Úradný vestník
Európskej únie

SK
Séria C

C/2026/3795

16.7.2026

VAROVANIE EURÓPSKEHO VÝBORU PRE SYSTÉMOVÉ RIZIKÁ

z 25. júna 2026

o systémových kybernetických rizikách vyplývajúcich z pokročilých modelov umelej inteligencie

(ESRB/2026/3)

(C/2026/3795)

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. c) 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 a 19,

keďže:

(1) Poprední poskytovatelia umelej inteligencie vyvinuli pokročilé modely umelej inteligencie, ktoré veľmi dobre fungujú v oblasti kybernetickej bezpečnosti a dokážu vykonávať plne automatizované kybernetické útoky na komplexné systémy, a to aj prostredníctvom odhaľovania zraniteľností a vývoja exploitov a ich premeny na zbraň, čím sa zásadne mení prostredie kybernetických hrozieb.

(2) Pokročilé modely umelej inteligencie sú pri hľadaní spôsobov vykonávania kybernetických útokov výrazne lepšie ako predchádzajúce modely umelej inteligencie a zároveň prekonávajú predchádzajúce modely z hľadiska nákladov, rýchlosti a presnosti a v súčasnosti konkurujú popredným odborníkom.

(3) Pokročilé modely umelej inteligencie sú schopné ohroziť systémy, na ktorých sú založené prostredia informačných a komunikačných technológií (IKT), ktoré sú nevyhnutné pre fungovanie finančnej infraštruktúry, čím sa zvyšuje pravdepodobnosť a závažnosť kybernetických incidentov so systémovým vplyvom.

(4) Pokročilé modely umelej inteligencie preukázali schopnosť odhaľovať zraniteľnosti a vytvárať nové exploity, čím vystavujú významné operačné systémy a softvéry používané v prostrediach IKT takmer všetkých organizácií riziku kybernetických útokov.

(5) V minulosti bolo odhalenie takýchto zraniteľností zriedkavé a častokrát ich odhalili výskumní pracovníci v oblasti bezpečnosti, čo umožnilo cielenú nápravu. V takýchto prípadoch majú poskytovatelia softvéru bežne k dispozícii štandardizovaný časový rámec – zvyčajne 90 dní – na opravu zraniteľnosti pred jej zverejnením. Pokročilé modely umelej inteligencie však pravdepodobne zvýšia objem zistených zraniteľností.

(6) Súčasné postupy týkajúce sa opráv softvéru vo finančnom systéme sú prevažne reaktívne a spoliehajú sa na pravidelné aktualizácie a ad hoc reakcie na odhalené zraniteľnosti. Tento prístup funguje v prostredí hrozieb, kde je vzhľadom na dostatok času odhalenie zraniteľnosti ešte zvládnuteľné. Vzhľadom na nárast objemu zraniteľností však súčasné postupy nemusia stačiť na zachovanie prevádzkovej odolnosti.

(7) Vzhľadom na toto zvýšenie objemu sú preťažené aj súčasné procesy opráv, keďže s cieľom zabezpečiť prevádzkovú stabilitu tieto procesy uprednostňujú nápravné opatrenia na základe miery rizika a vyžadujú, aby sa pred zavedením uskutočnilo testovanie opráv softvéru. Ak sa v krátkom časovom období zistí príliš veľa zraniteľností s kritickým vplyvom a podstatne sa zvýši počet potrebných kritických opráv softvéru, môžu byť finančné inštitúcie nútené sa rozhodnúť, či sa vystavia významným kybernetickým rizikám alebo znížia požiadavky na testovanie opráv a budú tak riskovať, že dôjde k prevádzkovým incidentom a výpadkom.

([1]) Ú. v. ES L 1, 3.1.1994, s. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) Ú. v. E=U L 331, 15.12.2010, s. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) Ú. v. EÚ C 58, 24.2.2011, s. 4.

(8) Premena na zbraň sa v minulosti vykonávala prevažne manuálne a odborníkom trvala niekoľko dní alebo týždňov, zatiaľ čo teraz ju môžu vykonávať pokročilé modely umelej inteligencie v priebehu niekoľkých minút alebo hodín. Strácajú sa tak časové rezervy na obranu, ktoré sú potrebné na zachovanie kontinuity kritických a dôležitých funkcií počas nápravy.

(9) Spolu s nárastom exploitov kritických zraniteľností a ich premeny na zbraň s pomocou umelej inteligencie a zodpovedajúcim skrátením časových rezerv na obranu sa prudko zvyšuje riziko pre jednotlivé kritické alebo dôležité funkcie a inštitúcie. Ak by sa takéto riziká prejavili súčasne pri viacerých týchto funkciách a inštitúciách, mohlo by to viesť k trvalému zvýšeniu systémového kybernetického rizika, pre ktoré v súčasnosti nie je k dispozícii plne účinný rámec na jeho zmiernenie. Vzhľadom na silnú prepojenosť v rámci finančného sektora Únie, ako aj medzi týmto sektorom a inými sektormi a jurisdikciami, predstavuje táto situácia systematické riziko a má potenciál viesť k systémovej nestabilite.

(10) Okrem toho pokročilé modely umelej inteligencie v súčasnosti vyvíja len niekoľko poskytovateľov umelej inteligencie, z ktorých viacerí vyjadrili obavy, že budúce pokročilé modely umelej inteligencie môžu byť príliš výkonné na to, aby k nim mala verejnosť neobmedzený prístup.

(11) Subjekty s nekalými úmyslami už využívajú umelú inteligenciu na posilnenie kybernetických útokov. Je pravdepodobné, že takéto subjekty napokon získajú, či už prostredníctvom únikov, krádeže, nezávislého vývoja alebo otvoreného prístupu, modely umelej inteligencie so spôsobilosťami porovnateľnými s tými, ktoré sú v súčasnosti používané v kontrolovaných obranných prostrediach.

(12) Hoci pokročilé modely umelej inteligencie môžu výrazne zvýšiť útočné spôsobilosti a pravdepodobnosť sofistikovaných kybernetických útokov, posilnia aj obranné spôsobilosti jednotlivých inštitúcií, najmä pokiaľ ide o odhaľovanie zraniteľností, koreláciu údajov a nápravné opatrenia. V krátkodobom až strednodobom horizonte však zvýšenie rýchlosti, rozsahu a presnosti útočných spôsobilostí pravdepodobne preváži nad prínosmi týchto modelov.

(13) Vzhľadom na rýchly vývoj pokročilých modelov umelej inteligencie je nevyhnutné bezodkladne riešiť zistené riziká pre finančnú stabilitu s cieľom zabrániť ich naplneniu, alebo aspoň zmierniť ich potenciálny vplyv. S cieľom zabezpečiť finančnú stabilitu na finančných trhoch Únie by všetci členovia Európskeho výboru pre systémové riziká (ESRB) mali vo svojich opatreniach makroprudenciálnej a mikroprudenciálnej politiky zohľadniť dôsledky pokročilých modelov umelej inteligencie na prevádzkovú spôsobilosť a odolnosť finančných inštitúcií. Týmto nie sú dotknuté mandáty centrálnych bánk v Únii v oblasti menovej politiky. Ako príklad (okrem iných súčasných iniciatív rôznych orgánov) ECB v rámci svojej úlohy ako orgánu bankového dohľadu požiadala významné inštitúcie, aby bezodkladne posúdili vplyv vyvíjajúceho sa prostredia hrozieb a aby do 31. októbra 2026 vypracovali komplexný akčný plán, v ktorom uvedú konkrétne opatrenia zamerané na riešenie takýchto rizík ([4]).

(14) Keďže technológia umelej inteligencie je na vzostupe, je dôležité zabezpečiť, aby bola všetka kritická infraštruktúra, a zvlášť finančné inštitúcie, pripravené čeliť kybernetickým útokom riadeným pokročilými modelmi umelej inteligencie a uskutočnili včasné a primerané prípravy. Takéto obranné úsilie jednotlivých subjektov by však nebolo dostatočné. Na účinnú reakciu a zmierňovanie rizika je potrebná koordinovaná reakcia všetkých dotknutých osôb vrátane poskytovateľov umelej inteligencie, poskytovateľov softvéru, bezpečnostných spoločností, správcov otvorených zdrojových kódov, finančných inštitúcií a vnútroštátnych orgánov a orgánov Únie.

(15) Pri riešení uvedených otázok je dôležité pripomenúť príslušný právny a politický rámec Únie, najmä nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 ([5]), nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 ([6]), nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 ([7]) a odporúčanie Európskeho výboru pre systémové riziká (ESRB/2021/17) ([8]).

([4]) List pre významné inštitúcie je dostupný na webovom sídle bankového dohľadu ECB na www.bankingsupervision.europa.eu.

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

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Odporúčanie Európskeho výboru pre systémové riziká z 2. decembra 2021 o celoeurópskom rámci koordinácie systémových kybernetických incidentov pre príslušné orgány (ESRB/2021/17) (Ú v. EÚ C 134, 25.3.2022, s. 1).

(16) Nariadenie (EÚ) 2022/2554 poskytuje finančným inštitúciám komplexný rámec na identifikáciu, riadenie, monitorovanie a zmierňovanie IKT rizík vrátane rizík vyplývajúcich z kybernetických útokov. Vzhľadom na vzájomnú prepojenosť finančného sektora a jeho závislosť od systémov IKT a externých poskytovateľov služieb by úspešný kybernetický útok na jednu alebo viacero finančných inštitúcií alebo ich poskytovateľov kritických služieb mohol mať významné systémové dôsledky. Orgány finančného dohľadu by mali činnostiam dohľadu v tejto oblasti pripisovať náležitú prioritu so zreteľom na potenciálny vplyv takýchto kybernetických útokov na stabilitu, integritu a dôveryhodnosť finančného systému, ako aj na možné z toho vyplývajúce prevádzkové a finančné škody a škody spôsobené spotrebiteľom.

(17) V nariadení (EÚ) 2024/1689 sa stanovujú harmonizované pravidlá, pokiaľ ide o uvádzanie na trh, uvádzanie do prevádzky a používanie systémov umelej inteligencie a modelov umelej inteligencie na všeobecné účely v Únii vrátane, za určitých okolností, systémov a modelov poskytovaných poskytovateľmi umelej inteligencie so sídlom v tretích krajinách, ak sa výstup vytvorený systémom umelej inteligencie používa v Únii alebo ak je model umelej inteligencie integrovaný do systému uvedeného na trh Únie. V uvedenom nariadení sa stanovujú aj osobitné pravidlá vrátane prísnejšieho regulačného režimu pre modely klasifikované ako modely umelej inteligencie na všeobecné účely so systémovým rizikom.

(18) Nariadením (EÚ) 2024/2847 sa zavádzajú povinné požiadavky kybernetickej bezpečnosti pre výrobcov, ktoré sa vzťahujú na plánovanie, návrh, vývoj a údržbu hardvérových a softvérových produktov s digitálnymi prvkami uvádzaných na trh Únie. Takisto stanovuje povinnosť výrobcov riešiť zraniteľnosti počas životného cyklu ich produktov. Keď sa začne uvedené nariadenie v decembri 2027 plne uplatňovať, budú musieť finančné subjekty uvádzajúce takéto produkty na trh Únie takisto zabezpečiť, aby tieto produkty spĺňali uvedené požiadavky.

(19) V odporúčaní ESRB/2021/17 sa odporúča, aby európske orgány dohľadu vytvorili kolektívne prostredníctvom spoločného výboru a spolu s Európskou centrálnou bankou, ESRB a príslušnými vnútroštátnymi orgánmi účinnú koordinovanú reakciu na úrovni Únie v prípade závažného cezhraničného kybernetického incidentu alebo súvisiacej hrozby, ktorá by mohla mať systémový vplyv na finančný sektor Únie. Výsledkom bolo vytvorenie celoeurópskeho rámca koordinácie systémových kybernetických incidentov (pan-European Systemic Cyber Incident Coordination Framework – EU-SCICF), ktorý predstavuje cennú prevádzkovú platformu na výmenu informácií a koordináciu medzi finančnými orgánmi.

(20) ESRB na základe uvedených východísk týmto prijíma varovanie všeobecnej povahy, ktoré sa zaoberá významnými rizikami pre finančnú stabilitu umocnenými vývojom pokročilých modelov umelej inteligencie. Toto varovanie zohľadňuje analytickú prácu v dokumente ESRB s názvom *Addressing Frontier AI Models with Cyber capabilities from the financial stability perspective* uverejnenom v júni 2026 ([9]).

PRIJALA TOTO VAROVANIE:

ODDIEL 1

Varovanie

Nové rizikové prostredie

Rýchly vývoj pokročilých modelov umelej inteligencie s kybernetickými spôsobilosťami prináša pre finančný systém Únie významné zmeny rizikového prostredia. Podľa najnovších zistení sú pokročilé modely umelej inteligencie schopné odhaľovať zraniteľnosti, vytvárať funkčné exploity a autonómne vykonávať rozsiahle kybernetické útoky rýchlosťou, rozsahom a úrovňou presnosti, ktoré ďaleko presahujú predchádzajúce modely umelej inteligencie. To predstavuje zmenu paradigmy v oblasti kybernetickej bezpečnosti a bod zlomu, pokiaľ ide o spôsobilosť umelej inteligencie.

ESRB považuje tento vývoj za zdroj systémových rizík pre finančný systém s potenciálom spôsobiť významné nepriaznivé účinky pre kybernetickú bezpečnosť vzhľadom na zrýchlené odhaľovanie zraniteľností, skrátenie času, ktorý je k dispozícii na reakciu a účinnú obranu, zvýšený rozsah a sofistikovanosť kybernetických útokov a vznik nových závislostí a rizík koncentrácie v rámci finančného systému. Hoci ESRB uznáva posilnené obranné spôsobilosti, ktoré pokročilé modely umelej inteligencie ponúknu finančným inštitúciám, je pravdepodobné, že tieto spôsobilosti sa v nasledujúcich rokoch prejavia postupne, čo si bude vyžadovať, aby finančné inštitúcie fungovali počas prechodného obdobia so zvýšeným rizikom, vysokou neistotou a rýchlo sa vyvíjajúcim technologickým prostredím. Vzhľadom na rozsiahlu digitalizáciu a prepojenosť finančného systému by sa takéto nepriaznivé účinky na kybernetickú bezpečnosť mohli rýchlo šíriť, čo by ovplyvnilo kritické a dôležité funkcie vo všetkých finančných inštitúciách a v konečnom dôsledku by viedlo k systémovému narušeniu a strate dôvery vo finančný systém.

([9]) Dostupné na webovom sídle ECB na www.ecb.europa.eu.

Vznikajúce pokročilé modely umelej inteligencie zvyšujú inherentné IKT riziko, čo vedie k oslabeniu prevádzkovej odolnosti v celom finančnom sektore najmä v týchto štyroch oblastiach: a) čas, vrátane schopnosti rýchlo opraviť komplexné systémy bez toho, aby to spôsobilo prevádzkové zlyhanie, aj vzhľadom na stratu časových rezerv na obranu medzi zistením zraniteľnosti a premenou exploitov na zbraň; b) spôsobilosť obrancov, vrátane ich schopnosti vykonávať automatizované a manuálne testovanie bezpečnosti s pomocou pokročilých modelov umelej inteligencie, ako aj ich schopnosť chrániť a odhaľovať hrozby vyplývajúce z nepriateľského používania pokročilých modelov umelej inteligencie a reagovať na ne; c) koncentrácia, vrátane závislosti od obmedzeného počtu poskytovateľov umelej inteligencie, ktorí zasa závisia od poskytovateľov cloudových služieb, komponentov s otvoreným zdrojovým kódom a iných široko používaných softvérov; a d) spôsobilosť orgánov, vrátane kalibrácie očakávaní, stresového testovania a opatrení pripravenosti v súlade s vývojom pokročilých modelov umelej inteligencie, aby sa prevádzkové zlyhania nestali zdrojom širšej nestability.

Okrem toho je náročné získať a udržať prehľad o zavádzaní umelej inteligencie v akejkoľvek finančnej inštitúcii – vrátane úplného pochopenia toho, kde a ako sa umelá inteligencia zavádza – vzhľadom na to, že sa používa v zákazníckych rozhraniach, ako súčasť interných agentov, obchodných procesoch a v rámci integrácie s tretími osobami.

Systémové hodnotenie

Zistený vývoj môže podstatne zmeniť rozsah aj štruktúru kybernetického rizika, čím sa zvýšia priame aj nepriame riziká pre finančnú stabilitu. Spôsobilosti pokročilých modelov umelej inteligencie môžu vyvíjať značný tlak na existujúce rámce odolnosti, najmä ak sú incidenty rozšírené a vyskytnú sa viaceré súčasne. Incidenty sa tiež môžu medzi finančnými inštitúciami a trhmi rýchlo šíriť, ak sú nimi dotknutí kritickí externí poskytovatelia, spoločné technologické ekosystémy alebo vo veľkom rozsahu používané komponenty s otvoreným zdrojovým kódom, čím sa zvyšuje riziko súvisiacich narušení so systémovými dôsledkami.

Pokročilé modely umelej inteligencie menia tri zdroje asymetrie vo finančnom sektore: prvý medzi jurisdikciami, druhý medzi obrancami a útočníkmi a tretí medzi lepšie a horšie vybavenými finančnými inštitúciami.

Po prvé spôsobuje súčasná geografická koncentrácia popredných poskytovateľov umelej inteligencie mimo Únie, že Únia je vystavená strategickej závislosti a geopolitickému riziku. S cieľom zmierniť vedomostnú a technologickú asymetriu medzi jurisdikciami je potrebné prijať opatrenia na uľahčenie primeraného a proporcionálneho prístupu Únie a jej členských štátov k novovyvinutým pokročilým modelom umelej inteligencie. Takéto opatrenia by mali byť včasné, koherentné a účinné, a to tak z hľadiska politického nastavenia, ako aj z hľadiska ich vykonávania, a mali by primerane zohľadňovať rôzne finančné sektory Únie a využívať odborné znalosti príslušných európskych orgánov dohľadu. Tým sa zmierni nielen asymetria medzi Úniou a tretími krajinami, ale aj medzi finančnými inštitúciami so sídlom v rôznych členských štátoch, zachovajú sa rovnaké podmienky v rámci Únie aj mimo nej a minimalizuje sa systémové riziko. Opatrenia uľahčujúce prístup k pokročilým modelom umelej inteligencie len pre určité kategórie inštitúcií alebo vo vybraných jurisdikciách by prispeli k fragmentácii jednotného trhu s financiami, čím by sa znížila jeho likvidita a hĺbka.

Po druhé pokiaľ ide o asymetriu medzi útočníkmi a obrancami, pokročilé modely umelej inteligencie znižujú vstupné náklady útočníkov. Aktéri hrozieb sa pri vykonávaní technicky vyspelejších a pracovne náročnejších častí útočných operácií budú pravdepodobne čoraz viac spoliehať na pokročilé modely umelej inteligencie, čím sa im znížia náklady. Obrancovia sú naopak obmedzení prevádzkovými požiadavkami, závislosťami a regulačnými povinnosťami, ktoré obmedzujú účinok a rozsah, v akom môžu využívať pokročilé modely umelej inteligencie v krátkodobom až strednodobom horizonte, čo si v konečnom dôsledku vyžaduje dlhšie obdobia na prispôsobenie.

Po tretie existujú rozdiely v tom, aké majú finančné inštitúcie zdroje a vybavenie na riešenie výziev, ktoré predstavujú pokročilé modely umelej inteligencie. Tieto rozdiely môžu byť spôsobené nákladmi, ktoré sú svojou povahou fixné a nie závislé od veľkosti inštitúcií, obmedzenými zdrojmi a obmedzeným prístupom k odborníkom. Ak existuje asymetria v schopnosti vyrovnať sa s takýmito výzvami, najslabší článok reťazca môže ovplyvniť stabilitu celého systému.

Dôsledky

Je nevyhnutné zabezpečiť, aby systémovo dôležité platobné systémy a systémy vyrovnania a infraštruktúry finančného trhu boli aj naďalej chránené pred zraniteľnosťami vyplývajúcimi z používania a vývoja pokročilých modelov umelej inteligencie. Verejní a súkromní prevádzkovatelia by mali dôkladne preskúmať a aktualizovať svoje rámce kybernetickej bezpečnosti s cieľom zohľadniť takéto zraniteľnosti. Orgány zodpovedné za dohľad by mali prijať opatrenia na zabezpečenie primeranej ochrany systémov. Orgány a súkromné finančné inštitúcie by mali navzájom spolupracovať vždy, keď je to potrebné na zvýšenie bezpečnosti a odolnosti finančného systému Únie.

ESRB vo svojej správe o systémovom kybernetickom riziku z roku 2020 ([10]) identifikoval rýchlosť, rozsah a škodlivý zámer kybernetických hrozieb ako možné zdroje šírenia systémového rizika. Dotknuté orgány by si mali byť vedomé toho, že hoci pokročilé modely umelej inteligencie predstavujú nový zdroj šírenia systémového rizika, posilňujú aj existujúce predtým identifikované zdroje, a mali by tento poznatok začleniť do svojich politických opatrení. Vzhľadom na všetky riziká pre finančnú stabilitu vyplývajúce z operačnej expozície voči kybernetickému riziku vo finančnom sektore je dôležité zabezpečiť, aby sa problematické aspekty identifikované v tomto varovaní zohľadnili v práci v oblasti dohľadu a v politických postojoch prijatých príslušnými orgánmi v rámci ich príslušných mandátov.

Príslušné orgány by si v rámci svojich príslušných právomocí a konkrétne podľa rámca stanoveného nariadením (EÚ) 2022/2554 mali byť vedomé troch uvedených zdrojov asymetrie spôsobených pokročilými modelmi umelej inteligencie vo finančnom sektore. S cieľom znížiť tieto asymetrie by sa popri existujúcich testovacích rámcoch malo zvážiť aj zavedenie dohôd o spolupráci a sektorovej koordinácii ([11]). Finančné orgány by mali takisto zabezpečiť, aby boli správne rady súkromných finančných inštitúcií v plnej miere odhodlané zmierňovať kybernetické riziká vyvolané pokročilými modelmi umelej inteligencie, aby boli zavedené jasné rámce riadenia a zodpovednosti a aby sa primerane plánovali včasné reakcie spolu so zodpovedajúcimi internými investíciami.

Niekoľko možných vývojov zohľadnených v tomto varovaní – či už ide o systémový vplyv, geopolitické riziko alebo zmenenú rovnováhu medzi útočníkmi a obrancami – má potenciál ovplyvniť fungovanie finančného systému a dôveru v tento systém. S cieľom neustále posudzovať tieto vývoje zohľadní ESRB potrebu zaoberať sa nimi pri posudzovaní rizík, v testovacích rámcoch a v rámci očakávaní v oblasti dohľadu, ako aj pri vypracúvaní budúcich scenárov. ESRB bude takisto monitorovať používanie a vývoj pokročilých modelov umelej inteligencie a ich vplyv na finančný sektor z hľadiska systémového rizika. ESRB okrem toho prehodnotí najnovší vývoj v rámci každého štvrťročného posúdenia rizika na úrovni generálnej rady a v prípade potreby zváži ďalšie opatrenia.

ODDIEL 2

Vymedzenie pojmov

Na účely tohto varovania sa uplatňuje toto vymedzenie pojmov:

1. „poskytovateľ AI“ je poskytovateľ, ako je vymedzený v článku 3 bode 3 nariadenia (EÚ) 2024/1689;

2. „pokročilé modely umelej inteligencie“ (Frontier AI Models – FAIM) sú pokročilé modely umelej inteligencie na všeobecné účely, ktoré sú spôsobilé podstatne ovplyvniť útočné alebo obranné kybernetické operácie;

3. „kybernetický útok“ je kybernetický útok, ako je vymedzený v článku 1 nariadenia Rady (EÚ) 2019/796 ([12]), a to aj vtedy, keď má pôvod v Únii;

4. „zraniteľnosť“ je zraniteľnosť, ako je vymedzená v článku 3 bode 16 nariadenia (EÚ) 2022/2554;

5. „exploit“ je nástroj, technika alebo metóda, ktoré sa používajú na využitie jednej alebo viacerých zraniteľností na účely získania neoprávneného prístupu do systémov, ich úpravy alebo narušenia, alebo ktoré inak vedú k vzniku IKT rizika alebo incidentov súvisiacich s IKT;

6. „premena na zbraň“ je príprava alebo prispôsobenie exploitov, ktoré umožňuje systematické alebo škálovateľné zneužívanie zraniteľností;

7. „kritická alebo dôležitá funkcia“ je kritická alebo dôležitá funkcia, ako je vymedzená v článku 3 bode 22 nariadenia (EÚ) 2022/2554;

8. „model AI na všeobecné účely“ je model AI na všeobecné účely, ako je vymedzený v článku 3 bode 63 nariadenia (EÚ) 2024/1689;

9. „model AI na všeobecné účely so systémovým rizikom“ je model AI na všeobecné účely klasifikovaný ako model predstavujúci systémové riziko v súlade s článkom 51 ods. 1 nariadenia (EÚ) 2024/1689;

10. „incident súvisiaci s IKT“ je incident súvisiaci s IKT, ako je vymedzený v článku 3 bode 8 nariadenia (EÚ) 2022/2554;

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

([11]) Napr. etické červené tímy založené na spravodajských informáciách o hrozbách (threat intelligence-based ethical red teaming – TIBER), penetračné testovanie na základe konkrétnej hrozby (threat-led penetration testing – TLPT), pokročilé červené tímy (advanced red teaming – ART) a stresové testovanie kybernetickej odolnosti (cyber resilience stress testing – CyRST).

([12]) 12 Nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. „IKT riziko“ je IKT riziko, ako je vymedzené v článku 3 bode 5 nariadenia (EÚ) č. 2022/2554;

12. „prevádzková odolnosť“ je digitálna prevádzková odolnosť, ako je vymedzená v článku 3 bode 1 nariadenia (EÚ) č. 2022/2554.

Vo Frankfurte nad Mohanom 25. júna 2026

Vedúci sekretariátu ESRB

v mene Generálnej rady ESRB

Francesco MAZZAFERRO