Eiropas Savienības
Oficiālais Vēstnesis

LV
C sērija

C/2026/3795

16.7.2026.

EIROPAS SISTĒMISKO RISKU KOLĒĢIJAS BRĪDINĀJUMS

(2026. gada 25. jūnijs)

par sistēmiskiem kiberriskiem, ko rada avangarda mākslīgā intelekta modeļi

(ESRK/2026/3)

(C/2026/3795)

EIROPAS SISTĒMISKO RISKU KOLĒĢIJAS VALDE,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Līgumu par Eiropas Ekonomikas zonu ([1]) un jo īpaši tā IX pielikumu,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1092/2010 (2010. gada 24. novembris) par Eiropas Savienības finanšu sistēmas makrouzraudzību un Eiropas Sistēmisko risku kolēģijas izveidošanu ([2]) un jo īpaši tās 3. panta 2. punkta c) apakšpunktu, kā arī 16. un 18. pantu,

ņemot vērā Eiropas Sistēmisko risku kolēģijas Lēmumu ESRK/2011/1 (2011. gada 20. janvāris), ar ko pieņem Eiropas Sistēmisko risku kolēģijas Reglamentu ([3]), un jo īpaši tā 18. un 19. pantu,

tā kā:

(1) Vadošie mākslīgā intelekta (MI) nodrošinātāji izstrādājuši avangarda MI modeļus (AMIM), kas ir ļoti spējīgi kiberdrošības jomā un spēj veikt pilnībā automatizētus kiberuzbrukumus sarežģītām sistēmām, tostarp atklājot ievainojamības un izstrādājot mūķus, kā arī pielietojot tos uzbrukuma nolūkos, tādējādi būtiski mainot kiberdraudu ainu.

(2) AMIM ir ievērojami labāki nekā agrākie MI modeļi, meklējot veidus kiberuzbrukumu veikšanai un pārspējot agrākos modeļus izmaksu, ātruma un precizitātes ziņā, šobrīd jau konkurējot ar vadošajiem IKT speciālistiem.

(3) AMIM spēj apdraudēt sistēmas, kas ir pamatā informācijas un komunikācijas tehnoloģiju (IKT) videi, uz kuru balstās finanšu infrastruktūra, palielinot tādu kiberincidentu iespējamību un smagumu, kuriem ir sistēmiska ietekme.

(4) AMIM apliecinājuši spēju atklāt ievainojamības un izstrādāt jaunus mūķu veidus, tādējādi pakļaujot kiberuzbrukumu riskam izplatītākās operētājsistēmas un programmatūru, ko izmanto gandrīz visu organizāciju IKT vidēs.

(5) Vēsturiski šādu ievainojamību atklāšana ir bijusi reta, un tās bieži atklājuši drošības pētnieki, ļaujot veikt mērķtiecīgus ievainojamību novēršanas pasākumus. Šādos gadījumos programmatūras nodrošinātājiem bieži vien tiek dots standartizēts termiņš, parasti 90 dienas, lai novērstu ievainojamību pirms tās publiskošanas. Tomēr AMIM, visticamāk, palielinās konstatēto ievainojamību skaitu.

(6) Pašreizējā programmatūras lāpījumu prakse finanšu sistēmā galvenokārt ir reaģējoša, paļaujoties uz periodiskiem atjauninājumiem un *ad hoc* reakciju uz atklātajām ievainojamībām. Šāda pieeja ir efektīva apdraudējumu vidē, kurā reakcijai pieejamais laiks ļauj atklātās ievainojamības pārvaldīt. Tomēr, palielinoties ievainojamību skaitam, pašreizējā prakse var kļūt nepietiekama, lai saglabātu darbības noturību.

(7) Šāds skaita pieaugums arī pakļauj pārslodzei pašreizējos programmatūras lāpījumu procesus, jo tie korektīvo pasākumu prioritāti nosaka, pamatojoties uz risku, un, lai nodrošinātu darbības stabilitāti, pieprasa programmatūras lāpījumu testēšanu pirms to īstenošanas. Ja īsā laikā tiek atklāts pārāk daudz ievainojamību ar kritisku ietekmi, lai būtiski palielinātu vajadzīgo kritisko programmatūras lāpījumu skaitu, finanšu iestādēm var nākties izlemt, vai turpināt būt pakļautām būtiskiem kiberriskiem, vai samazināt lāpījumu testēšanas prasības un tādējādi riskēt ar darbības incidentiem un pārtraukumiem.

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

(8) Mūķu pielietošana uzbrukuma nolūkos iepriekš lielā mērā tika veikta manuāli un tai bija vajadzīgas IKT speciālistu darba dienas vai nedēļas, bet tagad AMIM to var izdarīt dažu minūšu vai stundu laikā. Tas nozīmē to aizsardzībai pieejamā laika rezervju sabrukumu, kas vajadzīgas, lai saglabātu kritiski svarīgo un svarīgo funkciju nepārtrauktību korektīvo pasākumu laikā.

(9) Pieaugot kritiski svarīgām ievainojamībām atbilstošo mūķu pielietošanai uzbrukuma nolūkos ar MI palīdzību un attiecīgi samazinoties aizsardzībai pieejamā laika rezervēm, strauji palielinās risks atsevišķām kritiski svarīgām vai svarīgām funkcijām un iestādēm. Šādiem riskiem īstenojoties vienlaikus vairākās minētajās funkcijās un iestādēs, varētu pastāvīgi palielināt sistēmisko kiberrisku, attiecībā uz kuru pašlaik nav pieejams pilnībā efektīvs riska mazināšanas regulējums. Ņemot vērā ciešās savstarpējās saiknes Savienības finanšu nozarē, kā arī saiknes starp šo nozari un citām nozarēm un jurisdikcijām, šāda situācija rada sistemātisku risku un var radīt sistēmisku nestabilitāti.

(10) Turklāt AMIM pašlaik izstrādā tikai neliels skaits MI nodrošinātāju, no kuriem vairāki pauduši bažas, ka topošie AMIM varētu būt pārāk spēcīgi neierobežotai publiskai piekļuvei.

(11) Ļaunprātīgas personas jau izmanto MI kiberuzbrukumu veicināšanai. Iespējams, ka šādas personas ar laiku, izmantojot noplūdes, zādzības, neatkarīgu izstrādi vai atvērtu piekļuvi, iegūs pieeju MI modeļiem ar spējām, kas ir salīdzināmas ar tām, kuras pašlaik tiek izmantotas kontrolētos aizsardzības apstākļos.

(12) Lai gan AMIM var ievērojami palielināt uzbrukuma spējas un sarežģītu kiberuzbrukumu iespējamību, tie arī stiprinās aizsardzības spējas, jo īpaši attiecībā uz ievainojamību atklāšanu, datu korelāciju un korektīviem pasākumiem, ko veic individuālas iestādes. Tomēr īstermiņā un vidējā termiņā uzbrukuma spēju ātruma, mēroga un precizitātes pieaugums, visticamāk, atsvērs ieguvumus.

(13) AMIM straujā attīstība liek nekavējoties reaģēt uz konstatētajiem riskiem finanšu stabilitātei, lai novērstu to materializēšanos vai vismaz mazinātu to iespējamo ietekmi. Lai nodrošinātu finanšu stabilitāti Savienības finanšu tirgos, visiem Eiropas Sistēmisko risku kolēģijas (ESRK) dalībniekiem būtu jāapsver AMIM ietekme uz finanšu iestāžu darbības spējām un noturību to makroprudenciālās un mikroprudenciālās politikas pasākumu kontekstā. Tas neskar Savienības centrālo banku pilnvaras monetārās politikas jomā. Piemēram, līdztekus citu iestāžu pašreizējām iniciatīvām ECB kā banku uzraudzības iestāde lūgusi nozīmīgās iestādes nekavējoties novērtēt mainīgās apdraudējumu vides ietekmi un līdz 2026. gada 31. oktobrim izstrādāt visaptverošu rīcības plānu, kurā izklāstīti konkrēti pasākumi šādu risku novēršanai ([4]).

(14) Pieaugot MI tehnoloģiju izplatībai, ir svarīgi nodrošināt, ka visa kritiskā infrastruktūra un jo īpaši finanšu iestādes ir gatavas stāties pretī kiberuzbrukumiem, kuros izmanto AMIM, un savlaicīgi un pienācīgi tam sagatavojušās. Tomēr šādi aizsardzības centieni atsevišķu iestāžu līmenī var nebūt pietiekami. Efektīvai reaģēšanai un riska mazināšanai vajadzīga koordinēta reakcija, kurā iesaistītas visas skartās personas, tostarp MI nodrošinātāji, programmatūras nodrošinātāji, drošības uzņēmumi, atklātā pirmkoda uzturētāji, finanšu iestādes un varas iestādes gan nacionālajā, gan Savienības līmenī.

(15) Risinot iepriekš minētos jautājumus, svarīgi atgādināt par attiecīgajiem Savienības tiesiskajiem un politikas regulējumiem, jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 ([5]), Eiropas Parlamenta un Padomes Regulu (ES) 2024/1689 ([6]), Eiropas Parlamenta un Padomes Regulu (ES) 2024/2847 ([7]) un Eiropas Sistēmisko risku kolēģijas ieteikumu (ESRB/2021/17) ([8]).

([4]) Nozīmīgajām iestādēm adresētā vēstule pieejama ECB banku uzraudzībai veltītajā tīmekļa vietnē www.bankingsupervision.europa.eu.

([5]) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (OV L, 2024/1689, 12.7.2024., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) (OV L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Eiropas Sistēmisko risku kolēģijas ieteikums (2021. gada 2. decembris) par sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānismu attiecīgajām iestādēm (ESRK/2021/17) (OV C 134, 25.3.2022., 1. lpp.).

(16) Regula (ES) 2022/2554 nodrošina visaptverošu satvaru finanšu iestādēm, lai identificētu, pārvaldītu, monitorētu un mazinātu IKT riskus, tostarp riskus, kas izriet no kiberuzbrukumiem. Ņemot vērā savstarpējās saiknes finanšu nozarē un tās paļaušanos uz IKT sistēmām un pakalpojumu sniedzējiem, kas ir trešās personas, sekmīgam kiberuzbrukumam, kas skar vienu vai vairākas finanšu iestādes vai to kritiski svarīgo pakalpojumu sniedzējus, varētu būt būtiska sistēmiska ietekme. Finanšu uzraudzības iestādēm būtu jāpiešķir pienācīga prioritāte uzraudzības darbībām šajā jomā, ņemot vērā šādu kiberuzbrukumu iespējamo ietekmi uz finanšu sistēmas stabilitāti, integritāti un uzticamību, kā arī iespējamo darbības un finansiālo kaitējumu, kā arī kaitējumu patērētājiem.

(17) Regula (ES) 2024/1689 nosaka saskaņotus noteikumus MI sistēmu un vispārīga lietojuma MI modeļu laišanai tirgū, nodošanai ekspluatācijā un izmantošanai Savienībā, tostarp noteiktos apstākļos attiecībā uz sistēmām un modeļiem, ko piedāvā MI nodrošinātāji, kuri iedibināti trešās valstīs, ja MI sistēmas darba rezultātu izmanto Savienībā vai MI modelis integrēts sistēmā, kas tiek laista Savienības tirgū. Šajā regulā paredzēti arī īpaši noteikumi, tostarp stingrāks regulatīvais režīms attiecībā uz modeļiem, kas klasificēti kā vispārīga lietojuma MI modeļi ar sistēmisku risku.

(18) Ar Regulu (ES) 2024/2847 ražotājiem tiek ieviestas obligātas kiberdrošības prasības, kas attiecas uz Savienības tirgū laistās aparatūras un programmatūras produktu ar digitāliem elementiem plānošanu, projektēšanu, izstrādi un uzturēšanu. Tajā arī noteikts, ka ražotājiem jānovērš ievainojamības visā savu produktu aprites ciklā. Tiklīdz tā 2027. gada decembrī būs pilnībā piemērojamas, finanšu iestādēm, kas šādus produktus laiž Savienības tirgū, būs arī jānodrošina, ka minētie produkti atbilst šīm prasībām.

(19) Ieteikumā ESRK/2021/17 Eiropas uzraudzības iestādēm (EUI) tika ieteikts ar Apvienotās komitejas palīdzību un kopā ar Eiropas Centrālo banku (ECB), ESRK un attiecīgajām nacionālajām iestādēm izstrādāt efektīvu Savienības līmeņa koordinētu reakciju tāda liela pārrobežu kiberincidenta vai ar to saistīta apdraudējuma gadījumā, kam varētu būt sistēmiska ietekme uz Savienības finanšu nozari. Tā rezultātā tika izveidota Eiropas Sistēmiskā kiberincidentu koordinācijas sistēma (*European Systemic Cyber Incident Coordination Framework*; EU-SCICF), kas nodrošina vērtīgu un operatīvu platformu informācijas apmaiņai un koordinācijai starp finanšu iestādēm.

(20) Ņemot vērā iepriekš minēto, ESRK ar šo pieņem vispārīgu brīdinājumu par būtiskiem finanšu stabilitātes riskiem, ko pastiprina AMIM attīstība. Brīdinājumā ņemts vērā analītiskais darbs, kas izklāstīts ESRK piezīmē "Par ar kiberspējām apveltītiem avangarda MI modeļiem no finanšu stabilitātes perspektīvas" (*Addressing Frontier AI Models with cyber capabilities from a financial stability perspective*), kura publicēta 2026. gada jūnijā ([9]),

IR PIEŅĒMUSI ŠO BRĪDINĀJUMU.

1. IEDAĻA

Brīdinājums

Jauna risku vide

Ar kiberspējām apveltītu avangarda MI modeļu (AMIM) straujā attīstība rada būtiskas izmaiņas Savienības finanšu sistēmas risku vidē. Pašreiz pieejamā informācija liecina, ka AMIM spēj atklāt ievainojamības, radīt pielietojamus mūķus un autonomi veikt pilna mēroga kiberuzbrukumus ar ātrumu, mērogu un precizitātes līmeni, kas ievērojami pārsniedz iepriekšējos MI modeļus. Tas nozīmē paradigmas maiņu kiberdrošības jomā un pagrieziena punktu MI spēju ziņā.

ESRK uzskata, ka šīs norises rada sistēmiskus riskus finanšu sistēmai, kam var būt būtiska negatīva ietekme uz kiberdrošību, paātrinot ievainojamību atklāšanu, saīsinot reaģēšanas un efektīvas aizsardzības laiku, palielinot kiberuzbrukumu mērogu un sarežģītību un ieviešot jaunus atkarības un koncentrācijas riskus finanšu sistēmā. Lai gan ESRK atzīst pastiprinātās aizsardzības spējas, ko AMIM piedāvās finanšu iestādēm, šīs spējas, visticamāk, īstenosies pakāpeniski dažu nākamo gadu laikā, tāpēc finanšu iestādēm būs jādarbojas pārejas periodā, ko raksturo paaugstināts risks, liela nenoteiktība un strauji mainīga tehnoloģiskā vide. Ņemot vērā finanšu sistēmas izteikti digitalizēto un savstarpēji saistīto raksturu, šāda negatīva ietekme uz kiberdrošību varētu strauji izplatīties, ietekmējot kritiski svarīgas un svarīgas funkcijas visās finanšu iestādēs, galu galā izraisot sistēmiskus traucējumus un uzticības finanšu sistēmai zudumu.

([9]) Pieejama ESRK tīmekļa vietnē www.esrb.europa.eu.

Jaunie AMIM palielina raksturīgo IKT risku, tādējādi vājinot darbības noturību visā finanšu nozarē, jo īpaši četrās šādās jomās: a) laiks, tostarp spēja ātri veikt lāpījumus sarežģītās sistēmās, neradot darbības traucējumus un ņemot vērā aizsardzībai pieejamā laika rezervju trūkumu starp ievainojamības atklāšanu un mūķu pielietošanu uzbrukuma nolūkos; b) aizstāvju spējas, tostarp viņu spējas veikt AMIM atbalstītu automatizētu un manuālu drošības testēšanu, kā arī viņu spējas aizsargāt, atklāt un reaģēt uz draudiem, ko rada pretinieku izmantotie AMIM; c) koncentrācija, tostarp atkarība no ierobežota skaita MI nodrošinātāju, kas savukārt ir atkarīgi no mākoņdatošanas nodrošinātājiem, atklātā pirmkoda komponentiem un citas plaši izmantotas programmatūras; un d) varas iestāžu spējas, tostarp to īstenotā gaidu kalibrēšana, stresa testēšana un sagatavotības pasākumi atbilstoši AMIM attīstībai, lai darbības kļūmes nekļūtu par plašākas nestabilitātes avotu.

Turklāt pārredzamības ieviešana un nodrošināšana attiecībā uz MI izmantošanu jebkurā finanšu iestādē, tostarp pilnīga izpratne par to, kur un kā MI tiek izmantots, ir sarežģīta, ņemot vērā, ka MI izmanto klientu saskarnēs, iekšējos aģentos, uzņēmējdarbības procesos un integrācijā ar trešām personām.

Sistēmisks novērtējums

Konstatētās norises var būtiski mainīt gan kiberriska mērogu, gan struktūru, palielinot gan tiešos, gan netiešos riskus finanšu stabilitātei. AMIM spējas var radīt ievērojamu spiedienu uz esošajiem noturības mehānismiem, jo īpaši gadījumos, kuros incidenti ir plaši izplatīti un notiek vienlaikus. Incidenti var arī strauji izplatīties finanšu iestādēs un tirgos, ja tiek skarti kritiski svarīgi trešo personu pakalpojumu sniedzēji, kopīgas tehnoloģiskās ekosistēmas vai plaši izmantoti atklātā pirmkoda komponenti, palielinot saistīto traucējumu ar sistēmisku ietekmi risku.

AMIM maina trīs asimetrijas avotus finanšu nozarē – pirmkārt, jurisdikciju starpā, otrkārt, starp aizstāvjiem un uzbrucējiem un, treškārt, starp finanšu iestādēm ar labākiem resursiem un mazāk nodrošinātām finanšu iestādēm.

Pirmkārt, vadošo MI nodrošinātāju pašreizējā ģeogrāfiskā koncentrācija ārpus Savienības pakļauj Savienību stratēģiskai atkarībai un ģeopolitiskam riskam. Lai mazinātu zināšanu un tehnoloģisko asimetriju jurisdikciju starpā, jāpieņem pasākumi, kas veicinātu Savienības un tās dalībvalstu pienācīgu un samērīgu piekļuvi jaunizstrādātiem AMIM. Šādiem pasākumiem vajadzētu būt savlaicīgiem, saskaņotiem un efektīviem gan politikas, gan īstenošanas ziņā, un tajos būtu pienācīgi jāņem vērā dažādas Savienības finanšu nozares, izmantojot attiecīgo EUI speciālās zināšanas. Tas mazinās ne tikai asimetriju starp Savienības un trešo valstu jurisdikcijām, bet arī starp finanšu iestādēm, kas veic uzņēmējdarbību dažādās dalībvalstīs, saglabājot vienlīdzīgus konkurences apstākļus Savienībā un ārpus tās un līdz minimumam samazinot sistēmisko risku. Pasākumi, kas atvieglo piekļuvi AMIM tikai noteiktām iestāžu kategorijām vai izvēlētās jurisdikcijās, veicinātu vienotā finanšu tirgus sadrumstalotību, samazinot tā likviditāti un dziļumu.

Otrkārt, attiecībā uz asimetriju starp uzbrucējiem un aizstāvjiem AMIM samazina uzbrucējiem nepieciešamo līdzekļu apjomu. Apdraudējuma organizatori, visticamāk, arvien vairāk paļausies uz AMIM tehniski sarežģītāko un darbietilpīgāko uzbrukuma operāciju veikšanai, tādējādi samazinot izmaksas. Savukārt aizstāvjus ierobežo darbības prasības, atkarība no citiem un regulatīvie pienākumi, kas ierobežo efektivitāti un mērogu, kādā viņi var gūt labumu no AMIM īstermiņā līdz vidējā termiņā, un galu galā prasa ilgākus pielāgošanās periodus.

Treškārt, pastāv atšķirības attiecībā uz to, kādi finanšu iestādēm ir resursi un aprīkojums, lai risinātu AMIM radītās problēmas. Šīs atšķirības var radīt fiksētas, nevis mērogotas izmaksas, resursu ierobežojumi un ierobežota piekļuve speciālistiem. Ja spēja risināt šādas problēmas ir asimetriska, ķēdes vājākais posms var ietekmēt sistēmas stabilitāti.

Ietekme

Ir būtiski nodrošināt, ka sistēmiski nozīmīgas maksājumu un norēķinu sistēmas un finanšu tirgus infrastruktūras arī turpmāk ir aizsargātas pret ievainojamībām, ko rada AMIM izmantošana un attīstība. Publiskā un privātā sektora dalībniekiem būtu rūpīgi jāpārskata un jāatjaunina savi kiberdrošības mehānismi, lai ņemtu vērā šādas ievainojamības. Par uzraudzību vai pārraudzību atbildīgajām iestādēm būtu jāpieņem pasākumi, lai nodrošinātu sistēmu pienācīgu aizsardzību. Sadarbība starp varas iestādēm un privātām finanšu iestādēm būtu jāīsteno vienmēr, kad tas nepieciešams, lai palielinātu Savienības finanšu sistēmas drošību un noturību.

ESRK savā 2020. gada ziņojumā par sistēmisko kiberrisku ([10]) norādīja, ka iespējamie sistēmiskā riska izplatīšanās avoti ir kiberdraudu ātrums, mērogs un ļaunprātīgs nodoms. Varas iestādēm būtu jāapzinās, ka, lai gan AMIM ir jauns riska izplatīšanas avots, tie paplašina arī jau pastāvošos un iepriekš apzinātos riska avotus, un varas iestādēm šis ieskats būtu jāintegrē to īstenotajā politikā. Ņemot vērā visus finanšu stabilitātes riskus, kas izriet no operacionālās pakļautības kiberriskam finanšu nozarē, ir svarīgi nodrošināt, ka šajā brīdinājumā konstatētās bažas tiek atspoguļotas uzraudzības un pārraudzības darbā un politikas nostājās, ko attiecīgās iestādes pieņem savu attiecīgo pilnvaru ietvaros.

Attiecīgajām iestādēm savas kompetences ietvaros un jo īpaši saskaņā ar regulējumu, kas izveidots ar Regulu (ES) 2022/2554, jāapzinās trīs iepriekš minētie asimetrijas avoti, ko finanšu nozarē ieviesuši AMIM. Lai mazinātu šīs asimetrijas, līdztekus esošajiem testēšanas mehānismiem būtu jāapsver sadarbības mehānismi un nozaru koordinācija ([11]). Finanšu jomas varas iestādēm būtu arī jānodrošina, ka privāto finanšu iestāžu padomes un valdes ir pilnībā apņēmušās mazināt AMIM radītos kiberriskus, ka ieviesti skaidri pārvaldības un atbildības mehānismi un ka tiek pienācīgi plānota savlaicīga reaģēšana, kā arī atbilstošas iekšējās investīcijas.

Vairākas iespējamās norises, kas ņemtas vērā šajā brīdinājumā, piem., sistēmiskā ietekme, ģeopolitiskais risks vai mainītais līdzsvars starp uzbrucējiem un aizstāvjiem, var ietekmēt finanšu sistēmas darbību un uzticēšanos tai. Lai tos pastāvīgi izvērtētu, ESRK apsvērs vajadzību atspoguļot šādas norises riska novērtējumos, testēšanas sistēmās un uzraudzības gaidās, kā arī turpmāko scenāriju izstrādē. ESRK arī uzraudzīs AMIM izmantošanu un attīstību un to ietekmi uz finanšu nozari no sistēmiskā riska viedokļa. Turklāt ESRK atkārtoti izvērtēs norises katrā ceturkšņa riska novērtējumā ESRK Valdes līmenī un vajadzības gadījumā apsvērs citas darbības.

2. IEDAĻA

Definīcijas

Šajā brīdinājumā piemēro šādas definīcijas:

1. “MI nodrošinātājs” ir nodrošinātājs, kas definēts Regulas (ES) 2024/1689 3. panta 3) punktā;

2. “avangarda MI modeļi (AMIM)” ir moderni vispārīga lietojuma MI modeļi, kas spēj būtiski ietekmēt uzbrukuma vai aizsardzības kiberoperācijas;

3. “kiberuzbrukums” ir kiberuzbrukums, kas definēts Padomes Regulas (ES) 2019/796 ([12]) 1. pantā, t. sk., ja tā izcelsme ir Eiropas Savienībā;

4. “ievainojamība” ir ievainojamība, kas definēta Regulas (ES) 2022/2554 3. panta 16) punktā;

5. “mūķis” ir rīks, paņēmiens vai metode, ko izmanto, lai ar vienas vai vairāku ievainojamību palīdzību iegūtu neatļautu piekļuvi sistēmām, tās pārveidotu vai traucētu to darbību, vai citādi radītu IKT risku vai ar IKT saistītus incidentus;

6. “pielietošana uzbrukuma nolūkos” ir tādu mūķu sagatavošana vai pielāgošana, kas ļauj sistemātiski vai mērogojami izmantot ievainojamības;

7. “kritiski svarīga vai svarīga funkcija” ir kritiski svarīga vai svarīga funkcija, kas definēta Regulas (ES) 2022/2554 3. panta 22) punktā;

8. “vispārīga lietojuma MI modelis” ir MI modelis, kas definēts Regulas (ES) 2024/1689 3. panta 63) punktā;

9. “vispārīga lietojuma MI modelis ar sistēmisku risku” ir vispārīga lietojuma MI modelis, kas klasificēts kā tāds, kurš rada sistēmisku risku saskaņā ar Regulas (ES) 2024/1689 51. panta 1. punktu;

10. “ar IKT saistīts incidents” ir incidents, kas definēts Regulas (ES) 2022/2554 3. panta 8) punktā;

([10]) Sk. *Systemic cyber risk*, ESRK, 2020. gada februāris, pieejams ESRK tīmekļa vietnē www.esrb.europa.eu.

([11]) Piem., ētiska ielaušanās simulācija apdraudējuma izlūkošanas nolūkos (*threat intelligence-based ethical red teaming*; TIBER), draudu vadīta ielaušanās testēšana (*threat-led penetration testing*; TLPT), uzlabota ielaušanās simulācija (*advanced red teaming*; ART) un kibernoturības stresa testēšana (*cyber resilience stress testing*; CyRST).

([12]) Padomes Regula (ES) 2019/796 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 1. lpp., ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. “IKT risks” ir risks, kas definēts Regulas (ES) 2022/2554 3. panta 5) punktā;

12. “darbības noturība” ir digitālās darbības noturība, kas definēta Regulas (ES) 2022/2554 3. panta 1) punktā.

Frankfurtē pie Mainas, 2026. gada 25. jūnijā

ESRK Valdes vārdā –
ESRK sekretariāta vadītājs
Francesco MAZZAFERRO