C/2026/3795

16.7.2026

VAROVÁNÍ EVROPSKÉ RADY PRO SYSTÉMOVÁ RIZIKA

ze dne 25. června 2026

o systémových kybernetických rizicích vyplývajících z hraničních modelů umělé inteligence

(ESRB/2026/3)

(C/2026/3795)

GENERÁLNÍ RADA EVROPSKÉ RADY PRO SYSTÉMOVÁ RIZIKA,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na Dohodu o Evropském hospodářském prostoru ([1]), a zejména na přílohu IX této 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. c) 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 a 19 uvedeného rozhodnutí,

vzhledem k těmto důvodům:

(1) Přední poskytovatelé umělé inteligence (AI) vyvinuli hraniční modely umělé inteligence (FAIM), které jsou velmi pokročilé v oblasti kybernetické bezpečnosti a schopné provádět plně automatizované kybernetické útoky na složité systémy, mimo jiné prostřednictvím odhalování zranitelností a vývoje a útočného využití exploitů, čímž se zásadně mění prostředí kybernetických hrozeb.

(2) Modely FAIM jsou výrazně pokročilejší než dřívější modely AI při hledání způsobů, jak provádět kybernetické útoky, překonávají dřívější modely z hlediska nákladů, rychlosti i přesnosti a konkurují již předním lidským odborníkům.

(3) Modely FAIM jsou schopny ohrozit systémy, na nichž je založeno prostředí informačních a komunikačních technologií (IKT), na kterém je závislá finanční infrastruktura, což zvyšuje pravděpodobnost a závažnost kybernetických incidentů se systémovým dopadem.

(4) Modely FAIM prokázaly schopnost odhalit zranitelnosti a vytvářet nové exploity, čímž vystavují hlavní operační systémy a softwarové produkty používané v prostředí IKT téměř všech organizací riziku kybernetických útoků.

(5) V minulosti byly tyto zranitelnosti jen zřídka odhalovány a často se o jejich odhalení zasloužili výzkumní pracovníci v oblasti bezpečnosti, a byla tak možná cílená náprava. V těchto případech mají poskytovatelé softwaru běžně k dispozici standardizovaný časový rámec – obvykle 90 dnů – na opravu zranitelnosti před jejím zveřejněním. Modely FAIM však pravděpodobně povedou ke zvýšení počtu zjištěných zranitelností.

(6) Stávající postupy provádění softwarových oprav ve finančním systému jsou převážně reaktivní povahy a spoléhají se na pravidelné aktualizace a ad hoc reakce na odhalené zranitelnosti. Tento přístup je funkční v prostředí hrozeb, kde je dostatek času na zvládnutí odhalené zranitelnosti. S nárůstem objemu zranitelností však nemusí stávající postupy postačovat k zachování provozní odolnosti.

(7) Tento nárůst objemu rovněž přetěžuje stávající procesy softwarových oprav, neboť v zájmu zajištění provozní stability tyto procesy upřednostňují nápravná opatření na základě míry rizika a vyžadují, aby softwarové opravy byly před nasazením otestovány. Pokud je v krátkém časovém období odhaleno příliš mnoho zranitelností s kritickým dopadem, a podstatně se tak zvýší počet potřebných kritických softwarových oprav, mohou se finanční instituce ocitnout před volbou, zda zůstanou vystaveny významným kybernetickým rizikům, nebo zda sníží požadavky na testování oprav, a budou tak riskovat provozní incidenty a výpadky.

([1]) Úř. věst. L 1, 3.1.1994, s. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) Úř. věst. L 331, 15.12.2010, s. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) Úř. věst. C 58, 24.2.2011, s. 4.

(8) Tvorba útočných exploitů dříve probíhala převážně manuálně a vyžadovala dny či týdny práce lidských odborníků, zatímco nyní jsou modely FAIM schopny je vytvořit v řádu minut či hodin. Ztrácí se tak časové rezervy na obranu, které jsou nezbytné k zachování kontinuity zásadních a důležitých funkcí během nápravy.

(9) Se šířením útočného využití exploitů kritických zranitelností za pomoci AI a s odpovídajícím poklesem časových rezerv na obranu se prudce zvyšuje riziko pro jednotlivé zásadní nebo důležité funkce a instituce. Pokud by se tato rizika projevila současně ve více takových funkcích a institucích, mohlo by to vést k trvalému nárůstu systémového kybernetického rizika, pro které v současné době neexistuje plně účinný rámec zmírňujících opatření. Vzhledem k silné provázanosti v rámci finančního sektoru Unie, jakož i mezi tímto sektorem a dalšími odvětvími a jurisdikcemi, představuje tato situace systematické riziko a může vést k systémové nestabilitě.

(10) Kromě toho modely FAIM v současné době vyvíjí pouze několik poskytovatelů AI, z nichž někteří vyjádřili obavy, že budoucí modely FAIM mohou být příliš výkonné na to, aby k nim měla veřejnost neomezený přístup.

(11) Nepřátelské subjekty již využívají AI k posílení kybernetických útoků. Je pravděpodobné, že tyto subjekty nakonec získají, ať už prostřednictvím úniků, krádeže, nezávislého vývoje nebo otevřeného přístupu, modely AI, jejichž schopnosti budou srovnatelné s těmi, které jsou v současné době zaváděny v kontrolovaném obranném prostředí.

(12) Modely FAIM mohou sice výrazně zvýšit útočné schopnosti a pravděpodobnost sofistikovaných kybernetických útoků, posílí ale také schopnosti obrany, zejména pokud jde o odhalování zranitelností, korelaci údajů a nápravná opatření ze strany jednotlivých institucí. V krátkodobém až střednědobém horizontu však zvýšení rychlosti, rozsahu a přesnosti útočných schopností pravděpodobně převáží nad přínosy těchto modelů.

(13) Rychlý vývoj modelů FAIM vyžaduje bezodkladné řešení zjištěných rizik pro finanční stabilitu, aby se předešlo jejich naplnění nebo aby se alespoň zmírnil jejich potenciální dopad. V zájmu zajištění finanční stability na finančních trzích Unie by všichni členové Evropské rady pro systémová rizika (ESRB) měli v rámci svých opatření makroobezřetnostní a mikroobezřetnostní politiky zvážit dopady modelů FAIM na provozní schopnost a odolnost finančních institucí. Tím není dotčen mandát centrálních bank v Unii v oblasti měnové politiky. Jako příklad (vedle stávajících iniciativ různých orgánů) ECB v rámci své úlohy orgánu bankovního dohledu požádala významné instituce, aby neprodleně posoudily dopad vyvíjejícího se prostředí hrozeb a do 31. října 2026 vypracovaly komplexní akční plán, v němž uvedou konkrétní opatření zaměřená na řešení těchto rizik ([4]).

(14) Se šířením technologie AI je důležité zajistit, aby veškerá kritická infrastruktura a zejména finanční instituce byly připraveny čelit kybernetickým útokům ze strany modelů FAIM a včas a náležitě se na ně připravovat. Takové obranné kroky ze strany jednotlivých subjektů by však nebyly dostatečné. Účinná reakce a zmírňování rizik vyžaduje koordinovanou odpověď za účasti všech dotčených stran, včetně poskytovatelů AI, poskytovatelů softwaru, bezpečnostních firem, správců „open source“ kódů, finančních institucí a orgánů na vnitrostátní úrovni i na úrovni Unie.

(15) Při řešení výše uvedených problémů je důležité připomenout příslušné právní a politické rámce Unie, zejména nařízení Evropského parlamentu a Rady (EU) 2022/2554 ([5]), nařízení Evropského parlamentu a Rady (EU) 2024/1689 ([6]), nařízení Evropského parlamentu a Rady (EU) 2024/2847 ([7]) a doporučení Evropské rady pro systémová rizika (ESRB/2021/17) ([8]).

([4]) Dopis adresovaný významným institucím je k dispozici na internetových stránkách bankovního dohledu ECB na adrese www.bankingsupervision.europa.eu.

([5]) 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), ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (Úř. věst. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) 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) (Úř. věst. C 134, 25.3.2022, s. 1).

(16) Nařízení (EU) 2022/2554 poskytuje finančním institucím komplexní rámec pro identifikaci, řízení, sledování a zmírňování rizik v oblasti IKT, včetně rizik vyplývajících z kybernetických útoků. Vzhledem k provázanosti finančního sektoru a jeho závislosti na systémech IKT a poskytovatelích služeb z řad třetích stran by úspěšný kybernetický útok postihující jednu nebo více finančních institucí nebo jejich poskytovatele kritických služeb mohl mít významné systémové důsledky. Orgány finančního dohledu by měly náležitě upřednostňovat činnosti dohledu v této oblasti s ohledem na možný dopad těchto kybernetických útoků na stabilitu, integritu a důvěryhodnost finančního systému, jakož i na provozní, finanční a spotřebitelské škody, které z nich mohou vyplynout.

(17) Nařízení (EU) 2024/1689 stanoví harmonizovaná pravidla pro uvádění systémů AI a obecných modelů AI na trh a do provozu a jejich využívání v Unii, a to za určitých okolností včetně systémů a modelů nabízených poskytovateli AI usazenými ve třetích zemích, pokud se výstup vytvořený systémem AI používá v Unii nebo je model AI začleněn do systému uvedeného na trh Unie. Toto nařízení rovněž stanoví zvláštní pravidla, včetně přísnějšího regulačního režimu, pro modely klasifikované jako obecné modely AI se systémovým rizikem.

(18) Nařízení (EU) 2024/2847 zavádí povinné požadavky na kybernetickou bezpečnost pro výrobce, které se vztahují na plánování, návrh, vývoj a údržbu hardwarových a softwarových produktů s digitálními prvky uváděných na trh Unie. Vyžaduje také, aby výrobci řešili zranitelnosti během životního cyklu svých produktů. Jakmile budou tyto požadavky v prosinci 2027 plně použitelné, finanční subjekty uvádějící tyto produkty na trh Unie budou muset rovněž zajistit, aby produkty odpovídaly zmíněným požadavkům.

(19) V doporučení ESRB/2021/17 se doporučuje, aby evropské orgány dohledu společně prostřednictvím společného výboru a ve spolupráci s Evropskou centrální bankou (ECB), ESRB a příslušnými vnitrostátními orgány vytvořily účinnou koordinovanou reakci na úrovni Unie v případě závažného přeshraničního kybernetického bezpečnostního incidentu nebo související hrozby, jež by mohla mít systémový dopad na finanční sektor Unie. Výsledkem bylo vytvoření celoevropského rámce pro koordinaci příslušných orgánů v případě systémových kybernetických bezpečnostních incidentů (EU–SCICF), který poskytuje cennou operativní platformu pro výměnu informací a koordinaci mezi finančními orgány.

(20) Na základě těchto východisek přijímá ESRB varování obecné povahy, které se zabývá významnými riziky pro finanční stabilitu umocněnými vývojem modelů FAIM. Varování zohledňuje analytickou práci v dokumentu ESRB s názvem „Addressing Frontier AI Models with cyber capabilities from a financial stability perspective“, který byl zveřejněn v červnu 2026 ([9]),

PŘIJALA TOTO VAROVÁNÍ:

ODDÍL 1

Varování

Nové rizikové prostředí

Rychlý vývoj hraničních modelů umělé inteligence (FAIM) s kybernetickými schopnostmi s sebou přináší podstatné změny oblasti rizik pro finanční systém Unie. Z aktuálně dostupných zjištění vyplývá, že modely FAIM jsou schopny odhalit zranitelnosti, generovat funkční exploity a autonomně provádět plnohodnotné kybernetické útoky s rychlostí, rozsahem a úrovní přesnosti, které dalece předčí možnosti předchozích modelů AI. To představuje změnu paradigmatu v oblasti kybernetické bezpečnosti a zlomový bod, pokud jde o schopnosti umělé inteligence.

ESRB považuje tento vývoj za zdroj systémových rizik pro finanční systém, který může mít v důsledku rychlejšího odhalování zranitelností, kratší doby na reakci a účinnou obranu, většího rozsahu a propracovanosti kybernetických útoků a vzniku nových závislostí a rizik koncentrace v rámci finančního systému významné nepříznivé dopady na kybernetickou bezpečnost. Ačkoli ESRB uznává posílené obranné schopnosti, které modely FAIM finančním institucím nabídnou, je pravděpodobné, že praktické využití těchto možností bude reálné až v průběhu několika příštích let, a finanční instituce tak budou nuceny projít přechodným obdobím, které se bude vyznačovat zvýšeným rizikem, vysokou nejistotou a rychle se vyvíjejícím technologickým prostředím. Vzhledem k vysoce digitalizované a vzájemně provázané povaze finančního systému by se tyto nepříznivé dopady na kybernetickou bezpečnost mohly rychle šířit a ovlivnit zásadní a důležité funkce napříč finančními institucemi, což by v konečném důsledku vedlo k systémovému narušení a ke ztrátě důvěry ve finanční systém.

([9]) K dispozici na internetových stránkách ESRB na adrese www.esrb.europa.eu.

Nově vznikající modely FAIM zvyšují inherentní riziko v oblasti IKT, což vede k oslabení provozní odolnosti v celém finančním sektoru, a to zejména ve čtyřech oblastech: a) čas, včetně schopnosti rychle opravovat složité systémy, aniž by vznikaly provozní poruchy, s přihlédnutím ke ztrátě časových rezerv na obranu, které jsou k dispozici mezi odhalením zranitelnosti a útočným využitím exploitů, b) způsobilost obránců, včetně jejich schopnosti provádět automatizované bezpečnostní testování s využitím modelů FAIM a manuální bezpečnostní testování, jakož i jejich schopnost ochrany, odhalování a reakce ve vztahu k hrozbám vyplývajícím z nepřátelského využití modelů FAIM, c) koncentrace, včetně závislosti na omezeném počtu poskytovatelů AI, kteří jsou dále závislí na poskytovatelích cloudových služeb, „open source“ komponentech a jiných běžně používaných softwarových produktech, a d) schopnosti orgánů, včetně nastavení očekávání, zátěžového testování a opatření v oblasti připravenosti v souladu s vývojem modelů FAIM tak, aby se provozní poruchy nestávaly zdrojem širší nestability.

Kromě toho není v rámci žádné finanční instituce snadné získat a udržet přehled o nasazení umělé inteligence – včetně plného pochopení toho, kde a jak je AI nasazena – s přihlédnutím k tomu, že se používá v klientských rozhraních, jako součást interních agentů, obchodních procesů a v rámci integrace se třetími stranami.

Systémové posouzení

Zjištěný vývoj může podstatně změnit rozsah i strukturu kybernetických rizik a zvýšit přímá i nepřímá rizika pro finanční stabilitu. Schopnosti modelů FAIM mohou vystavovat stávající rámce odolnosti značnému tlaku, zejména pokud jde o rozsáhlé a souběžné incidenty. Incidenty se navíc mohou rychle šířit napříč finančními institucemi a trhy, pokud jsou dotčeni kritičtí poskytovatelé z řad třetích stran, sdílené technologické ekosystémy nebo ve velkém rozsahu používané „open source“ komponenty, což zvyšuje riziko souvisejících narušení se systémovými důsledky.

Modely FAIM mění tři zdroje asymetrie ve finančním sektoru: zaprvé mezi jurisdikcemi, zadruhé mezi obránci a útočníky a zatřetí mezi lépe a hůře vybavenými finančními institucemi.

Zaprvé, současná zeměpisná koncentrace předních poskytovatelů AI mimo Unii vystavuje Unii strategické závislosti a geopolitickému riziku. Ke zmírnění znalostní a technologické asymetrie mezi jurisdikcemi je třeba přijmout opatření k usnadnění odpovídajícího a přiměřeného přístupu Unie a jejích členských států k nově vytvořeným modelům FAIM. Taková opatření by měla být včasná, soudržná a efektivní, a to jak z hlediska politického nastavení, tak z hlediska jejich provádění, a měla by náležitě zohledňovat různé finanční sektory Unie a využívat odborné znalosti příslušných evropských orgánů dohledu. Tím se zmírní nejen asymetrie mezi Unií a třetími zeměmi, ale také mezi finančními institucemi usazenými v různých členských státech, čímž se zachovají rovné podmínky v rámci Unie i mimo ni a minimalizuje se systémové riziko. Ujednání usnadňující přístup k modelům FAIM pouze pro určité kategorie institucí nebo ve vybraných jurisdikcích by přispěla k roztříštěnosti jednotného finančního trhu a omezila by jeho likviditu a hloubku.

Zadruhé, pokud jde o asymetrii mezi útočníky a obránci, modely FAIM snižují vstupní náklady na straně útočníků. Je pravděpodobné, že aktéři hrozeb se budou při provádění technicky vyspělejších a pracovně náročnějších částí útočných operací stále více spoléhat na modely FAIM, čímž sníží své náklady. Obránci jsou naopak limitováni provozními požadavky, závislostmi a regulačními povinnostmi, což má nepříznivý vliv na účinek a rozsah možného využití modelů FAIM v krátkodobém až střednědobém horizontu, a v konečném důsledku tak budou obránci potřebovat více času na adaptaci.

Zatřetí existují rozdíly ve zdrojích a vybavenosti finančních institucí, pokud jde o řešení výzev spojených s modely FAIM. Tyto rozdíly mohou být způsobeny náklady, které jsou svou povahou fixní, a nikoli závislé na rozsahu, dále omezenými zdroji a omezeným přístupem ke specialistům. Existuje-li asymetrie ve schopnosti vypořádat se s těmito výzvami, může nejslabší článek řetězce ovlivnit stabilitu celého systému.

Důsledky

Je zcela nezbytné zajistit, aby systémově významné platební a vypořádací systémy a infrastruktury finančních trhů byly i nadále chráněny vůči zranitelnostem vyplývajícím z využívání a vývoje modelů FAIM. Veřejní i soukromí provozovatelé by měli důkladně přezkoumat a aktualizovat své rámce kybernetické bezpečnosti tak, aby braly na tyto zranitelnosti ohled. Orgány pověřené dohledem nebo dozorem by měly přijmout opatření k zajištění odpovídající ochrany systémů. Veřejné orgány a soukromé finanční instituce by měly navzájem spolupracovat, kdykoli je to nezbytné ke zvýšení bezpečnosti a odolnosti finančního systému Unie.

Ve své zprávě o systémových kybernetických rizicích ([10]) z roku 2020 ESRB označila rychlost a rozsah kybernetických hrozeb a zlovolný záměr stojící za jejich využíváním za možné zdroje šíření systémového rizika. Dotyčné orgány by si měly být vědomy toho, že i když modely FAIM představují nový zdroj šíření systémového rizika, zároveň umocňují již dříve identifikované zdroje, a měly by tento poznatek začlenit do svých politických opatření. Vzhledem ke všem rizikům pro finanční stabilitu vyplývajícím z provozní expozice vůči kybernetickému riziku ve finančním sektoru je důležité zajistit, aby se problematické aspekty popsané v tomto varování odrážely v činnostech uskutečňovaných v oblasti dohledu a dozoru a v politických postojích přijatých příslušnými orgány v rámci jejich mandátu.

Relevantní orgány by si měly být v rámci svých pravomocí a konkrétně v rámci stanoveném nařízením (EU) 2022/2554 vědomy třech výše uvedených zdrojů asymetrie, jež způsobují modely FAIM ve finančním sektoru. Ve snaze tyto asymetrie omezit je třeba vedle stávajících testovacích rámců zvážit ujednání o spolupráci a také koordinaci v rámci daných odvětví ([11]). Finanční orgány by měly rovněž zajistit, aby se správní rady soukromých finančních institucí plně zavázaly ke zmírňování kybernetických rizik vyvolaných modely FAIM, aby byly zavedeny jasné rámce správy a odpovědnosti a aby byly náležitě naplánovány včasné reakce spolu s odpovídajícími interními investicemi.

Několik možných aspektů zvažovaných v tomto varování – ať už jde o systémový dopad, geopolitické riziko, nebo změnu rovnováhy mezi útočníky a obránci – může mít dopad na fungování finančního systému a důvěru v něj. Za účelem jejich průběžného hodnocení zváží ESRB nutnost zohlednit tyto aspekty při posuzování rizik, v testovacích rámcích a také v rámci očekávání v oblasti dohledu, jakož i při sestavování budoucích scénářů. ESRB bude rovněž sledovat používání a vývoj modelů FAIM a jejich dopad na finanční sektor z hlediska systémového rizika. Kromě toho ESRB znovu posoudí vývoj v rámci každého čtvrtletního hodnocení rizik na úrovni generální rady a v případě potřeby zváží další opatření.

ODDÍL 2

Definice

Pro účely tohoto varování se použijí tyto definice:

1) „poskytovatelem AI“ se rozumí poskytovatel ve smyslu čl. 3 bodu 3 nařízení (EU) 2024/1689;

2) „hraničními modely AI (FAIM)“ se rozumí pokročilé obecné modely AI schopné podstatně ovlivnit útočné nebo obranné kybernetické operace;

3) „kybernetickým útokem“ se rozumí kybernetický útok ve smyslu článku 1 nařízení Rady (EU) 2019/796 ([12]), a to i tehdy, má-li původ v Unii;

4) „zranitelností“ se rozumí zranitelnost smyslu čl. 3 bodu 16 nařízení (EU) 2022/2554;

5) „exploitem“ se rozumí nástroj, technika nebo metoda, které se používají k využití jedné nebo více zranitelností a získání neoprávněného přístupu do systémů, jejich změně nebo narušení nebo jinému vyvolání rizika v oblasti IKT nebo incidentů souvisejících s IKT;

6) „útočným využitím“ se rozumí příprava nebo úprava exploitů umožňující systematické nebo škálovatelné využívání zranitelností;

7) „zásadní nebo důležitou funkcí“ se rozumí zásadní nebo důležitá funkce ve smyslu čl. 3 bodu 22 nařízení (EU) 2022/2554;

8) „obecným modelem AI“ se rozumí model AI ve smyslu čl. 3 bodu 63 nařízení (EU) 2024/1689;

9) „obecným modelem AI se systémovým rizikem“ se rozumí obecný model AI klasifikovaný jako model představující systémové riziko v souladu s čl. 51 odst. 1 nařízení (EU) 2024/1689;

10) „incidentem souvisejícím s IKT“ se rozumí incident ve smyslu čl. 3 bodu 8 nařízení (EU) 2022/2554;

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

([11]) Např. etické testování metodou červeného týmu založené na zpravodajství o hrozbách (TIBER), penetrační testování na základě hrozeb (TLPT), pokročilé testování metodou červeného týmu (ART) a zátěžové testování kybernetické odolnosti (CyRST).

([12]) Nařízení Rady (EU) 2019/796 ze dne 17. května 2019, o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) „rizikem v oblasti IKT“ se rozumí riziko ve smyslu čl. 3 bodu 5 nařízení (EU) 2022/2554;

12) „provozní odolností“ se rozumí digitální provozní odolnost ve smyslu čl. 3 bodu 1 nařízení (EU) 2022/2554.

Ve Frankfurtu nad Mohanem dne 25. června 2026.

Vedoucí sekretariátu ESRB,
jménem generální rady ESRB,
Francesco MAZZAFERRO