležitá pozornosť zásade opodstatnenej potreby a zásade proporcionality a zároveň zohľadňovať cieľ a obsah každého odporúčania;

b) v súvislosti s každým odporúčaním by mali byť splnené osobitné kritériá súladu stanovené v prílohe.

3. **Lehoty na uskutočnenie nadväzujúcich krokov**

V súlade s článkom 17 ods. 1 nariadenia (EÚ) č. 1092/2010 sú adresáti povinní oznámiť Európskemu parlamentu, Rade, Komisii a ESRB opatrenia prijaté v reakcii na toto odporúčanie alebo náležite odôvodniť prípadné nekonanie. Adresáti sa vyzývajú, aby takéto oznámenie uskutočnili v súlade s týmito lehotami:

1. Odporúčanie A

   a) Európske orgány dohľadu sa vyzývajú, aby do 30. júna 2023, nie však skôr ako šesť mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložili Európskemu parlamentu, Rade, Komisii a ESRB priebežnú správu o implementácii odporúčania A bodu 1.

   b) Európske orgány dohľadu sa vyzývajú, aby do 30. júna 2024, nie však skôr ako 18 mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložili Európskemu parlamentu, Rade, Komisii a ESRB záverečnú správu o implementácii odporúčania A bodu 1.

   c) Európske orgány dohľadu sa vyzývajú, aby do 30. júna 2025, nie však skôr ako 30 mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložili Európskemu parlamentu, Rade, Komisii a ESRB správu o implementácii odporúčania A bodu 2.

2. Odporúčanie B

   Európske orgány dohľadu, ECB a členské štáty sa vyzývajú, aby do 30. júna 2023, nie však skôr ako šesť mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložili Európskemu parlamentu, Rade, Komisii a ESRB správu o implementácii odporúčania B.

3. Odporúčanie C

   a) Komisia sa vyzýva, aby do 31. decembra 2023, nie však skôr ako 12 mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložila Európskemu parlamentu, Rade a ESRB správu o implementácii odporúčania C s ohľadom na priebežnú správu európskych orgánov dohľadu v súlade s odporúčaním A bodom 1.

([37]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

([38]) Odporúčanie Európskeho výboru pre systémové riziká ESRB/2011/3 z 22. decembra 2011 o makroprudenciálnom mandáte vnútroštátnych orgánov (Ú. v. EÚ C 41, 14.2.2012, s. 1).

b) Komisia sa vyzýva, aby do 31. decembra 2025, nie však skôr ako 36 mesiacov po tom, ako nadobudne účinnosť nariadenie o digitálnej prevádzkovej odolnosti, predložila Európskemu parlamentu, Rade a ESRB správu o implementácii odporúčania C s ohľadom na správy európskych orgánov dohľadu v súlade s odporúčaním A.

4. **Monitorovanie a hodnotenie**

1. Sekretariát ESRB bude:

a) pomáhať adresátom tohto odporúčania tým, že zabezpečí koordináciu predkladania správ, poskytne príslušné formuláre a v prípade potreby uvedie podrobnosti o postupe a časovom rámci pre kroky, ktoré je potrebné uskutočniť v nadväznosti na odporúčania;

b) overovať, či adresáti podnikli kroky v nadväznosti na odporúčania, poskytovať pomoc na ich žiadosť, a podávať generálnej rade správy o podniknutých krokoch. Hodnotenia sa uskutočnia takto:

i) do 12 mesiacov od nadobudnutia účinnosti nariadenia o digitálnej prevádzkovej odolnosti, pokiaľ ide o implementáciu odporúčaní A a B;

ii) do 18 mesiacov od nadobudnutia účinnosti nariadenia o digitálnej prevádzkovej odolnosti, pokiaľ ide o implementáciu odporúčania C;

iii) do 24 mesiacov od nadobudnutia účinnosti nariadenia o digitálnej prevádzkovej odolnosti, pokiaľ ide o implementáciu odporúčania A;

iv) do 36 mesiacov od nadobudnutia účinnosti nariadenia o digitálnej prevádzkovej odolnosti, pokiaľ ide o implementáciu odporúčania A;

v) do 42 mesiacov od nadobudnutia účinnosti nariadenia o digitálnej prevádzkovej odolnosti, pokiaľ ide o implementáciu odporúčania C.

2. Generálna rada hodnotí prijaté opatrenia a odôvodnenia oznámené adresátmi tohto odporúčania a v relevantných prípadoch môže rozhodnúť o tom, že toto odporúčanie nebolo zohľadnené a jeho adresát neodôvodnil dostatočne svoju nečinnosť.

Vo Frankfurte nad Mohanom 2. decembra 2021

Vedúci sekretariátu ESRB
v mene Generálnej rady ESRB
Francesco MAZZAFERRO

PRÍLOHA

ŠPECIFIKÁCIA UPLATNITEĽNÝCH KRITÉRIÍ SÚLADU S ODPORÚČANIAMI

Odporúčanie A – Vytvorenie celoeurópskeho rámca koordinácie systémových kybernetických incidentov (EU-SCICF)

V prípade odporúčania A bodu 1 platia nasledujúce kritériá súladu.

1. Európske orgány dohľadu konajúce prostredníctvom spoločného výboru a spolu s Európskou centrálnou bankou (ECB), Európskym výborom pre systémové riziká (ESRB) a príslušnými vnútroštátnymi orgánmi, a ak je to potrebné, po konzultácii s Agentúrou Európskej únie pre sieťovú a informačnú bezpečnosť a s Komisiou, by pri príprave účinnej koordinovanej reakcie na úrovni Únie, ktorá by mala zahŕňať postupné vytvorenie rámca EU-SCICF prostredníctvom výkonu právomocí, ktoré sa predpokladajú v budúcom nariadení Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora (ďalej len „nariadenie o digitálnej prevádzkovej odolnosti“), mali zvážiť zahrnutie týchto aspektov do predpokladanej prípravy rámca EU-SCICF:

   a. analýza požiadaviek na zdroje pre účinný vývoj rámca EU-SCICF;

   b. vypracovanie cvičení týkajúcich sa krízového riadenia, ako aj krízových udalostí zahŕňajúcich scenáre kybernetického útoku s cieľom rozvíjať komunikačné kanály;

   c. vývoj spoločného slovníka;

   d. vypracovanie koherentnej klasifikácie kybernetických incidentov;

   e. vytvorenie bezpečných a spoľahlivých kanálov na výmenu informácií vrátane systémov zálohovania;

   f. určenie kontaktných miest;

   g. riešenie otázky dôvernosti pri výmene informácií;

   h. iniciatívy týkajúce sa spolupráce a výmeny informácií s kybernetickým spravodajstvom v oblasti finančného sektora;

   i. vývoj účinných postupov aktivácie a eskalácie prostredníctvom situačnej informovanosti;

   j. objasnenie úloh účastníkov rámca;

   k. vývoj rozhraní pre medzisektorovú koordináciu a v príslušných prípadoch koordináciu s tretími krajinami;

   l. zaistenie zrozumiteľnej komunikácie príslušných orgánov s verejnosťou s cieľom zachovať dôveru;

   m. vytvorenie vopred stanovených komunikačných platforiem na včasnú komunikáciu;

   n. uskutočnenie primeraných testov rámca vrátane testovania vo viacerých jurisdikciách a koordinácie s tretími krajinami a hodnotení, z ktorých by sa získali poznatky a pomohli by s vývojom rámca;

   o. zabezpečenie účinnej komunikácie a protiopatrení proti dezinformáciám.

Odporúčanie B – Stanovenie kontaktných miest EU-SCICF

V prípade odporúčania B platia nasledujúce kritériá súladu.

1. Európske orgány dohľadu, ECB a príslušné vnútroštátne orgány každého členského štátu by sa mali dohodnúť na spoločnom prístupe k výmene a aktualizácii zoznamu určených kontaktných miest v rámci EU-SCICF.

2. Určenie kontaktného miesta by sa malo posúdiť s ohľadom na určené jednotné kontaktné miesto podľa smernice (EÚ) 2016/1148, ktoré členské štáty určili v súvislosti s bezpečnosťou sietí a informačných systémov s cieľom zaistiť cezhraničnú spoluprácu s inými členskými štátmi a so skupinou pre spoluprácu v oblasti sietí a informačných systémov.

Odporúčanie C – Zmeny právneho rámca Únie

V prípade odporúčania C platí nasledujúce kritérium súladu.

Komisia by mala zvážiť, či sú na základe analýzy vykonanej v súlade s odporúčaním A potrebné akékoľvek opatrenia vrátane zmien príslušných právnych predpisov Únie s cieľom zabezpečiť, aby európske orgány dohľadu mohli prostredníctvom spoločného výboru a spolu s ECB, ESRB a príslušnými vnútroštátnymi orgánmi vytvoriť rámec EU-SCICF v súlade s odporúčaním A bodom 1 a aby sa európske orgány dohľadu, ECB, ESRB a príslušné vnútroštátne orgány, ako aj iné orgány mohli zapojiť do koordinačných činností a výmeny informácií, ktoré sú dostatočne podrobné a jednotné, aby podporili účinný rámec EU-SCICF.