Europos Sąjungos
oficialusis leidinys

LT
C serija

C/2026/3795

2026 7 16

EUROPOS SISTEMINĖS RIZIKOS VALDYBOS ĮSPĖJIMAS

2026 m. birželio 25 d.

dėl sisteminės kibernetinės rizikos, kurią kelia avangardiniai dirbtinio intelekto modeliai

(ESRB/2026/3)

(C/2026/3795)

EUROPOS SISTEMINĖS RIZIKOS VALDYBOS BENDROJI VALDYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į Europos ekonominės erdvės susitarimą ([1]), ypač į jo IX priedą,

atsižvelgdama į 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1092/2010 dėl Europos Sąjungos finansų sistemos makrolygio rizikos ribojimo priežiūros ir Europos sisteminės rizikos valdybos įsteigimo ([2]), ypač į jo 3 straipsnio 2 dalies c punktą ir 16 ir 18 straipsnius,

atsižvelgdama į 2011 m. sausio 20 d. Europos sisteminės rizikos valdybos sprendimą ESRV/2011/1, kuriuo patvirtinamos Europos sisteminės rizikos valdybos darbo tvarkos taisyklės ([3]), ypač į jo 18 ir 19 straipsnius,

kadangi:

(1) pirmaujantys dirbtinio intelekto (DI) tiekėjai sukūrė avangardinius DI modelius (angl. *Frontier AI Models,* FAIM), kurie yra labai pajėgūs kibernetinio saugumo srityje ir gali atlikti visiškai automatizuotus kibernetinius išpuolius prieš sudėtingas sistemas, be kita ko, atrasdami pažeidžiamumą ir kurdami bei suginklindami saugumo spragų išnaudojimo priemones, taip iš esmės pakeisdami kibernetinių grėsmių aplinką;

(2) kalbant apie būdų kibernetiniams išpuoliams vykdyti suradimą, avangardiniai DI modeliai yra žymiai pranašesni už ankstesnius DI modelius, pranoksta juos kainos, spartos ir tikslumo požiūriu ir dabar konkuruoja su didžiausią patirtį turinčiais žmonėmis ekspertais;

(3) avangardiniai DI modeliai gali kelti grėsmę sistemoms, kuriomis grindžiama informacinių ir ryšių technologijų (IRT) aplinka, nuo kurios priklauso finansų infrastruktūra, ir taip padidinti sisteminį poveikį turinčių kibernetinių incidentų tikimybę ir rimtumą;

(4) įrodyta, kad avangardiniai DI modeliai gali nustatyti pažeidžiamumus ir kurti naujas saugumo spragų išnaudojimo priemones, taip sukeldami kibernetinių išpuolių riziką pagrindinėms operacinėms sistemoms ir programinei įrangai, naudojamoms beveik visų organizacijų IRT aplinkoje;

(5) istoriškai tokie pažeidžiamumai buvo nustatomi retai ir juos dažnai aptikdavo saugumo tyrėjai, todėl buvo galima tikslingai ištaisyti trūkumus. Tokiais atvejais programinės įrangos tiekėjams dažnai nustatomas standartinis terminas (paprastai 90 dienų) pažeidžiamumui ištaisyti prieš jį viešai atskleidžiant. Tačiau tikėtina, kad, naudojant avangardinius DI modelius, nustatytų pažeidžiamumų skaičius padidės;

(6) dabartinė pataisų praktika finansų sistemoje daugiausia yra reaktyvi, grindžiama periodiniais atnaujinimais ir *ad hoc* atsaku į atskleistus pažeidžiamumus. Šis metodas taikomas grėsmių aplinkoje, kurioje laikas sudaro sąlygas toliau valdyti pažeidžiamumo nustatymą. Tačiau didėjant pažeidžiamumų skaičiui dabartinė praktika gali tapti nepakankama veiklos atsparumui išlaikyti;

(7) dėl šio padidėjusio pažeidžiamumų skaičiaus dabartiniai pataisų procesai taip pat yra perkrauti, nes juose pirmenybė teikiama rizika grindžiamoms trūkumų ištaisymo priemonėms ir reikalaujama prieš įgyvendinimą išbandyti programinės įrangos pataisas, kad būtų užtikrintas veiklos stabilumas. Jei per trumpą laiką nustatoma per daug kritinį poveikį turinčių pažeidžiamumų ir dėl to labai padidėja reikalingų ypatingos svarbos programinės įrangos pataisų skaičius, finansų įstaigoms gali tekti nuspręsti, ar susidurti su didele kibernetine rizika, ar sumažinti pataisų testavimo reikalavimus ir taip rizikuoti patirti operacinius incidentus bei atjungimus;

([1]) OL L 1, 1994 1 3, p. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) OL L 331, 2010 12 15, p. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) OL C 58, 2011 2 24, p. 4.

(8) suginklintos saugumo spragų išnaudojimo priemonės anksčiau daugiausia buvo kuriamos rankiniu būdu ir tam reikėdavo dienas ar savaites trunkančio žmonių ekspertų darbo, o dabar avangardiniai DI modeliai tai gali padaryti per kelias minutes ar valandas. Tai reiškia, kad prarandami gynybai skirti laiko rezervai, kurių reikia siekiant išlaikyti ypatingos svarbos ir svarbių funkcijų tęstinumą pažeidžiamumų ištaisymo metu;

(9) daugėjant suginklintų saugumo spragų išnaudojimo priemonių, susijusių su DI sukeltu kritiniu pažeidžiamumu, ir atitinkamai trumpinant gynybai skirtus laiko rezervus, smarkiai išauga rizika atskiroms ypatingos svarbos ar svarbioms funkcijoms ir institucijoms. Jei tokia rizika pasireikštų vienu metu visoms toms funkcijoms ir institucijoms, tai galėtų sukelti nuolatinę padidėjusią sisteminę kibernetinę riziką, kuriai šiuo metu nėra visiškai veiksmingos rizikos mažinimo sistemos. Dėl stiprių Sąjungos finansų sektoriaus, taip pat to sektoriaus ir kitų sektorių bei jurisdikcijų tarpusavio sąsajų ši padėtis kelia sistemingą riziką ir gali sukelti sisteminį pažeidžiamumą;

(10) be to, avangardinius DI modelius šiuo metu kuria tik nedidelis skaičius DI tiekėjų, iš kurių keli išreiškė susirūpinimą, kad būsimi avangardiniai DI modeliai gali būti pernelyg galingi, kad visuomenė galėtų naudotis nevaržoma prieiga prie jų;

(11) piktavaliai subjektai jau naudoja DI kibernetiniams išpuoliams sustiprinti. Tikėtina, kad tokie subjektai dėl informacijos nutekėjimo, vagysčių, kurdami savarankiškai ar naudodamiesi atvira prieiga galiausiai įgis DI modelius, kurių pajėgumai bus panašūs į šiuo metu kontroliuojamoje gynybos aplinkoje diegiamus pajėgumus;

(12) nors avangardiniai DI modeliai gali gerokai padidinti puolimo pajėgumus ir sudėtingų kibernetinių išpuolių tikimybę, jie taip pat sustiprins gynybos pajėgumus, visų pirma susijusius su pažeidžiamumo nustatymu, duomenų koreliacija ir atskirų institucijų taisomaisiais veiksmais. Tačiau trumpuoju ir vidutinės trukmės laikotarpiu puolimo pajėgumų spartos, masto ir tikslumo padidėjimas greičiausiai nusvers naudą;

(13) dėl sparčios avangardinių DI modelių raidos būtina nedelsiant pašalinti nustatytą riziką finansiniam stabilumui, kad būtų užkirstas kelias jos atsiradimui arba bent jau sušvelnintas galimas jos poveikis. Siekiant užtikrinti finansinį stabilumą Sąjungos finansų rinkose, visi Europos sisteminės rizikos valdybos (ESRV) nariai, imdamiesi makroprudencinės ir mikroprudencinės politikos veiksmų, turėtų apsvarstyti avangardinių DI modelių poveikį finansų įstaigų veiklos pajėgumui ir atsparumui. Tai nepažeidžia Sąjungos centrinių bankų įgaliojimų pinigų politikos srityje. Pavyzdžiui, ir tai yra viena iš kitų institucijų dabartinių iniciatyvų, ECB, veikiančio kaip bankų priežiūros institucija, prašymu svarbios įstaigos turi nedelsdamos įvertinti kintančios grėsmių padėties poveikį ir iki 2026 m. spalio 31 d. parengti išsamų veiksmų planą, jame numatydamos konkrečias tokiai rizikai pašalinti skirtas priemones ([4]);

(14) plintant DI technologijoms, svarbu užtikrinti, kad visa ypatingos svarbos infrastruktūra, ypač finansų įstaigos, būtų pasirengusios kovoti su avangardinių DI modelių vykdomais kibernetiniais išpuoliais ir būtų laiku ir tinkamai pasirengusios. Tačiau tokių atskirų subjektų apsaugos pastangų nepakaktų. Norint veiksmingai reaguoti ir mažinti riziką, reikia koordinuoto atsako, apimančio visas paveiktas šalis, įskaitant DI tiekėjus, programinės įrangos tiekėjus, saugumo įmones, atvirojo kodo techninės priežiūros darbuotojus, finansų įstaigas ir institucijas tiek nacionaliniu, tiek Sąjungos lygmenimis;

(15) sprendžiant pirmiau nurodytus klausimus svarbu priminti atitinkamas Sąjungos teisines ir politikos sistemas, visų pirma Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 ([5]), Europos Parlamento ir Tarybos reglamentą (ES) 2024/1689 ([6]), Europos Parlamento ir Tarybos reglamentą (ES) 2024/2847 ([7]) ir Europos sisteminės rizikos valdybos rekomendaciją (ESRV/2021/17) ([8]);

([4]) Svarbioms įstaigoms skirtas laiškas yra paskelbtas ECB bankų priežiūros interneto svetainėje www.bankingsupervision.europa.eu.

([5]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (OL L 333, 2022 12 27, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas) (OL L 2024/1689, 2024 7 12, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) 2021 m. gruodžio 2 d. Europos sisteminės rizikos valdybos rekomendacija dėl Europos sisteminių kibernetinių incidentų koordinavimo tarp atitinkamų institucijų sistemos (ESRV/2021/17) (OL C 134, 2022 3 25, p. 1).

(16) Reglamentu (ES) 2022/2554 nustatyta išsami sistema, pagal kurią finansų įstaigos gali nustatyti, valdyti, stebėti ir mažinti IRT riziką, įskaitant riziką, kylančią dėl kibernetinių išpuolių. Atsižvelgiant į finansų sektoriaus tarpusavio sąsajas ir jo priklausomybę nuo IRT sistemų ir paslaugas teikiančių trečiųjų šalių, sėkmingas kibernetinis išpuolis, darantis poveikį vienai ar daugiau finansų įstaigų arba jų ypatingos svarbos paslaugų teikėjams, galėtų sukelti reikšmingų sisteminių pasekmių. Finansų priežiūros institucijos turėtų teikti tinkamą pirmenybę priežiūros veiklai šioje srityje, atsižvelgdamos į galimą tokių kibernetinių išpuolių poveikį finansų sistemos stabilumui, vientisumui ir patikimumui, taip pat į galimą veiklos, finansinę žalą ir žalą vartotojams;

(17) Reglamentu (ES) 2024/1689 nustatomos suderintos taisyklės dėl DI sistemų ir bendrosios paskirties DI modelių pateikimo rinkai, pradėjimo naudoti ir naudojimo Sąjungoje, įskaitant tam tikromis aplinkybėmis sistemas ir modelius, kuriuos tiekia DI tiekėjai, įsisteigę trečiosiose valstybėse, kuriose DI sistemos sugeneruoti išvediniai naudojami Sąjungoje arba DI modelis yra integruotas į Sąjungos rinkai pateiktą sistemą. Šiame reglamente taip pat nustatomos konkrečios taisyklės, įskaitant griežtesnę reguliavimo tvarką, taikomos modeliams, kurie klasifikuojami kaip sisteminės rizikos bendrosios paskirties DI modeliai;

(18) Reglamentu (ES) 2024/2847 gamintojams nustatomi privalomi kibernetinio saugumo reikalavimai, apimantys Sąjungos rinkai pateikiamų aparatinės ir programinės įrangos produktų su skaitmeniniais elementais planavimą, projektavimą, kūrimą ir techninę priežiūrą. Jame taip pat reikalaujama, kad gamintojai šalintų pažeidžiamumus per savo produktų gyvavimo ciklą. Kai 2027 m. gruodžio mėn. reglamentas bus pradėtas visapusiškai taikyti, tokius produktus Sąjungos rinkai pateikiantys finansų sektoriaus subjektai taip pat turės užtikrinti, kad tie produktai atitiktų šiuos reikalavimus;

(19) Rekomendacijoje ESRV/2021/17 rekomenduojama, kad Europos priežiūros institucijos (EPI) drauge per Jungtinį komitetą ir kartu su Europos Centriniu Banku (ECB), ESRV ir atitinkamomis nacionalinėmis institucijomis parengtų veiksmingą koordinuotą Sąjungos lygmens atsaką didelio tarpvalstybinio kibernetinio incidento arba susijusios grėsmės, kuri galėtų turėti sisteminį poveikį Sąjungos finansų sektoriui, atveju. Taip buvo sukurta visos Europos sisteminių kibernetinių incidentų koordinavimo sistema (ES-SCICF), kuri yra vertinga ir veikianti finansų institucijų keitimosi informacija ir veiklos koordinavimo platforma;

(20) atsižvelgdama į tai, ESRV priima bendro pobūdžio įspėjimą dėl didelės rizikos finansiniam stabilumui, kurią didina avangardinių DI modelių plėtra. Įspėjime atsižvelgiama į analitinį darbą, atliktą 2026 m. birželio mėn. paskelbtame ESRV pranešime, kuriame aptariami avangardiniai DI modeliai, turintys kibernetinius pajėgumus, finansinio stabilumo požiūriu ([9]),

PRIĖMĖ ŠĮ ĮSPĖJIMĄ:

1 SKIRSNIS

Įspėjimas

Nauja rizikos aplinka

Spartus avangardinių DI modelių, turinčių kibernetinių pajėgumų, kūrimas iš esmės keičia Sąjungos finansų sistemai kylančią riziką. Iš dabartinių įrodymų matyti, kad avangardiniai DI modeliai gali nustatyti pažeidžiamumus, sukurti veikiančias saugumo spragų išnaudojimo priemones ir savarankiškai vykdyti plataus masto kibernetinius išpuolius tokiu greičiu, mastu ir tikslumu, kuris gerokai viršija ankstesnius DI modelius. Tai yra esminis pokytis kibernetinio saugumo srityje ir DI pajėgumų lūžio taškas.

ESRV mano, kad šie pokyčiai yra sisteminės rizikos finansų sistemai šaltinis ir gali turėti didelį neigiamą poveikį kibernetiniam saugumui dėl spartesnio pažeidžiamumo nustatymo, trumpesnio reagavimo ir veiksmingos gynybos laiko, padidėjusio kibernetinių išpuolių masto ir sudėtingumo, taip pat naujos priklausomybės ir koncentracijos rizikos finansų sistemoje. Nors ESRV pripažįsta sustiprintus gynybinius pajėgumus, kuriuos avangardiniai DI modeliai suteiks finansų įstaigoms, tikėtina, kad šie pajėgumai bus palaipsniui įgyvendinti per artimiausius kelerius metus, todėl finansų įstaigos turės veikti pereinamuoju laikotarpiu, kuriam būdinga padidėjusi rizika, didelis neapibrėžtumas ir sparčiai kintanti technologinė aplinka. Atsižvelgiant į tai, kad finansų sistema yra labai skaitmenizuota ir tarpusavyje susijusi, toks neigiamas poveikis kibernetiniam saugumui galėtų greitai išplisti ir daryti poveikį ypatingos svarbos ir svarbioms funkcijoms visose finansų įstaigose, o tai galiausiai sukeltų sisteminius sutrikimus ir būtų prarastas pasitikėjimas finansų sistema.

([9]) Paskelbta ESRV interneto svetainėje www.esrb.europa.eu.

Dėl atsirandančių avangardinių DI modelių didėja būdinga IRT rizika, todėl visame finansų sektoriuje silpnėja veiklos atsparumas, visų pirma keturiose srityse: a) laiko, įskaitant gebėjimą greitai atlikti sudėtingų sistemų pataisas nenutraukiant veiklos ir atsižvelgiant į prarandamus gynybai skirtus laiko rezervus, kuriais buvo galima naudotis nuo pažeidžiamumo atradimo iki saugumo spragų išnaudojimo priemonių suginklinimo; b) kibernetinio saugumo ekspertų gebėjimų, įskaitant jų gebėjimą atlikti avangardiniu DI modeliu pagrįstą automatizuotą ir rankinį saugumo testavimą, taip pat jų gebėjimą apsaugoti, nustatyti ir reaguoti į grėsmes, kylančias dėl priešiško avangardinio DI modelio naudojimo; c) koncentracijos, įskaitant priklausomybę nuo riboto DI tiekėjų, kurie savo ruožtu priklauso nuo debesijos paslaugų teikėjų, atvirojo šaltinio komponentų ir kitos plačiu mastu naudojamos programinės įrangos, skaičiaus, ir d) institucijų pajėgumo, įskaitant jų suderintus lūkesčius, testavimą nepalankiausiomis sąlygomis ir parengties priemones, atsižvelgiant į avangardinių DI modelių tobulėjimą, kad veiklos nutraukimas netaptų platesnio masto nestabilumo šaltiniu.

Be to, nustatyti ir išlaikyti DI diegimo matomumą bet kurioje finansų įstaigoje, be kita ko, visapusiškai suprasti, kur ir kaip DI diegiamas, yra sudėtinga, atsižvelgiant į tai, kad jis naudojamas klientų sąsajose, vidaus darbuotojų darbe, verslo procesuose ir integracijos su trečiosiomis šalimis veikloje.

Sisteminis vertinimas

Nustatyti pokyčiai gali iš esmės pakeisti kibernetinės rizikos mastą ir struktūrą, padidindami tiek tiesioginę, tiek netiesioginę riziką finansiniam stabilumui. Avangardinio DI modelio pajėgumai gali sukelti didelį spaudimą esamoms atsparumo sistemoms, ypač jei incidentai yra plačiai paplitę ir įvyksta vienu metu. Incidentai taip pat gali sparčiai plisti tarp finansų įstaigų ir rinkų, jei daromas poveikis ypatingos svarbos paslaugas teikiančioms trečiosioms šalims, bendroms technologinėms ekosistemoms arba plačiai naudojamiems atvirojo kodo komponentams, taip padidinant susijusių sutrikimų, sukeliančių sisteminių pasekmių, riziką.

Avangardiniai DI modeliai finansų sektoriuje keičia tris asimetrijos šaltinius: pirmasis – tarp jurisdikcijų, antrasis – tarp kibernetinio saugumo ekspertų ir užpuolikų, ir trečiasis – tarp geriau aprūpintų ir mažiau aprūpintų finansų įstaigų.

Pirma, dėl dabartinės pirmaujančių DI tiekėjų geografinės koncentracijos už Sąjungos ribų Sąjunga patiria strateginę priklausomybę ir geopolitinę riziką. Siekiant sumažinti jurisdikcijų žinių ir technologinę asimetriją, reikia patvirtinti priemones, kuriomis būtų sudarytos palankesnės sąlygos Sąjungai ir jos valstybėms narėms tinkamai ir proporcingai naudotis naujai sukurtais avangardiniais DI modeliais. Tokios priemonės turėtų būti savalaikės, nuoseklios ir veiksmingos tiek politikos, tiek įgyvendinimo požiūriu ir jomis turėtų būti tinkamai atsižvelgiama į skirtingus Sąjungos finansų sektorius, pasinaudojant atitinkamų EPI ekspertinėmis žiniomis. Taip bus sumažinta ne tik Sąjungos ir trečiųjų valstybių jurisdikcijų, bet ir skirtingose valstybėse narėse įsisteigusių finansų įstaigų asimetrija, išsaugant vienodas sąlygas Sąjungoje ir už jos ribų ir kuo labiau sumažinant sisteminę riziką. Susitarimai, kuriais palengvinama prieiga prie avangardinių DI modelių tik tam tikrų kategorijų įstaigoms arba pasirinktose jurisdikcijose, prisidėtų prie bendrosios finansų rinkos susiskaidymo ir sumažintų jos likvidumą bei gylį.

Antra, kalbant apie užpuolikų ir kibernetinio saugumo ekspertų asimetriją, avangardiniai DI modeliai padeda užpuolikams sumažinti neteisėtos prieigos kainą. Tikėtina, kad grėsmę keliantys subjektai vis labiau kliausis avangardiniais DI modeliais, kad galėtų vykdyti techniškai pažangesnes ir daug darbo reikalaujančias puolamųjų operacijų dalis, taip mažindami išlaidas. Kita vertus, kibernetinio saugumo ekspertai yra suvaržyti veiklos reikalavimų, priklausomybės ir reguliavimo įpareigojimų, todėl trumpuoju ir vidutinės trukmės laikotarpiu ribojamas avangardinių DI modelių poveikis ir mastas, kuriuo jie gali pasinaudoti, o tam galiausiai prireikia ilgesnių prisitaikymo laikotarpių.

Trečia, skiriasi tai, kaip finansų įstaigos yra apsirūpinusios ištekliais ir priemonėmis avangardinių DI modelių keliamiems iššūkiams spręsti. Šiuos skirtumus gali lemti pastoviosios, o ne kintamo dydžio išlaidos, išteklių apribojimai ir ribotos galimybės kliautis specialistais. Tais atvejais, kai gebėjimas įveikti tokius iššūkius yra asimetriškas, silpniausia grandinės jungtis gali turėti įtakos sistemos stabilumui.

Pasekmės

Labai svarbu užtikrinti, kad sistemiškai svarbios mokėjimo ir atsiskaitymo sistemos ir finansų rinkos infrastruktūros ir toliau būtų apsaugotos nuo pažeidžiamumo, atsirandančio dėl avangardinių DI modelių naudojimo ir plėtros. Viešieji ir privatieji veiklos vykdytojai turėtų nuodugniai peržiūrėti ir atnaujinti savo kibernetinio saugumo sistemas, kad būtų atsižvelgta į tokį pažeidžiamumą. Už priežiūrą atsakingos institucijos turėtų imtis priemonių, kad būtų užtikrinta tinkama sistemų apsauga. Prireikus valdžios institucijos ir privačios finansų įstaigos turėtų bendradarbiauti, kad padidintų Sąjungos finansų sistemos saugumą ir atsparumą.

2020 m. ataskaitoje dėl sisteminės kibernetinės rizikos ([10]) ESRV nurodė, kad kibernetinių grėsmių sparta, mastas ir piktavališki ketinimai yra galimi sisteminės rizikos plitimo šaltiniai. Valdžios institucijos turėtų žinoti, kad nors avangardiniai DI modeliai yra naujas sklaidos šaltinis, jie taip pat dar labiau sustiprina esamus anksčiau nustatytus šaltinius, ir turėtų įtraukti šią įžvalgą į savo politikos veiksmus. Atsižvelgiant į visą riziką finansiniam stabilumui, kylančią dėl kibernetinės rizikos poveikio veiklai finansų sektoriuje, svarbu užtikrinti, kad šiame įspėjime nustatyti susirūpinimą keliantys klausimai atsispindėtų priežiūros ir kontrolės darbe ir atitinkamų institucijų pagal joms suteiktus įgaliojimus priimtose politikos pozicijose.

Atitinkamos institucijos pagal joms suteiktą kompetenciją ir konkrečiai pagal Reglamentu (ES) 2022/2554 nustatytą sistemą turėtų žinoti apie tris pirmiau minėtus asimetrijos, kurią finansų sektoriuje sukelia avangardiniai DI modeliai, šaltinius. Siekiant sumažinti šią asimetriją, kartu su esamomis testavimo sistemomis reikėtų apsvarstyti bendradarbiavimo susitarimus ir sektorių koordinavimą ([11]). Finansų institucijos taip pat turėtų užtikrinti, kad privačių finansų įstaigų valdybos būtų visapusiškai įsipareigojusios mažinti avangardinių DI modelių keliamą kibernetinę riziką, kad būtų nustatytos aiškios valdymo ir atskaitomybės sistemos ir kad būtų laiku tinkamai planuojami atsakomieji veiksmai kartu su atitinkamomis vidaus investicijomis.

Keletas šiame įspėjime apsvarstytų galimų pokyčių – sisteminis poveikis, geopolitinė rizika arba pasikeitusi užpuolikų ir kibernetinio saugumo ekspertų pusiausvyra – gali turėti įtakos finansų sistemos veikimui ir pasitikėjimui ja. Siekdama nuolat juos vertinti, ESRV apsvarstys poreikį atsižvelgti į tokius pokyčius rizikos vertinimuose, testavimo sistemose ir formuodama priežiūros lūkesčius, taip pat rengiant būsimus scenarijus. ESRV taip pat stebės avangardinių DI modelių naudojimą ir plėtojimą bei jų poveikį finansų sektoriui sisteminės rizikos požiūriu. Be to, ESRV iš naujo įvertins kiekvieno ketvirčio rizikos vertinimo pokyčius bendrosios valdybos lygmeniu ir prireikus apsvarstys galimybę imtis kitų veiksmų.

2 SKIRSNIS

Sąvokų apibrėžtys

Šiame įspėjime vartojamos šios sąvokų apibrėžtys:

1) DI tiekėjas – tiekėjas, kaip apibrėžta Reglamento (ES) Nr. 2024/1689 3 straipsnio 3 punkte;

2) avangardiniai DI modeliai – pažangūs bendrosios paskirties DI modeliai, galintys daryti reikšmingą poveikį puolamosioms arba gynybinėms kibernetinėms operacijoms;

3) kibernetinis išpuolis – kibernetinis išpuolis, kaip apibrėžta Tarybos reglamento (ES) 2019/796 ([12]) 1 straipsnyje, įskaitant atvejus, kai toks išpuolis vykdomas iš Sąjungos teritorijos;

4) pažeidžiamumas – pažeidžiamumas, kaip apibrėžta Reglamento (ES) Nr. 2022/2554 3 straipsnio 16 punkte;

5) saugumo spragų išnaudojimo priemonė – priemonė, būdas arba metodas, kuriuo siekiama pasinaudoti vienu ar keliais pažeidžiamumo apsektais siekiant gauti neteisėtą prieigą prie sistemų, jas pakeisti arba sutrikdyti, arba kitais būdais sukelti IRT riziką arba su IRT susijusius incidentus;

6) suginklinimas – saugumo spragų išnaudojimo priemonių parengimas arba pritaikymas, sudarant sąlygas sistemingai arba kintamu mastu išnaudoti pažeidžiamumus;

7) ypatingos svarbos arba svarbi funkcija – ypatingos svarbos arba svarbi funkcija, kaip apibrėžta Reglamento (ES) Nr. 2022/2554 3 straipsnio 22 punkte;

8) bendrosios paskirties DI modelis – DI modelis, kaip apibrėžta Reglamento (ES) Nr. 2024/1689 3 straipsnio 63 punkte;

9) bendrosios paskirties DI modelis, galintis kelti sisteminę riziką, – bendrosios paskirties DI modelis, kuris klasifikuojamas kaip keliantis sisteminę riziką pagal Reglamento (ES) 2024/1689 51 straipsnio 1 dalį;

10) su IRT susijęs incidentas – incidentas, kaip apibrėžta Reglamento (ES) Nr. 2022/2554 3 straipsnio 8 punkte;

([10]) Žr. ESRV 2020 m. vasario mėn. leidinį „Systemic cyber risk“ (liet. „Sisteminė kibernetinė rizika“), paskelbtą ESRV interneto svetainėje www.esrb.europa.eu.

([11]) Pavyzdžiui, grėsmių žvalgyba grindžiamas etiško įsiveržimo tyrimas (TIBER-EU), grėsme grindžiamas skverbimosi testavimas (TLPT), pažangusis etiško įsiveržimo tyrimas (ART) ir kibernetinio atsparumo testavimas nepalankiausiomis sąlygomis (CyRST).

([12]) 2019 m. gegužės 17 d. Tarybos reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms (OL L 129 I, 2019 5 17, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) IRT rizika – rizika, kaip apibrėžta Reglamento (ES) Nr. 2022/2554 3 straipsnio 5 punkte;

12) veiklos atsparumas – skaitmeninės veiklos atsparumas, kaip apibrėžta Reglamento (ES) Nr. 2022/2554 3 straipsnio 1 punkte.

Priimta Frankfurte prie Maino 2026 m. birželio 25 d.

ESRV bendrosios valdybos vardu

ESRV sekretoriato vadovas

Francesco MAZZAFERRO