I

(Usnesení, doporučení a stanoviska)

DOPORUČENÍ

EVROPSKÁ RADA PRO SYSTÉMOVÁ RIZIKA

DOPORUČENÍ EVROPSKÉ RADY PRO SYSTÉMOVÁ RIZIKA

ze dne 2. prosince 2021

o celoevropském rámci pro koordinaci příslušných orgánů v případě systémových kybernetických bezpečnostních incidentů (EU-SCICF)

(ESRB/2021/17)

(2022/C 134/01)

GENERÁLNÍ RADA EVROPSKÉ RADY PRO SYSTÉMOVÁ RIZIKA,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na Dohodu o Evropském hospodářském prostoru ([1]), zejména na přílohu IX uvedené dohody,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 1092/2010 ze dne 24. listopadu 2010 o makroobezřetnostním dohledu nad finančním systémem na úrovni Evropské unie a o zřízení Evropské rady pro systémová rizika ([2]), a zejména na čl. 3 odst. 2 písm. b) a d) a články 16 a 18 uvedeného nařízení,

s ohledem na rozhodnutí Evropské rady pro systémová rizika ESRB/2011/1 ze dne 20. ledna 2011, kterým se přijímá jednací řád Evropské rady pro systémová rizika ([3]), a zejména na články 18 až 20 uvedeného rozhodnutí,

vzhledem k těmto důvodům:

(1) Jak je uvedeno ve 4. bodě odůvodnění doporučení Evropské rady pro systémová rizika ESRB/2013/1 ([4]), konečným cílem makroobezřetnostní politiky je přispět k zajištění stability finančního systému jako celku, mimo jiné posilováním odolnosti finančního systému a omezováním nárůstu systémových rizik, a tím zaručit, že finanční sektor bude v udržitelné míře přispívat k hospodářskému růstu. Evropská rada pro systémová rizika (ESRB) odpovídá za makroobezřetnostní dohled nad finančním systémem v Unii. Při plnění svého mandátu by ESRB měla přispívat k prevenci a zmírňování systémových rizik pro finanční stabilitu, včetně rizik spojených s kybernetickými bezpečnostními incidenty, a navrhovat způsob zmírnění těchto rizik.

(2) Vzhledem ke svému potenciálu narušit kritické finanční služby a operace mohou závažné kybernetické bezpečnostní incidenty představovat systémové riziko pro finanční systém. K zesílení počátečního šoku může dojít buď šířením provozní nebo finanční nákazy nebo narušením důvěry ve finanční systém. Není-li finanční systém schopen tyto otřesy absorbovat, bude ohrožena finanční stabilita a tato situace může vést k systémové kybernetické krizi ([5]).

([1]) Úř. věst. L 1, 3.1. 1994, s. 3.
([2]) Úř. věst. L 331, 15.12.2010, s. 1.
([3]) Úř. věst. C 58, 24.2.2011, s. 4.
([4]) Doporučení Evropské rady pro systémová rizika ESRB/2013/1 ze dne 4. dubna 2013 o průběžných cílech a nástrojích makroobezřetnostní politiky (Úř. Věst. C 170, 15.6.2013, s. 1).
([5]) Viz dokument ESRB s názvem „Systemic cyber risk“, únor 2020, k dispozici na internetových stránkách ESRB www.esrb.europa.eu

(3) Neustálý vývoj kybernetických hrozeb a nedávný nárůst závažných kybernetických bezpečnostních incidentů jsou ukazateli zvýšeného rizika pro finanční stabilitu v Unii. Pandemie COVID-19 zdůraznila význam úlohy technologie pro fungování finančního systému. Příslušné orgány a instituce musely přizpůsobit svou technickou infrastrukturu a rámce pro řízení rizik náhlému nárůstu práce na dálku, což zvýšilo celkovou expozici finančního systému vůči kybernetickým hrozbám a umožnilo pachatelům trestné činnosti nalézt nové způsoby fungování a přizpůsobit stávající metody s cílem využít dané situace ([6]). V této souvislosti je třeba uvést, že počet kybernetických bezpečnostních incidentů oznámených bankovnímu dohledu ECB se v roce 2020 zvýšil o 54 % ve srovnání s rokem 2019 ([7]).

(4) Potenciálně velký rozsah, rychlost a míra šíření významného kybernetického bezpečnostního incidentu vyžadují účinnou reakci ze strany příslušných orgánů s cílem zmírnit možné negativní dopady na finanční stabilitu. Rychlá koordinace a komunikace mezi příslušnými orgány na úrovni Unie může pomoci včas posoudit dopad významného kybernetického bezpečnostního incidentu na finanční stabilitu, zachovat důvěru ve finanční systém a omezit rozšíření nákazy na jiné finanční instituce, a přispět tak k tomu, aby se významný kybernetický bezpečnostní incident nestal rizikem pro finanční stabilitu.

(5) Ve srovnání s tradiční finanční a likviditní krizí, které příslušné orgány obvykle čelí, vzniká výchozí otřes novým způsobem. Kromě finančních aspektů musí celkové posouzení rizik zahrnovat rozsah a dopad narušení provozu, neboť to může ovlivnit výběr makroobezřetnostních nástrojů. Finanční stabilita může rovněž podobně ovlivnit volbu prostředků ke zmírnění operačního rizika ze strany odborníků na kybernetickou bezpečnost. To vyžaduje úzkou a rychlou koordinaci a otevřenou komunikaci s cílem mimo jiné zvýšit informovanost o situaci.

(6) Selhání koordinace mezi jednotlivými orgány je reálným rizikem, které je třeba řešit. Bude zapotřebí, aby příslušné orgány v Unii spolupracovaly jak navzájem, tak i s jinými orgány, jako je například Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), s níž nemusí běžně komunikovat. Vzhledem k tomu, že značný počet finančních institucí Unie působí globálně, závažný kybernetický bezpečnostní incident se pravděpodobně projeví nejen v Unii, nebo případně může být vyvolán mimo Unii a může vyžadovat koordinaci globální reakce.

(7) Je zapotřebí, aby příslušné orgány byly na tyto koordinované postupy připraveny. Jinak hrozí, že přijmou nejednotná opatření, která budou v rozporu s reakcí jiných orgánů nebo ohrozí jejich účinek. Uvedené selhání koordinace by mohlo zesílit otřes pro finanční systém tím, že povede k podlomení důvěry ve fungování finančního systému, což by v případě nejhoršího scénáře mohlo představovat riziko pro finanční stabilitu ([8]). Je proto třeba přijmout nezbytné kroky k řešení rizika pro finanční stabilitu, které vyplývá ze selhání koordinace v případě závažného kybernetického bezpečnostního incidentu.

(8) Ve zprávě ESRB o zmírňování systémového kybernetického rizika z roku 2021 ([9]) se konstatuje, že je zapotřebí vytvořit celoevropský rámec pro koordinaci příslušných orgánů v případě systémových kybernetických bezpečnostních incidentů (*pan-European systemic cyber incident coordination framework* - EU-SCICF). Cílem EU-SCICF by bylo zvýšit míru připravenosti příslušných orgánů s cílem usnadnit koordinovanou reakci na potencionálně závažný kybernetický bezpečnostní incident. Zpráva ESRB o zmírňování systémového kybernetického rizika z roku 2021 obsahuje hodnocení charakteristik, které by měl uvedený rámec nevyhnutelně mít, aby řešil riziko selhání koordinace.

(9) Hlavním cílem tohoto doporučení je navázat na jednu z předpokládaných úloh evropských orgánů dohledu podle návrhu nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru ([10]) (dále jen „DORA“), která spočívá v postupném umožnění účinné koordinované reakce na úrovni Unie v případě závažného přeshraničního incidentu souvisejícího s informačními a komunikačními technologiemi (IKT) nebo související hrozby se systémovým dopadem na celý finanční sektor Unie. Tento proces povede k vytvoření rámce EU-SCICF pro příslušné orgány.

([6]) Viz zpráva Europolu s názvem „Internet Organised Crime Threat Assessment“, 2020, k dispozici na internetových stránkách Europolu www.europol.europa.eu

([7]) Viz dokument s názvem „IT and cyber risk: a constant challenge“, ECB, 2021, k dispozici na internetových stránkách bankovního dohledu ECB www.bankingsupervision.europa.eu

([8]) Viz zpráva ESRB s názvem „Systemic cyber risk“ z února 2020, k dispozici na internetových stránkách ESRB www.esrb.europa.eu

([9]) Viz „Mitigating systemic cyber risk“, ESRB, 2021, (nadcházející).

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

(10) Cílem EU-SCICF by nemělo být nahradit stávající rámce, ale překlenout případné mezery v koordinaci a komunikaci mezi příslušnými orgány navzájem a s ostatními orgány v Unii a dalšími klíčovými subjekty na mezinárodní úrovni. V této souvislosti je třeba zvážit postavení EU-SCICF ve stávajícím rámci pro řešení finančních krizí a rámci Unie pro kybernetické bezpečnostní incidenty. Pokud jde o koordinaci mezi příslušnými orgány navzájem, je vedle zapojení agentury ENISA třeba mimo jiné zvážit úlohy a činnosti skupiny pro spolupráci v oblasti sítí a informačních systémů pro finanční subjekty podle směrnice (EU) Evropského parlamentu a Rady 2016/1148 ([11]), jakož i mechanismy koordinace, s nimiž se počítá prostřednictvím zřízení Společné kybernetické jednotky.

(11) Cílem návrhu na zahájení přípravy EU-SCICF je zejména podpořit potenciální úlohy evropských orgánů dohledu ve smyslu návrhu nařízení DORA. V návrhu nařízení DORA se uvádí, že „evropské orgány dohledu mohou prostřednictvím společného výboru a ve spolupráci s příslušnými orgány, Evropskou centrální bankou (ECB) a ESRB vytvářet mechanismy umožňující sdílení osvědčených postupů ve finančních odvětvích, které zlepší znalost situace a identifikují společná kybernetická zranitelná místa a rizika napříč odvětvími“ a „mohou připravovat cvičení v oblastech krizového řízení a reakce na nepředvídané události zahrnující scénáře kybernetického útoku, jejichž cílem bude rozvoj komunikačních kanálů a postupné umožnění účinné koordinované reakce na úrovni EU v případě závažného přeshraničního incidentu souvisejícího s IKT nebo související hrozby se systémovým dopadem na celý finanční sektor Unie“ ([12]). Celoevropský rámec, jako je EU-SCICF, dosud neexistuje a měl by být vytvořen a rozvíjen v kontextu DORA.

(12) Vzhledem k riziku pro finanční stabilitu v Unii vyplývajícímu z kybernetického rizika by přípravné práce na postupném vytvoření EU-SCICF měly být v maximálním možném rozsahu zahájeny ještě předtím, než bude požadovaný právní a politický rámec pro jeho vytvoření plně použitelný. Tento právní a politický rámec bude v plném rozsahu dokončen, jakmile začnou platit příslušná ustanovení nařízení DORA a souvisejících aktů v přenesené pravomoci.

(13) Účinná komunikace přispívá k zajištění informovanosti o situaci mezi příslušnými orgány, a je tudíž nezbytným předpokladem pro celounijní koordinaci během závažných kybernetických bezpečnostních incidentů. V této souvislosti by měla být vymezena komunikační infrastruktura potřebná ke koordinaci reakce na závažný kybernetický bezpečnostní incident. To by znamenalo stanovit druh informací, které je třeba sdílet, obvyklé kanály, které mají být používány ke sdílení těchto informací, a kontaktní místa, s nimiž by měly být informace sdíleny. Sdílení informací musí respektovat stávající právní požadavky. Kromě toho může být nutné, aby příslušné orgány stanovily jasný akční plán a protokoly, které je třeba dodržovat, aby byla zajištěna řádná koordinace mezi orgány zapojenými do přípravy koordinované reakce na závažný kybernetický bezpečnostní incident.

(14) Systémová kybernetická krize bude vyžadovat zahájení plné spolupráce na vnitrostátní úrovni i na úrovni Unie. Proto lze uvažovat o vytvoření kontaktních míst v rámci evropských orgánů dohledu, ECB a příslušných vnitrostátních orgánů každého členského státu, která by měla být oznámena evropským orgánům dohledu, s cílem určit hlavní partnery v koordinačním systému EU-SCICF, kteří by byli informováni v případě závažného kybernetického bezpečnostního incidentu. Potřeba určit kontaktní místa by měla být posouzena během vytváření EU-SCICF, a to s ohledem na určené jednotné kontaktní místo podle směrnice (EU) 2016/1148, které členské státy zřídily pro oblast bezpečnosti sítí a informačních systémů s cílem zajistit přeshraniční spolupráci s ostatními členskými státy a se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací ([13]).

(15) Provádění cvičení v oblastech krizového řízení a reakce na nepředvídané události by mohlo usnadnit implementaci EU-SCICF a umožnit orgánům vyhodnotit jejich připravenost na systémovou kybernetickou krizi na úrovni Unie. Tato cvičení by orgánům poskytla poznatky a umožnila by neustálé zlepšování a vývoj EU-SCICF.

([11]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

([12]) Viz článek 43 návrhu nařízení DORA.

([13]) Viz Evropská komise, skupina pro spolupráci v oblasti bezpečnosti sítí a informací, k dispozici na internetových stránkách Evropské komise na adrese ec.europa.eu

(16) Pro vytvoření EU-SCICF je zásadní, aby evropské orgány dohledu společně provedly příslušné přípravné práce s cílem posoudit potenciální klíčové prvky rámce, jakož i zdroje a potřeby, které jsou nezbytné k jeho dalšímu rozvoji. Poté by evropské orgány dohledu mohly začít pracovat na předběžné analýze případných překážek, které by evropským orgánům dohledu a příslušným orgánům mohly bránit ve vytvoření EU-SCICF a výměně příslušných informací prostřednictvím komunikačních kanálů v případě závažného kybernetického bezpečnostního incidentu. Tato analýza by byla důležitým krokem, od něhož by se odvíjela jakákoli další opatření, ať už legislativní povahy, nebo jiné podpůrné iniciativy, které může Evropská komise přijmout ve fázi po zavedení DORA,

PŘIJALA TOTO DOPORUČENÍ:

ODDÍL 1

DOPORUČENÍ

Doporučení A – Vytvoření celoevropského rámce pro koordinaci v případě systémových kybernetických bezpečnostních incidentů (EU-SCICF)

1. V souladu s návrhem nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru (dále jen „DORA“), který předložila Komise, se doporučuje, aby evropské orgány dohledu společně prostřednictvím společného výboru a ve spolupráci s Evropskou centrální bankou (ECB), Evropskou radou pro systémová rizika (ESRB) a příslušnými vnitrostátními orgány zahájily přípravu na postupném vytvoření účinné koordinované reakce na úrovni Unie v případě závažného přeshraničního kybernetického bezpečnostního incidentu nebo související hrozby, jež by mohla mít systémový dopad na finanční sektor Unie. Přípravné práce k zajištění koordinované reakce na úrovni Unie by měly zahrnovat postupné vytvoření celoevropského rámce pro koordinaci evropských orgánů dohledu, ECB, ESRB a příslušných vnitrostátních orgánů v případě systémových kybernetických bezpečnostních incidentů. Tyto práce by měly rovněž zahrnovat posouzení požadavků na zdroje pro účinné vytvoření EU-SCICF.

2. Doporučuje se, aby evropské orgány dohledu s ohledem na dílčí doporučení A.1 provedly po konzultaci s ECB a ESRB zmapování a následnou analýzu stávajících překážek - právních a jiných provozních překážek - bránících účinnému vytvoření EU-SCICF.

Doporučení B – Zřízení kontaktních míst pro účely EU-SCICF

Doporučuje se, aby evropské orgány dohledu, ECB a každý členský stát mezi svými příslušnými vnitrostátními orgány určily hlavní kontaktní místo, které by mělo být oznámeno evropským orgánům dohledu. Tento seznam kontaktních míst usnadní vytváření rámce / EU-SCICF a po jeho zavedení by kontaktní místa a ESRB měly být informovány v případě závažného kybernetického bezpečnostního incidentu. Mělo by se rovněž uvažovat o koordinaci mezi EU-SCICF a určeným jednotným kontaktním místem podle směrnice (EU) 2016/1148, které členské státy zřídily pro oblast bezpečnosti sítí a informačních systémů s cílem zajistit přeshraniční spolupráci s ostatními členskými státy a se skupinou pro spolupráci v oblasti sítí a informačních systémů.

Doporučení C – Vhodná opatření na úrovni Unie

Doporučuje se, aby Komise na základě výsledků analýzy provedené v souladu s doporučením A zvážila přijetí vhodných opatření nezbytných k zajištění účinné koordinace reakcí na systémové kybernetické bezpečnostní incidenty.

ODDÍL 2

PROVÁDĚNÍ

1. **Definice**

Pro účely tohoto doporučení se použijí tyto definice:

a) výrazem „kybernetický“ se rozumí týkající se propojené informační infrastruktury interakcí mezi osobami, procesy, daty a informačními systémy, včetně jevů probíhajících uvnitř této infrastruktury nebo jejím prostřednictvím ([14])

([14]) Viz dokument Rady pro finanční stabilitu s názvem „Cyber Lexicon“, ze dne 12. listopadu 2018, k dispozici na internetových stránkách FSB www.fsb.org.

b) „závažným kybernetickým bezpečnostním incidentem“ se rozumí incident související s IKT s potenciálně rozsáhlými nepříznivými dopady na síť a informační systémy využívané k zajištění zásadních funkcí finančních subjektů ([15]);

c) „systémovou kybernetickou krizi“ se rozumí závažný kybernetický incident, který způsobí takovou míru narušení finančního systému Unie, která by mohla mít závažné negativní důsledky pro hladké fungování vnitřního trhu a fungování reálné ekonomiky. Taková krize by mohla být důsledkem závažného kybernetického incidentu, který způsobuje šoky v řadě kanálů, včetně operačního kanálu, kanálu důvěry a finančního kanálu;

d) „evropskými orgány dohledu“ se rozumí Evropský orgán dohledu (Evropský orgán pro bankovnictví) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1093/2010 ([16]), Evropský orgán dohledu (Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1094/2010 ([17]) a Evropský orgán dohledu (Evropský orgán pro cenné papíry a trhy) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1095/2010 ([18]).

e) „společným výborem“ se rozumí společný výbor evropských orgánů dohledu zřízený článkem 54 nařízení (EU) č. 1093/2010, nařízení (EU) č. 1094/2010 a nařízení (EU) č. 1095/2010;

f) „příslušným vnitrostátním orgánem“ se rozumí:

1. příslušný orgán nebo orgán dohledu v členském státě stanovený v aktech Unie uvedených v čl. 1 odst. 2 nařízení (EU) č. 1093/2010, nařízení (EU) č. 1094/2010 a nařízení (EU) č. 1095/2010, a jakýkoli jiný vnitrostátní příslušný orgán stanovený v aktech Unie, které svěřují úkoly evropským orgánům dohledu;

2. příslušný orgán v členském státě určený v souladu s:

i. článkem 4 směrnice Evropského parlamentu a Rady 2013/36/EU ([19]), aniž jsou dotčeny zvláštní úkoly svěřené ECB nařízením Rady (EU) č. 1024/2013 ([20]);

ii. článkem 22 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ([21]);

iii. článkem 37 směrnice Evropského parlamentu a Rady 2009/110/ES ([22]);

iv. článkem 4 směrnice Evropského parlamentu a Rady (EU) 2019/2034 ([23]);

([15]) Viz čl. 3 bod 7 návrhu nařízení DORA.

([16]) Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

([17]) Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES ((Úř. věst. L 331, 15.12.2010, s. 48).

([18]) Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84).

([19]) Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

([20]) Nařízení Rady (EU) č. 1024/2013 ze dne 15. října 2013, kterým se Evropské centrální bance svěřují zvláštní úkoly týkající se politik, které se vztahují k obezřetnostnímu dohledu nad úvěrovými institucemi (Úř. věst. L 287, 29.10.2013, s. 63).

([21]) Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, o změně směrnice 2002/65/ES, 2009/110/ES, 2013/36/EU a nařízení (EU) č. 1093/2010 a o zrušení směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35).

([22]) Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES (Úř. věst. L 267, 10.10.2009, s. 7).

([23]) Směrnice Evropského parlamentu a Rady (EU) 2019/2034 ze dne 27. listopadu 2019 o obezřetnostním dohledu nad investičními podniky a o změně směrnic 2002/87/ES, 2009/65/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU a 2014/65/EU (Úř. věst. L 314, 5.12.2019, s. 64).

v. čl. 3 odst. 1 bodem ee) první odrážkou návrhu nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937 ([24]);

vi. článkem 11 nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ([25]);

vii. článkem 22 nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ([26]);

viii. článkem 67 směrnice Evropského parlamentu a Rady 2014/65/ES ([27]);

ix. článkem 22 nařízení (EU) č. 648/2012;

x. článkem 44 směrnice Evropského parlamentu a Rady 2011/61/EU ([28]);

xi. článkem 97 směrnice Evropského parlamentu a Rady 2009/65/ES ([29]);

xii. článkem 30 směrnice Evropského parlamentu a Rady 2009/138/ES ([30]);

xiii. článkem 12 směrnice Evropského parlamentu a Rady (EU) 2016/97 ([31]);

xiv. článkem 47 směrnice Evropského parlamentu a Rady (EU) 2016/2341 ([32]);

xv. článkem 22 nařízení Evropského parlamentu a Rady (ES) č. 1060/2009 ([33]);

xvi. čl. 3 odst. 2 a článkem 32 směrnice Evropského parlamentu a Rady 2006/43/ES ([34]);

xvii. článkem 40 nařízení Evropského parlamentu a Rady (EU) 2016/1011 ([35]);

xviii. článkem 29 nařízení Evropského parlamentu a Rady (EU) 2020/1503 ([36]);

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

([25]) Nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnic 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012 (Úř. věst. L 257, 28.8.2014, s. 1).

([26]) Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1).

([27]) Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349).

([28]) Směrnice Evropského parlamentu a Rady 2011/61/EU ze dne 8. června 2011 o správcích alternativních investičních fondů a o změně směrnic 2003/41/ES a 2009/65/ES a nařízení (ES) č. 1060/2009 a (EU) č. 1095/2010 (Úř. věst. L 174, 1.7.2011, s. 1).

([29]) Směrnice Evropského parlamentu a Rady 2009/65/ES ze dne 13. července 2009 o koordinaci právních a správních předpisů týkajících se subjektů kolektivního investování do převoditelných cenných papírů (SKIPCP) (Úř. věst. L 302, 17.11.2009, s. 32).

([30]) Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II) (Úř. věst. L 335, 17.12.2009, s. 1).

([31]) Směrnice Evropského parlamentu a Rady (EU) 2016/97 ze dne 20. ledna 2016 o distribuci pojištění (Úř. věst. L 26, 2.2.2016, s. 19).

([32]) Směrnice Evropského parlamentu a Rady (EU) 2016/2341 ze dne 14. prosince 2016 o činnostech institucí zaměstnaneckého penzijního pojištění (IZPP) a dohledu nad nimi (Úř. věst. L 354, 23.12.2016, s. 37).

([33]) Nařízení Evropského parlamentu a Rady (ES) č. 1060/2009 ze dne 16. září 2009 o ratingových agenturách (Úř. věst. L 302, 17.11.2009, s. 1).

([34]) Směrnice Evropského parlamentu a Rady 2006/43/ES ze dne 17. května 2006 o povinném auditu ročních a konsolidovaných účetních závěrek, o změně směrnic Rady 78/660/EHS a 83/349/EHS a o zrušení směrnice Rady 84/253/EHS (Úř. věst. L 157, 9.6.2006, s. 87).

([35]) Nařízení Evropského parlamentu a Rady (EU) 2016/1011 ze dne 8. června 2016 o indexech, které jsou používány jako referenční hodnoty ve finančních nástrojích a finančních smlouvách nebo k měření výkonnosti investičních fondů, a o změně směrnic 2008/48/ES a 2014/17/EU a nařízení (EU) č. 596/2014 (Úř. věst. L 171, 29.6.2016, s. 1).

([36]) Nařízení Evropského parlamentu a Rady (EU) 2020/1503 ze dne 7. října 2020 o evropských poskytovatelích služeb skupinového financování pro podniky a o změně nařízení (EU) 2017/1129 a směrnice (EU) 2019/1937 (EU) 2019/1937 (Úř. věst. L 347, 20.10.2020, s. 1).

3. orgán pověřený přijímáním a/nebo aktivací opatření makroobezřetnostní politiky nebo jinými úkoly v oblasti finanční stability, jako je související podpůrná analýza, a to včetně:

   i. pověřeného orgánu podle kapitoly 4 hlavy VII směrnice 2013/36/EU nebo čl. 458 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ([37]);

   ii. makroobezřetnostní orgán s cíli, mechanismy, úkoly, pravomocemi, nástroji, požadavky týkajícími se odpovědnosti a jinými znaky vymezenými v doporučení Evropské rady pro systémová rizika ESRB/2011/3 ([38]);

g) „relevantním orgánem" se rozumí:

   1. evropský orgán dohledu;

   2. ECB, pokud jde o úkoly, které jí byly svěřeny v souladu s čl. 4 odst. 1 a 2 a čl. 5 odst. 2 nařízení (EU) č. 1024/2013;

   3. příslušný vnitrostátní orgán;

2. **Prováděcí kritéria**

Při provádění tohoto doporučení se uplatňují následující kritéria:

a) náležitou pozornost je třeba věnovat zásadě „vědět jen to nejnutnější" a zásadě proporcionality při současném zohlednění cíle a obsahu každého doporučení;

b) ve vztahu ke každému doporučení by měla být splněna zvláštní kritéria pro soulad, která jsou stanovena v příloze.

3. **Časový rámec pro návazné kroky**

V souladu s čl. 17 odst. 1 nařízení (EU) č. 1092/2010 jsou adresáti povinni informovat Evropský parlament, Radu, Komisi a ESRB o opatřeních přijatých v reakci na toto doporučení nebo odůvodnit případnou nečinnost. Adresáti se vyzývají, aby toto sdělení předložili v souladu s tímto časovým rámcem:

1. Doporučení A

   a) Evropské orgány dohledu se vyzývají, aby do 30. června 2023, avšak nejdříve šest měsíců po vstupu nařízení DORA v platnost, předložily Evropskému parlamentu, Radě, Komisi a ESRB předběžnou zprávu o provádění dílčího doporučení A.1.

   b) Evropské orgány dohledu se vyzývají, aby do 30. června 2024, avšak nejdříve 18 měsíců po vstupu nařízení DORA v platnost, předložily Evropskému parlamentu, Radě, Komisi a ESRB závěrečnou zprávu o provádění dílčího doporučení A.1.

   c) Evropské orgány dohledu se vyzývají, aby do 30. června 2025, avšak nejdříve 30 měsíců po vstupu nařízení DORA v platnost, předložily Evropskému parlamentu, Radě, Komisi a ESRB zprávu o provádění dílčího doporučení A.2.

2. Doporučení B

   Evropské orgány dohledu, ECB a členské státy se vyzývají, aby do 30. června 2023, avšak nejdříve šest měsíců po vstupu nařízení DORA v platnost, předložili Evropskému parlamentu, Radě, Komisi a ESRB zprávu o provádění doporučení B.

3. Doporučení C

   a) Komise se vyzývá, aby do 31. prosince 2023, avšak nejdříve 12 měsíců po vstupu nařízení DORA v platnost, předložila Evropskému parlamentu, Radě a ESRB zprávu o provádění doporučení C s ohledem na průběžnou zprávu evropských orgánů dohledu podle dílčího doporučení A.1.

([37]) Nařízení Evropského parlamentu a rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

([38]) Doporučení Evropské rady pro systémová rizika ESRB/2011/3 ze dne 22. prosince 2011 o makroobezřetnostním mandátu vnitrostátních orgánů (Úř. věst. C 41, 14.2.2012, s. 1).

b) Komise se vyzývá, aby do 31. prosince 2025, avšak nejdříve 36 měsíců po vstupu nařízení DORA v platnost, předložila Evropskému parlamentu, Radě a ESRB zprávu o provádění doporučení C s ohledem na zprávy evropských orgánů dohledu podle doporučení A.

4. **Sledování a hodnocení**

1. Sekretariát ESRB bude:

a) napomáhat adresátům tím, že zajistí koordinaci podávání zpráv, poskytne jim příslušné vzory a v případě potřeby upřesní postup a lhůty pro návazné kroky;

b) ověřovat provádění návazných kroků ze strany adresátů doporučení, poskytovat jim pomoc na jejich žádost a podávat generální radě zprávy o návazných krocích. Hodnocení se uskuteční takto:

i) do 12 měsíců od vstupu nařízení DORA v platnost, pokud se týká provádění doporučení A a B;

ii) do 18 měsíců od vstupu nařízení DORA v platnost, pokud se týká provádění doporučení C;

iii) do 24 měsíců od vstupu nařízení DORA v platnost, pokud se týká provádění doporučení A;

iv) do 36 měsíců od vstupu nařízení DORA v platnost, pokud se týká provádění doporučení A;

v) do 42 měsíců od vstupu nařízení DORA v platnost, pokud se týká provádění doporučení C;

2. Generální rada vyhodnotí přijatá opatření a zdůvodnění oznámená adresáty tohoto doporučení a případně může rozhodnout, že toto doporučení nebylo zohledněno a že adresát řádně neodůvodnil svou nečinnost.

Ve Frankfurtu nad Mohanem dne 2. prosince 2021.

Vedoucí sekretariátu ESRB
jménem generální rady ESRB
Francesco MAZZAFERRO

PŘÍLOHA

SPECIFIKACE KRITÉRIÍ PRO SOULAD S DOPORUČENÍMI

Doporučení A – Vytvoření celoevropského rámce pro koordinaci v případě systémových kybernetických bezpečnostních incidentů (EU-SCICF)

V případě dílčího doporučení A.1 platí následující kritéria souladu.

1. Při přípravě účinné koordinované reakce na úrovni Unie, která by měla zahrnovat postupné vytvoření EU-SCICF prostřednictvím výkonu pravomocí stanovených v budoucím nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru (dále jen „DORA“), by evropské orgány dohledu jednající prostřednictvím společného výboru a společně s Evropskou centrální bankou (ECB), Evropskou radou pro systémová rizika (ESRB) a příslušnými vnitrostátními orgány, a v případě potřeby po konzultaci s Agenturou Evropské unie pro bezpečnost sítí a informací a Komisí, měly zvážit zahrnutí následujících aspektů do plánované přípravy EU-SCICF:

   a. analýza požadavků na zdroje pro účinný rozvoj EU-SCICF;

   b. příprava cvičení v oblastech krizového řízení a reakce na nepředvídané události zahrnující scénáře kybernetického útoku, jejichž cílem bude rozvoj komunikačních kanálů;

   c. vypracování společného slovníku;

   d. vytvoření jednotné klasifikace kybernetických incidentů;

   e. zřízení bezpečných a spolehlivých kanálů pro sdílení informací, včetně záložních systémů;

   f. zřízení kontaktních míst;

   g. řešení otázek důvěrnosti při sdílení informací;

   h. iniciativy v oblasti spolupráce a sdílení informací s kybernetickou zpravodajskou komunitou pro oblast finančního sektoru;

   i. rozvoj účinných procesů aktivace a eskalace prostřednictvím informovanosti o situaci;

   j. vyjasnění povinností účastníků rámce;

   k. rozvoj rozhraní pro meziodvětvovou koordinaci a případně koordinaci s třetími zeměmi;

   l. zajištění soudržné komunikace příslušných orgánů s veřejností s cílem zachovat důvěru;

   m. vytvoření předem určených komunikačních kanálů pro včasnou komunikaci;

   n. provádění vhodného testování rámce včetně testování v rámci více jurisdikcí a koordinace se třetími zeměmi, a hodnocení, jejichž výsledkem jsou získané poznatky a vývoj rámce;

   o. zajištění účinné komunikace a protiopatření proti dezinformacím.

Doporučení B – Zřízení kontaktních míst pro účely EU-SCICF

V případě doporučení B platí následující kritéria souladu.

1. Evropské orgány dohledu, ECB a každý členský stát v rámci svých příslušných vnitrostátních orgánů by se měly dohodnout na společném přístupu ke sdílení a aktualizaci seznamu určených kontaktních míst EU-SCICF.

2. Při určení kontaktního místa je třeba vzít v úvahu určené jednotné kontaktní místo podle směrnice (EU) 2016/1148, které členské státy zřídily pro bezpečnost sítí a informačních systémů s cílem zajistit přeshraniční spolupráci s ostatními členskými státy a se skupinou pro spolupráci v oblasti sítí a informačních systémů.

Doporučení C – Změny právního rámce Unie

V případě doporučení C platí následující kritéria souladu.

Komise by měla zvážit, zda je na základě analýzy provedené v souladu s doporučením A zapotřebí přijmout nějaká opatření, včetně změn příslušných právních předpisů Unie, aby se zajistilo, že evropské orgány dohledu mohou prostřednictvím společného výboru a společně s ECB, ESRB a příslušnými vnitrostátními orgány vytvořit EU-SCICF v souladu s dílčím doporučením A.1 a aby se zajistilo, že se evropské orgány dohledu, ECB, ESRB a příslušné vnitrostátní orgány, jakož i další orgány mohou zapojit do koordinačních opatření a vyměňovat si informace, které jsou dostatečně podrobné a konzistentní na podporu účinného nástroje EU-SCICF.