C/2026/3795

2026.7.16.

AZ EURÓPAI RENDSZERKOCKÁZATI TESTÜLET ÁLTAL KIADOTT FIGYELMEZTETÉS

(2026. június 25.)

az élvonalbeli mesterségesintelligencia-modellekből eredő rendszerszintű kiberkockázatokról

(ERKT/2026/3)

(C/2026/3795)

AZ EURÓPAI RENDSZERKOCKÁZATI TESTÜLET IGAZGATÓTANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az Európai Gazdasági Térségről szóló megállapodásra ([1]) és különösen annak IX. mellékletére,

tekintettel a pénzügyi rendszer európai uniós makroprudenciális felügyeletéről és az Európai Rendszerkockázati Testület létrehozásáról szóló, 2010. november 24-i 1092/2010/EU európai parlamenti és tanácsi rendeletre ([2]) és különösen annak 3. cikke (2) bekezdésének d) pontjára, valamint 16. és 18. cikkére,

tekintettel az Európai Rendszerkockázati Testület eljárási szabályzatának elfogadásáról szóló, 2011. január 20-i ERKT/2011/1 európai rendszerkockázati testületi határozatra ([3]) és különösen annak 18. és 19. cikkére,

mivel:

(1) A vezető mesterségesintelligencia-szolgáltatók élvonalbeli mesterségesintelligencia-modelleket (élvonalbeli MI-modellek) fejlesztettek ki, amelyek rendkívüli képességekkel rendelkeznek a kiberbiztonság területén, és teljes mértékben automatizált kibertámadásokat képesek végrehajtani összetett rendszerek ellen, többek között a sérülékenységek felfedezése és a sebezhetőségek kihasználásának fejlesztése és fegyverként való felhasználása révén, alapjaiban megváltoztatva ezáltal a kiberfenyegetési környezetet.

(2) Az élvonalbeli MI-modellek a korábbi MI-modelleknél sokkal jobbak a kibertámadások végrehajtási módjainak megtalálásában, a költségek, a gyorsaság és a pontosság tekintetében jobbak a korábbi modelleknél, és mostanra felveszik a versenyt a legjobb emberi szakértőkkel.

(3) Az élvonalbeli MI-modellek képesek veszélyeztetni a pénzügyi infrastruktúra alapját képező információs és kommunikációs technológiai (IKT) környezet alapjául szolgáló rendszereket, növelve a rendszerszintű hatással járó kiberbiztonsági események valószínűségét és súlyosságát.

(4) Az élvonalbeli MI-modellek bebizonyították, hogy meg tudják találni a sérülékenységeket és ki tudják alakítani a sebezhetőségek kihasználásának új változatait, kibertámadási kockázatnak kitéve ezáltal a szinte minden szervezet IKT-környezetében használt főbb operációs rendszereket és szoftvereket.

(5) Az ilyen sérülékenységek felfedezése a múltban ritkán fordult elő, és gyakran a biztonsági területen tevékenykedő kutatók tárták fel azokat, ez pedig lehetővé tette a célzott helyreállítást. Ilyen esetben a szoftverszolgáltatóknak gyakran egy rendszeresített időkeretet – általában 90 napot – biztosítanak arra, hogy a nyilvános bevezetés előtt kijavítsák a sérülékenységet. Az élvonalbeli MI-modellek azonban valószínűleg növelni fogják a feltárt sérülékenységek volumenét.

(6) A pénzügyi rendszer jelenlegi hibajavító gyakorlatai túlnyomórészt reaktívak, időszakos frissítésekre és a feltárt sérülékenységekre adott ad hoc válaszokra támaszkodnak. Ez a megközelítés olyan fenyegetettségi környezetben működik, ahol van arra idő, hogy a sérülékenységek felfedezése kezelhető maradjon. A sérülékenységek volumenének növekedésével azonban a jelenlegi gyakorlatok elégtelenné válhatnak a működési reziliencia fenntartásához.

(7) Ez a volumennövekedés túlterheli a jelenlegi hibajavító folyamatokat is, mivel azok a kockázaton alapuló korrekciós intézkedéseket részesítik előnyben, és a működési stabilitás biztosítása érdekében a végrehajtás előtt megkövetelik a szoftverjavítások tesztelését. Ha rövid időn belül túl sok kritikus hatású sérülékenységet fedeznek fel és így jelentősen nő a szükséges kritikus szoftverjavítások száma, előfordulhat, hogy a pénzügyi intézményeknek választaniuk kell: vagy jelentős kiberkockázatoknak teszik ki magukat, vagy csökkentik a javítástesztelési követelményeket és ezáltal kockáztatják a működési zavarokat és üzemszüneteket.

([1]) HL L 1., 1994.1.3., 3. o., ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) HL L 331., 2010.12.15., 1. o., ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) HL C 58., 2011.2.24., 4. o.

(8) A sebezhetőségek kihasználásának fegyverként való felhasználása korábban nagyrészt manuálisan történt és az emberi szakértőknek napokra vagy hetekre volt ehhez szükségük, az élvonalbeli MI-modellek azonban jelenleg perceken vagy órákon belül megvalósítják azt. Ez a kritikus és fontos funkciók helyreállítás közbeni folytonosságának a fenntartásához szükséges védelmi időpufferek összeomlását jelenti.

(9) Az MI-n alapuló kritikus sérülékenységeknek megfeleltethető, a sebezhetőségek kihasználása fegyverként való felhasználásának elterjedésével és a védelmi időpufferek ennek megfelelő rövidülésével meredeken nő az egyes kritikus vagy fontos funkciókat és intézményeket fenyegető kockázat. Ha ezek a kockázatok egyidejűleg jelentkeznek az említett funkcióknál és intézményekben, ez a rendszerszintű kiberkockázat tartós fokozódását eredményezheti, amelyre vonatkozóan jelenleg nem áll rendelkezésre teljes mértékben hatékony kockázatcsökkentési keretrendszer. Az uniós pénzügyi ágazaton belüli, valamint az ezen ágazat és más ágazatok és országok közötti erős összekapcsoltság miatt ez a helyzet rendszeres kockázatot jelent, és rendszerszintű instabilitást teremthet.

(10) Emellett jelenleg csak kevés MI-szolgáltató fejleszt élvonalbeli MI-modelleket, és közülük többen aggodalmukat fejezték ki amiatt, hogy a jövőbeli élvonalbeli MI-modellek túl erősek lehetnek a korlátlan nyilvános hozzáférhetővé tételhez.

(11) Rosszindulatú szereplők már most is MI-t használnak a kibertámadások fokozására. Valószínű, hogy – akár szivárgás, lopás, független fejlesztés vagy nyílt hozzáférés révén – ezek a szereplők végül olyan MI-modellekhez jutnak, amelyek a jelenleg ellenőrzött defenzív környezetben alkalmazott modellekhez hasonló képességekkel rendelkeznek.

(12) Bár az élvonalbeli MI-modellek jelentősen növelhetik a támadó jellegű képességeket és a kifinomult kibertámadások valószínűségét, ugyanakkor erősítik a védekező képességeket is, különösen a sérülékenységek feltárása, az adatok összevetése és az egyes intézmények korrekciós intézkedései tekintetében. Rövid- és középtávon azonban a támadó jellegű képességek sebességének, nagyságrendjének és pontosságának növekedése valószínűleg meghaladja az előnyöket.

(13) Az élvonalbeli MI-modellek gyors fejlődése szükségessé teszi a pénzügyi stabilitást fenyegető azonosított kockázatok haladéktalan kezelését azok bekövetkezésének megelőzése vagy legalább potenciális hatásuk enyhítése érdekében. Az uniós pénzügyi piacok pénzügyi stabilitásának biztosítása érdekében makroprudenciális és mikroprudenciális szakpolitikai intézkedéseikkel összefüggésben az Európai Rendszerkockázati Testület (ERKT) valamennyi tagjának figyelembe kell vennie az élvonalbeli MI-modelleknek a pénzügyi intézmények működési képességére és rezilienciájára gyakorolt hatásait. Ez nem sérti az uniós központi bankok monetáris politika területén fennálló mandátumát. Például – és egyben más hatóságok jelenlegi kezdeményezései mellett – az EKB felügyeleti szerepkörében eljárva azt kérte a jelentős intézetektől, hogy késedelem nélkül értékeljék a fokozódó fenyegetettségi környezet hatásait, és hogy 2026. október 31-éig alakítsanak ki átfogó cselekvési tervet az ilyen kockázatok kezelését célzó konkrét intézkedésekkel ([4]).

(14) Az MI-technológia terjedésével fontos biztosítani azt, hogy valamennyi kritikus infrastruktúra és különösen a pénzügyi intézmények felkészültek legyenek az élvonalbeli MI-modelleken alapuló kibertámadásokkal szembeni fellépésre, valamint azt, hogy időben és megfelelő előkészületeket tegyenek. Az egyes szervezetek ilyen védelmi erőfeszítései azonban nem lennének elegendőek. A hatékony reagáláshoz és kockázatcsökkentéshez összehangolt válaszra van szükség, amelyben valamennyi érintett fél részt vesz, beleértve az MI-szolgáltatókat, a szoftverszolgáltatókat, a biztonsági cégeket, a nyílt forráskódú karbantartókat, a pénzügyi intézményeket, valamint a nemzeti és uniós szintű hatóságokat.

(15) A fenti kérdések kezelése során fontos emlékeztetni a vonatkozó uniós jogi és szakpolitikai keretekre, különösen az (EU) 2022/2554 európai parlamenti és tanácsi rendeletre ([5]), az (EU) 2024/1689 európai parlamenti és tanácsi rendeletre ([6]), az (EU) 2024/2847 európai parlamenti és tanácsi rendeletre ([7]) és az ERKT/2021/17 európai rendszerkockázati testületi ajánlásra ([8]).

([4]) A jelentős intézeteknek címzett levél elérhető az EKB bankfelügyeleti honlapján: www.bankingsupervision.europa.eu.

([5]) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333., 2022.12.27., 1. o., ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet)(HL L 2024/1689, 2024.7.12., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Az Európai Rendszerkockázati Testület ajánlása (2021. december 2.) a rendszerszintű kiberbiztonsági események érintett hatóságok számára létrehozandó páneurópai koordinációs keretéről (ERKT/2021/17) (HL C 134., 2022.3.25., 1. o.).

(16) Az (EU) 2022/2554 rendelet átfogó keretet biztosít a pénzügyi intézmények számára az IKT-kockázatok – többek között a kibertámadásokból eredő kockázatok – azonosításához, kezeléséhez, nyomon követéséhez és csökkentéséhez. Tekintettel a pénzügyi ágazat összekapcsoltságára, valamint az IKT-rendszerekre és harmadik fél szolgáltatókra való támaszkodására, az egy vagy több pénzügyi intézményt vagy azok kritikus szolgáltatóit érintő sikeres kibertámadás jelentős rendszerszintű következményekkel járhat. A pénzügyi felügyeleti hatóságoknak megfelelő elsőbbséget kell biztosítaniuk az e területen végzett felügyeleti tevékenységeknek, tekintettel az ilyen kibertámadásoknak a pénzügyi rendszer stabilitására, integritására és megbízhatóságára gyakorolt lehetséges hatására, valamint az ebből eredő működési, pénzügyi és fogyasztókat érintő károkra.

(17) Az (EU) 2024/1689 rendelet harmonizált szabályokat állapít meg az MI-rendszerek és az általános célú MI-modellek Unión belüli forgalomba hozatalára, üzembe helyezésére és használatára vonatkozóan, ideértve bizonyos körülmények között a harmadik országokban letelepedett MI-szolgáltatók által biztosított rendszereket és modelleket is, ha az MI-rendszer által előállított kimenet használatára az Unióban kerül sor, vagy ha egy MI-modellt az uniós piacon forgalomba hozott rendszerbe integrálnak. A rendelet egyedi szabályokat is megállapít, ideértve a rendszerszintű kockázatot jelentő általános célú MI-modellként besorolt modellekre vonatkozó szigorúbb szabályozási rendszert is.

(18) Az (EU) 2024/2847 rendelet kötelező kiberbiztonsági követelményeket vezet be a gyártók számára, amelyek kiterjednek az uniós piacon forgalomba hozott, digitális elemeket tartalmazó hardver- és szoftvertermékek tervezésére, kialakítására, fejlesztésére és karbantartására. Előírja továbbá a gyártók számára azt, hogy termékeik élettartama alatt kezeljék a sérülékenységeket. Amint 2027 decemberében teljes mértékben alkalmazandóvá válik, az ilyen termékeket az uniós piacon forgalomba hozó pénzügyi szervezeteknek azt is biztosítaniuk kell, hogy ezek a termékek megfeleljenek ezeknek a követelményeknek.

(19) Az ERKT/2021/17 ajánlás azt ajánlotta, hogy az európai felügyeleti hatóságok (EFH-k) a vegyes bizottságon keresztül közösen, valamint az Európai Központi Bankkal (EKB), az ERKT-val és az érintett nemzeti hatóságokkal közösen dolgozzanak ki eredményes, koordinált uniós szintű elhárítást olyan jelentős, határokon átnyúló kiberbiztonsági esemény vagy az ahhoz kapcsolódó fenyegetés esetén, amely rendszerszintű hatással lehet az Unió pénzügyi ágazatára. Ennek eredményeként létrejött a rendszerszintű kiberbiztonsági események páneurópai koordinációs kerete (EU-SCICF), amely értékes és operatív platformot biztosít a pénzügyi hatóságok közötti információcseréhez és koordinációhoz.

(20) Mindezek alapján az ERKT általános jellegű figyelmeztetést fogad el a pénzügyi stabilitásra vonatkozó, az élvonalbeli MI-modellek fejlődése által felerősített jelentős kockázatok kezeléséről. A figyelmeztetés figyelembe veszi az ERKT-nak a kiberképességekkel rendelkező élvonalbeli MI-modellek pénzügyi stabilitási szempontból történő kezelése témakörben 2026 júniusában közzétett feljegyzésében ([9]) végzett elemző munkát,

ELFOGADTA EZT A FIGYELMEZTETÉST:

1. SZAKASZ

Figyelmeztetés

Új kockázati környezet

A kiberképességekkel rendelkező élvonalbeli mesterségesintelligencia-modellek (élvonalbeli MI-modellek) gyors fejlődése lényeges változásokat hoz az uniós pénzügyi rendszer kockázati környezetében. A jelenlegi bizonyítékok azt mutatják, hogy az élvonalbeli MI-modellek képesek feltárni a sérülékenységeket, működőképesen ki tudják használni a sebezhetőségeket és autonóm módon teljes körű kibertámadást tudnak végrehajtani a korábbi MI-modelleket jóval felülmúló sebességgel, léptékben és pontossággal. Ez paradigmaváltást jelent a kiberbiztonság területén, és inflexiós pontot az MI-képességek tekintetében.

Az ERKT úgy véli, hogy ezek a fejlemények rendszerszintű kockázatokat jelentenek a pénzügyi rendszerre nézve, és a sérülékenységek gyorsabb feltárása, a reagálásra és a hatékony védelemre rendelkezésre álló idő lerövidülése, a kibertámadások nagyobb léptéke és kifinomultsága, valamint a pénzügyi rendszeren belüli új függőségek és koncentrációs kockázatok megjelenése révén jelentős káros hatást gyakorolhatnak a kiberbiztonságra. Miközben az ERKT elismeri az élvonalbeli MI-modellek által a pénzügyi intézményeknek kínált megerősített védekező képességeket, ezek a képességek valószínűleg a következő néhány évben fognak fokozatosan megjelenni, ez pedig szükségszerűen azzal jár, hogy a pénzügyi intézmények egy olyan átmeneti időszakban fognak működni, amelyet magas kockázat, nagy fokú bizonytalanság és gyorsan változó technológiai környezet jellemez. Tekintettel a pénzügyi rendszer nagymértékben digitalizált és összefonódó jellegére, a kiberbiztonságra gyakorolt ilyen káros hatások gyorsan átterjedhetnek a pénzügyi intézmények kritikus és fontos funkcióira, ami végső soron rendszerszintű zavarokhoz és a pénzügyi rendszerbe vetett bizalom elvesztéséhez vezethet.

([9]) Elérhető az ERKT honlapján: www.esrb.europa.eu.

A kialakulóban lévő élvonalbeli MI-modellek növelik az eredendő IKT-kockázatot, ami a pénzügyi ágazat működési rezilienciájának gyengüléséhez vezet, különösen négy területen: a) idő, ideértve annak képességét is, hogy üzemzavar nélkül gyorsan kijavítsák az összetett rendszereket, figyelembe véve a sérülékenységek felfedezése és a sebezhetőségek kihasználásának fegyverként való felhasználása közötti védelmi időpufferek összeomlását; b) a védekezők képességei, ideértve az élvonalbeli MI-modellekkel támogatott automatizált és manuális biztonsági tesztelések elvégzésére való képességüket, valamint azt a képességüket, hogy az élvonalbeli MI-modellek rosszindulatú használatából eredő fenyegetéssel szemben védelmet biztosítsanak, felfedezzék azt és reagáljanak arra; c) koncentráció, ideértve a korlátozott számú MI-szolgáltatótól való függőségi viszonyt, ami ugyanakkor felhőszolgáltatóktól, nyílt forráskódú elemektől és egyéb széleskörben használt szoftverektől függ, valamint d) a hatóságok képességei, ideértve az elvárásaik, a stressztesztelés és a felkészültségi intézkedések élvonalbeli MI-modellek fejlődéséhez illeszkedő kiigazítását annak érdekében, hogy az üzemzavarok ne képezzék tágabb összefüggésű instabilitás forrását.

Emellett bármely pénzügyi intézményben kihívást jelent az MI alkalmazásának láthatóvá tétele és ennek megőrzése – ideértve annak teljes körű megértését is, hogy hol és hogyan alkalmazzák az MI-t –, figyelembe véve, hogy azt használják ügyfélinterfészekben, belső ágensekben, üzleti folyamatokban és harmadik felekkel való integráció keretében.

Rendszerszintű értékelés

Az azonosított fejlemények lényegesen megváltoztathatják a kiberkockázat mértékét és szerkezetét, növelve a pénzügyi stabilitást fenyegető közvetlen és közvetett kockázatokat egyaránt. Az élvonalbeli MI-modellek képességei jelentős nyomás alá helyezhetik a meglévő rezilienciakereteket, különösen akkor, ha a biztonsági események széles körben terjednek el és egyidejűleg következnek be. A biztonsági események gyorsan terjedhetnek a pénzügyi intézmények és piacok között is, ha kritikus harmadik fél szolgáltatókat, közös technológiai ökoszisztémákat vagy széles körben használt nyílt forráskódú összetevőket érintenek, növelve a rendszerszintű következményekkel járó kapcsolódó zavarok kockázatát.

Az élvonalbeli MI-modellek a pénzügyi ágazat három aszimmetria-forrását változtatják meg: az országok közöttit, a védekező és a támadó közöttit, és a jobban felszerelt és a kevésbé felszerelt pénzügyi intézmények közöttit.

A vezető MI-szolgáltatók jelenlegi földrajzi koncentrációja az Unión kívül stratégiai függőségnek és geopolitikai kockázatnak teszi ki az Uniót. Az országok közötti ismeretbeli és technológiai aszimmetria enyhítése érdekében olyan intézkedések elfogadására van szükség, amelyek megkönnyítik az Unió és tagállamai számára az újonnan kifejlesztett élvonalbeli MI-modellekhez való megfelelő és arányos hozzáférést. Ezeknek az intézkedéseknek időszerűnek, koherensnek és hatékonynak kell lenniük mind a szakpolitika, mind a végrehajtás tekintetében, és megfelelően figyelembe kell venniük a különböző uniós pénzügyi ágazatokat, kihasználva a megfelelő EFH-k szakértelmét. Ez enyhíteni fogja nem csupán az Unió és a harmadik országok közötti aszimmetriát, hanem a különböző tagállamokban letelepedett pénzügyi intézmények közötti aszimmetriát is, megőrizve az egyenlő versenyfeltételeket az Unión belül és kívül, és minimalizálva a rendszerszintű kockázatot. Az élvonalbeli MI-modellekhez való hozzáférést csak bizonyos intézménykategóriák vagy kiválasztott országok számára megkönnyítő megállapodások hozzájárulnának az egységes pénzügyi piac széttagoltságához, csökkentve annak likviditását és mélységét.

Ami a támadók és a védekezők közötti aszimmetriát illeti, az élvonalbeli MI-modellek csökkentik a támadók belépési költségét. A támadó jellegű műveletek technikailag fejlettebb és munkaerő-igényesebb részeinek végrehajtása során a fenyegető szereplők valószínűleg egyre nagyobb mértékben támaszkodnak élvonalbeli MI-modellekre, ez pedig csökkenti a költségeket. Ezzel szemben a védekezőket korlátozzák az operatív követelmények, a függőségek és a szabályozási kötelezettségek, ez pedig rövid és középtávon korlátozza az élvonalbeli MI-modellek jótékony hatását és annak nagyságrendjét, és végső soron hosszabb alkalmazkodási időt igényel.

Különbségek vannak abban, hogy a pénzügyi intézmények milyen mértékben rendelkeznek erőforrásokkal és eszközökkel ahhoz, hogy megbirkózzanak az élvonalbeli MI-modellek jelentette kihívásokkal. Ezek a különbségek a nem arányos, hanem állandó költségekből, az erőforrások szűkösségéből és a szakemberekhez való korlátozott hozzáférésből adódhatnak. Amennyiben aszimmetria áll fenn az ilyen kihívások kezelésére való képességben, a leggyengébb láncszem befolyásolhatja a rendszer stabilitását.

Várható hatások

Alapvető fontosságú annak biztosítása, hogy a rendszerszempontból jelentős fizetési és kiegyenlítési rendszerek és pénzügyi piaci infrastruktúrák továbbra is védettek maradjanak az élvonalbeli MI-modellek használatából és fejlesztéséből eredő sérülékenységekkel szemben. Az állami és magánszereplőknek alaposan felül kell vizsgálniuk és aktualizálniuk kell kiberbiztonsági keretrendszereiket az ilyen sérülékenységek figyelembevétele érdekében. A felügyeletért vagy felvigyázásért felelős hatóságoknak intézkedéseket kell elfogadniuk a rendszerek megfelelő védelmének biztosítása érdekében. Szükség esetén törekedni kell a hatóságok és a magán pénzügyi intézmények közötti együttműködésre az uniós pénzügyi rendszer biztonságának és ellenálló képességének növelése érdekében.

A rendszerszintű kiberkockázatokról szóló 2020. évi jelentésében ([10]) az ERKT a kiberfenyegetések sebességét, nagyságrendjét és rosszindulatú szándékát a rendszerszintű kockázatok terjedésének lehetséges forrásaként azonosította. A hatóságoknak tisztában kell lenniük azzal, hogy miközben az élvonalbeli MI-modellek új terjedési forrást jelentenek, egyben felerősítik a már létező és korábban azonosított forrásokat, és ezt a felismerést be kell építeniük szakpolitikai intézkedéseikbe. Figyelembe véve a pénzügyi ágazat kiberkockázatnak való működési kitettségéből eredő összes pénzügyi stabilitási kockázatot, fontos biztosítani azt, hogy az e figyelmeztetésben azonosított aggályok tükröződjenek az érintett hatóságok által saját megbízatásuk keretein belül végzett felügyeleti és felvigyázási munkában és elfogadott szakpolitikai irányvonalakban.

Az érintett hatóságoknak – saját hatáskörükön belül és különösen az (EU) 2022/2554 rendelettel létrehozott keret alapján – tisztában kell lenniük az élvonalbeli MI-modellek által a pénzügyi ágazatba behozott, korábban említett három aszimmetriát okozó forrással. Ezen aszimmetriák csökkentése érdekében a meglévő tesztelési keretek ([11]) mellett fontolóra kell venni együttműködési megállapodások kialakítását és az ágazati koordinációt is. A pénzügyi hatóságoknak azt is biztosítaniuk kell, hogy a magán pénzügyi intézmények igazgatótanácsai teljes mértékben elkötelezettek legyenek az élvonalbeli MI-modellekből fakadó kiberkockázatok csökkentése mellett, hogy egyértelmű irányítási és elszámoltathatósági keret álljon rendelkezésre, és hogy a megfelelő belső beruházásokkal kiegészítve megfelelően megtervezzék az időben történő reagálást.

Az e figyelmeztetésben számba vett számos lehetséges fejlemény – legyen szó akár a rendszerszintű hatásról, a geopolitikai kockázatról vagy a támadók és a védekezők közötti megváltozott egyensúlyról – hatással lehet a pénzügyi rendszer működésére és az abba vetett bizalomra. Folyamatos értékelésük érdekében az ERKT mérlegeli, hogy e fejleményeknek meg kell-e jelenniük a kockázatértékelésekben, a tesztelési keretekben és a felügyeleti elvárásokban, valamint a jövőbeli forgatókönyvek kidolgozásában. Az ERKT nyomon fogja követni az élvonalbeli MI-modellek használatát és alakulását is, valamint azoknak a rendszerkockázat szempontjából a pénzügyi szektorra gyakorolt hatását. Ezen túlmenően az ERKT minden igazgatótanácsi szintű negyedéves kockázatértékelés során újra fogja értékelni a fejleményeket, és szükség esetén egyéb intézkedéseket is fontolóra vesz.

2. SZAKASZ

Fogalommeghatározások

E figyelmeztetés alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

1. „MI-szolgáltató”: az (EU) 2024/1689 irányelv 3. cikkének 3. pontjában meghatározott szolgáltató;

2. „élvonalbeli mesterségesintelligencia-modellek (élvonalbeli MI-modellek)”: fejlett általános célú MI-modellek, amelyek képesek lényegesen befolyásolni a támadó jellegű vagy defenzív kiberműveleteket;

3. „kibertámadás”: az (EU) 2019/796 tanácsi rendelet ([12]) 1. cikkében meghatározott kibertámadás, ideértve azt az esetet is, amikor az az Unión belülről származik;

4. „sérülékenység”: az (EU) 2022/2554 rendelet 3. cikkének 16. pontjában meghatározott sérülékenység;

5. „sebezhetőség kihasználása”: olyan eszköz, technika vagy módszer, amelyet arra használnak, hogy egy vagy több sérülékenységet kihasználva jogosulatlan hozzáférést szerezzenek a rendszerekhez, módosítsák vagy megzavarják azokat, vagy más módon IKT-kockázatot vagy IKT-vonatkozású eseményt idézzenek elő;

6. „fegyverként való felhasználás”: a sebezhetőség kihasználásának előkészítése vagy kiigazítása annak lehetővé tétele érdekében, hogy rendszeres vagy skálázható mértékben kihasználják a sérülékenységeket;

7. „kritikus vagy fontos funkció”: az (EU) 2022/2554 rendelet 3. cikkének 22. pontjában meghatározott kritikus vagy fontos funkció;

8. „általános célú MI-modell”: az (EU) 2024/1689 irányelv 3. cikkének 63. pontjában meghatározott MI-modell;

9. „rendszerszintű kockázatot jelentő általános célú MI-modell”: az (EU) 2024/1689 rendelet 51. cikkének (1) bekezdésével összhangban rendszerszintű kockázatot jelentőnek besorolt általános célú MI-modell;

10. „IKT-vonatkozású esemény”: az (EU) 2022/2554 rendelet 3. cikkének 8. pontjában meghatározott esemény;

([10]) Lásd: „Systemic cyber risk” (A rendszerszintű kiberkockázat), ERKT, 2020. február, elérhető az ERKT honlapján: www.esrb.europa.eu.

([11]) Például: a fenyegetettségi információkon alapuló etikai érdekütköztetéses elemzés (TIBER), a fenyegetettségi szempontú behatolási tesztelés (TLPT), a fejlett érdekütköztetéses elemzőcsoportok (red team) (ART) és a kiberrezilienciával kapcsolatos stressztesztelés (CyRST).

([12]) A Tanács (EU) 2019/796 rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129 I., 2019.5.17., 1. o., ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11. „IKT-kockázat”: az (EU) 2022/2554 irányelv 3. cikkének 5. pontjában meghatározott kockázat;

12. „működési reziliencia”: az (EU) 2022/2554 irányelv 3. cikkének 1. pontjában meghatározott digitális működési reziliencia;

Kelt Frankfurt am Mainban, 2026. június 25-én.

az ERKT titkárságának vezetője,
az ERKT igazgatótanácsa nevében,
Francesco MAZZAFERRO