I

(Állásfoglalások, ajánlások és vélemények)

AJÁNLÁSOK

EURÓPAI RENDSZERKOCKÁZATI TESTÜLET

AZ EURÓPAI RENDSZERKOCKÁZATI TESTÜLET AJÁNLÁSA

(2021. december 2.)

a rendszerszintű kiberbiztonsági események érintett hatóságok számára létrehozandó páneurópai koordinációs keretéről

(ERKT/2021/17)

(2022/C 134/01)

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 b) és 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 18–20. cikkére,

mivel:

(1) Ahogyan azt az ERKT/2013/1 európai rendszerkockázati testületi ajánlás ([4]) (4) preambulumbekezdése megállapítja, a makroprudenciális politika végső célja a pénzügyi rendszer egésze stabilitásának megőrzéséhez való hozzájárulás – beleértve a pénzügyi rendszer ellenálló képességének növelésén és a rendszerszintű kockázatok felgyülemlésének csökkentésén keresztül történő hozzájárulást –, ezzel biztosítva a pénzügyi szektor gazdasági növekedéshez való fenntartható hozzájárulását. Az Európai Rendszerkockázati Testület (ERKT) felelős az Unió pénzügyi rendszerének makroprudenciális felügyeletéért. Megbízatásának ellátása során az ERKT-nak hozzá kell járulnia a pénzügyi stabilitást fenyegető, többek között a kiberbiztonsági eseményekkel kapcsolatos rendszerkockázatok megelőzéséhez vagy mérsékléséhez és javaslatokat kell tennie e kockázatok mérséklésének módjára.

(2) A jelentős kiberbiztonsági események rendszerszintű kockázatot jelenthetnek a pénzügyi rendszerre nézve, mivel képesek megzavarni a kulcsfontosságú pénzügyi szolgáltatásokat és tevékenységeket. A kezdeti sokk felerősödhet operatív vagy pénzügyi átterjedés révén, vagy a pénzügyi rendszerbe vetett bizalom megrendülésével. Ha a pénzügyi rendszer nem képes kezelni ezeket a sokkokat, veszélybe kerül a pénzügyi stabilitás, és ez a helyzet rendszerszintű kiberválsághoz vezethet ([5]).

([1]) HL L 1., 1994.1.3., 3. o.
([2]) HL L 331., 2010.12.15., 1. o.
([3]) HL C 58., 2011.2.24., 4. o.
([4]) Az Európai Rendszerkockázati Testület ERKT/2013/1 ajánlása (2013. április 4.) a makroprudenciális politika köztes célkitűzéseiről és eszközeiről (HL C 170., 2013.6.15., 1. o.).
([5]) Lásd: „Systemic cyber risk” (A rendszerszintű kiberkockázat), ERKT, 2020. február, elérhető az ERKT honlapján: www.esrb.europa.eu

(3) A gyorsan változó kiberfenyegetettségi helyzet és a jelentős kiberbiztonsági események számának közelmúltbeli növekedése jelzi az Unió pénzügyi stabilitását fenyegető nagyobb kockázatot. A Covid19-világjárvány rávilágított arra, hogy a technológia fontos szerepet játszik a pénzügyi rendszer működésének lehetővé tételében. Az érintett hatóságoknak és intézményeknek hozzá kellett igazítaniuk technikai infrastruktúrájukat és kockázatkezelési keretrendszereiket a távmunka hirtelen térnyeréséhez, ami növelte a pénzügyi rendszer kiberfenyegetésnek való általános kitettségét, és lehetővé tette a bűnözők számára, hogy új működési módokat dolgozzanak ki és a helyzet kihasználása érdekében kiigazítsák a meglévőket ([6]). Ennek fényében az EKB bankfelügyeletéhez bejelentett kiberbiztonsági események száma 2020-ban 54 %-kal nőtt 2019-hez képest ([7]).

(4) A jelentős kiberbiztonsági események potenciálisan nagy léptéke, terjedési sebessége és mértéke miatt az érintett hatóságoknak eredményes válaszlépéseket kell tenniük a pénzügyi stabilitásra gyakorolt esetleges negatív hatások enyhítése érdekében. Az érintett hatóságok közötti uniós szintű gyors koordináció és kommunikáció segíthet a jelentős kiberbiztonsági események pénzügyi stabilitásra gyakorolt hatásának korai értékelésében, a pénzügyi rendszerbe vetett bizalom fenntartásában és a más pénzügyi intézményekre való átterjedés korlátozásában, és ezáltal hozzájárulhat annak megelőzéséhez, hogy valamely jelentős kiberbiztonsági esemény kockázatot jelentsen a pénzügyi stabilitásra nézve.

(5) A releváns sokk az érintett hatóságok által általában tapasztalt hagyományos pénzügyi és likviditási válsághoz képest újszerű forrásból származik. A pénzügyi szempontokon kívül az átfogó kockázatértékelésnek ki kell terjednie a működési zavarok mértékére és hatására is, mivel ezek befolyásolhatják a makroprudenciális eszközök megválasztását. Hasonlóképpen, a pénzügyi stabilitás befolyásolhatja az operatív mérséklő eszközök kiberszakértők általi megválasztását is. Ez szoros és gyors koordinációt és nyílt kommunikációt tesz szükségessé többek között a helyzetismeret kialakítása érdekében.

(6) Fennáll annak a kockázata, hogy kudarcot vall a hatóságok koordinációja, és ezt kezelni kell. Az érintett uniós hatóságoknak egyeztetniük kell egymással és más hatóságokkal, például az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA; korábban: Európai Uniós Hálózat- és Információbiztonsági Ügynökség), amellyel lehet, hogy egyébként nem tartják a kapcsolatot. Mivel az uniós pénzügyi intézmények jelentős része globális szinten működik, egy jelentős kiberbiztonsági esemény valószínűleg nem korlátozódik az Unióra, vagy elképzelhető, hogy az Unión kívül következik be és összehangolt globális elhárítást tehet szükségessé.

(7) Az illetékes hatóságoknak fel kell készülniük az ilyen együttműködésre. Ellenkező esetben fennáll annak a kockázata, hogy olyan következetlen intézkedésekre kerül sor, amelyek ellentmondanak más hatóságok reakcióinak vagy veszélyeztetik azokat. Egy ilyen koordinációs kudarc felerősítheti a pénzügyi rendszert érő sokkhatást azáltal, hogy a pénzügyi rendszer működésébe vetett bizalom megrendüléséhez vezet, ami a legrosszabb esetben kockázatot jelentene a pénzügyi stabilitásra nézve ([8]). Ezért meg kell tenni a szükséges lépéseket annak érdekében, hogy jelentős kiberbiztonsági esemény esetén kezelni lehessen a koordináció kudarcából eredő, a pénzügyi stabilitást fenyegető kockázatot.

(8) Az ERKT „Mitigating systemic cyber risk” (A rendszerszintű kiberkockázat csökkentése) című, 2021. évi jelentése ([9]) megállapítja, hogy az érintett uniós hatóságok számára létre kell hozni a rendszerszintű kiberbiztonsági események páneurópai koordinációs keretét (EU-SCICF). Az EU-SCICF célja az lenne, hogy növelje az érintett hatóságok felkészültségét a potenciálisan jelentős kiberbiztonsági események összehangolt elhárításának megkönnyítése érdekében. Az ERKT „Mitigating systemic cyber risk” (A rendszerszintű kiberkockázat csökkentése) című, 2021. évi jelentése tartalmazza az ERKT értékelését a keretrendszer azon jellemzőiről, amelyekre elsőként szükség lenne a koordinációs kudarc kockázatának kezeléséhez.

(9) Ezen ajánlás fő célkitűzése, hogy a pénzügyi ágazat digitális működési rezilienciájáról szóló európai parlamenti és tanácsi rendeletre (a továbbiakban: DORA rendelet) irányuló javaslat ([10]) keretében az európai felügyeleti hatóságok (EFH-k) egyik tervezett szerepére építve fokozatosan lehetővé tegye az eredményes, koordinált uniós szintű elhárítást, hogy kezelhessék a jelentős, határokon átnyúló információs és kommunikációs technológiákat (IKT) érintő biztonsági eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére. Ez a folyamat az EU-SCICF létrehozásához vezet az érintett hatóságok számára.

([6]) Lásd: „Internet Organised Crime Threat Assessment” (A szervezett internetes bűnözésből fakadó fenyegetettséget vizsgáló jelentés), Europol, 2020., elérhető az Europol honlapján: www.europol.europa.eu

([7]) Lásd: „IT and cyber risk: a constant challenge” (IT és kiberkockázat: folyamatos kihívás), EKB, 2021., elérhető az EKB Bankfelügyelet honlapján: www.bankingsupervision.europa.eu

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

([9]) Lásd: „Mitigating systemic cyber risk” (A rendszerszintű kiberkockázat csökkentése), ERKT, 2021., (megjelenés előtt).

([10]) COM/2020/595 final.

(10) Az EU-SCICF-nek nem a meglévő keretrendszerek felváltására kell törekednie, hanem arra, hogy áthidalja a koordinációs és kommunikációs hiányosságokat egyrészt maguk az érintett hatóságok között, másrészt pedig az Unió más hatóságaival és más kulcsfontosságú nemzetközi szereplőkkel való kapcsolattartásuk során. Mérlegelni kell, hogy az EU-SCICF hol helyezkedik el a pénzügyi válság kezelésére szolgáló meglévő keret és a kiberbiztonsági eseményeket kezelő meglévő uniós keretrendszer alkotta mezőben. A maguk az érintett hatóságok közötti koordinációt illetően figyelembe kell venni – többek között – a pénzügyi szervezetek (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([11]) szerinti kiberbiztonsági együttműködési csoportjának szerepét és tevékenységeit, valamint a közös kiberbiztonsági egység létrehozása és az ENISA bevonása révén előirányzott koordinációs mechanizmusokat.

(11) Az EU-SCICF előkészítésének elindítására irányuló javaslat célja különösen az EFH-k DORA rendeletre irányuló javaslatban előirányzott potenciális szerepének támogatása. A DORA rendeletre irányuló javaslat szerint „az EFH-k a vegyes bizottság keretében, az EKB-val és az ERKT-val együttműködve mechanizmusokat alakíthatnak ki, amelyek lehetővé teszik az eredményes módszerek pénzügyi ágazatok közötti megosztását a helyzetismeret javítása, valamint a pénzügyi ágazatok számára közös kibersebezhetőségek és -kockázatok azonosítása céljából”, és „kibertámadási forgatókönyveket alkalmazó válságkezelési és vészhelyzeti műveleteket dolgozhatnak ki kommunikációs csatornák kialakítása, valamint az eredményes, koordinált uniós szintű elhárítás fokozatos lehetővé tétele érdekében, hogy kezelhessék a jelentős, határokon átnyúló IKT-vonatkozású biztonsági eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére” ([12]). Az EU-SCICF-hez hasonló páneurópai keret még nem létezik, és azt a DORA rendelettel összefüggésben kellene létrehozni és fejleszteni.

(12) Tekintettel arra, hogy a kiberkockázatok kockázatot jelentenek az Unió pénzügyi stabilitására nézve, az EU-SCICF fokozatos létrehozására irányuló előkészítő munkát a lehetőségekhez mérten már a létrehozásához szükséges jogi és szakpolitikai keret teljes körű alkalmazása előtt meg kellene kezdeni. Ez a jogi és szakpolitikai keret akkor válna teljes mértékben befejezetté és véglegessé, amint a DORA rendelet és a kapcsolódó felhatalmazáson alapuló jogi aktusok vonatkozó rendelkezései alkalmazandóvá válnak.

(13) Az eredményes kommunikáció hozzájárul az érintett hatóságok helyzetismeretéhez, és így a jelentős kiberbiztonsági események során az egész Unióra kiterjedő koordináció elengedhetetlen előfeltétele. E tekintetben meg kell határozni a jelentős kiberbiztonsági események elhárításának koordinálásához szükséges kommunikációs infrastruktúrát. Ez azt jelentené, hogy meg kell határozni a megosztandó információk típusát, az ilyen információk megosztására használt rendes csatornákat és azokat a kapcsolattartó pontokat, amelyekkel az információkat meg kell osztani. Az információmegosztásnak tiszteletben kell tartania a hatályos jogi követelményeket. Emellett az érintett hatóságoknak egyértelmű cselekvési tervet és a követendő protokollokat is meg kell határozniuk annak érdekében, hogy biztosítsák a jelentős kiberbiztonsági események összehangolt elhárításának tervezésében részt vevő hatóságok közötti megfelelő koordinációt.

(14) Egy rendszerszintű kiberválság szükségessé teszi a teljes körű nemzeti és uniós szintű együttműködés elindítását. Ezért elképzelhető, hogy az EFH-k, az EKB és az illetékes nemzeti hatóságaik közül az egyes tagállamok kijelölik a kapcsolattartó pontjaikat és ezekről tájékoztatják az EFH-kat, annak érdekében, hogy meghatározzák az EU-SCICF koordinációs rendszerében jelentős kiberbiztonsági esemény esetén értesítendő fő tárgyalópartnereket. Az EU-SCICF kidolgozása során értékelni kellene a kapcsolattartó pontok kijelölésének szükségességét, figyelembe véve a tagállamok által az (EU) 2016/1148 irányelv alapján a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására a más tagállamokkal és a kiberbiztonsági együttműködési csoporttal ([13]) való, határokon átnyúló együttműködés biztosítása érdekében kijelölt egyedüli kapcsolattartó pontokat.

(15) A válságkezelési és vészhelyzeti műveletek lefolytatása megkönnyítheti az EU-SCICF végrehajtását, és lehetővé teheti a hatóságok számára, hogy értékeljék az uniós szintű rendszerszintű kiberválságra való felkészültségüket. Ezek a műveletek biztosíthatnák a hatóságok számára tanulságok levonását és lehetővé tehetnék az EU-SCICF folyamatos fejlesztését és fejlődését.

([11]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

([12]) Lásd a DORA rendeletre irányuló javaslat tervezett 43. cikkét.

([13]) Lásd: Európai Bizottság, Kiberbiztonsági együttműködési csoport, elérhető az Európai Bizottság honlapján: www.ec.europa.eu

(16) Az EU-SCICF fejlesztéséhez elengedhetetlen, hogy az EFH-k közösen végezzék el a megfelelő előkészítő munkát annak érdekében, hogy megvizsgálják a keretrendszer lehetséges kulcsfontosságú elemeit és az annak fejlesztéséhez szükséges erőforrásokat és kapcsolódó igényeket. Ezt követően az EFH-k megkezdhetnék az olyan akadályok előzetes elemzését, amelyek akadályozhatják az EFH-kat és az érintett hatóságokat abban, hogy létrehozzák az EU-SCICF-et, és jelentős kiberbiztonsági esemény esetén kommunikációs csatornákon keresztül megosszák a releváns információkat. Egy ilyen elemzés fontos lépést jelentene minden további akár jogalkotási jellegű, akár az Európai Bizottság által a DORA rendeletet követő végrehajtási szakaszban tett egyéb támogató kezdeményezés tekintetében,

ELFOGADTA EZT AZ AJÁNLÁST:

1. SZAKASZ

AJÁNLÁSOK

A. ajánlás – A rendszerszintű kiberbiztonsági események páneurópai koordinációs keretének (EU-SCICF) létrehozása

(1) Ajánlott, hogy a pénzügyi ágazat digitális működési rezilienciájáról szóló európai parlamenti és tanácsi rendeletre (a továbbiakban: DORA rendelet) irányuló bizottsági javaslatban foglaltaknak megfelelően az európai felügyeleti hatóságok (EFH-k) a vegyes bizottságon keresztül közösen, valamint az Európai Központi Bankkal (EKB), az Európai Rendszerkockázati Testülettel (ERKT) és az érintett nemzeti hatóságokkal közösen kezdjék meg az eredményes, koordinált uniós szintű elhárítás fokozatos kialakításának előkészítését, hogy kezelhessék a jelentős, határokon átnyúló kiberbiztonsági eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazatra. Az uniós szintű összehangolt elhárításra irányuló előkészítő munkának magában kell foglalnia az EU-SCICF fokozatos fejlesztését az EFH-k, az EKB, az ERKT és az érintett nemzeti hatóságok számára. Ennek magában kell foglalnia az EU-SCICF hatékony fejlesztéséhez szükséges erőforrásigény értékelését is.

(2) Ajánlott, hogy az EFH-k az A(1) ajánlásra tekintettel az EKB-val és az ERKT-val konzultálva végezzék el az EU-SCICF hatékony fejlesztését gátló jelenlegi akadályok, jogi és egyéb működési korlátok feltérképezését és azt követő elemzését.

B. ajánlás – Az EU-SCICF kapcsolattartó pontok létrehozása

Ajánlott, hogy az EFH-k, az EKB és az illetékes nemzeti hatóságaik közül az egyes tagállamok jelöljék ki fő kapcsolattartó pontjukat és erről tájékoztassák az EFH-kat. Ez az kapcsolattartó lista megkönnyíti a keret kidolgozását, és az EU-SCICF létrejöttét követően jelentős kiberbiztonsági esemény esetén a kapcsolattartó pontokat és az ERKT-t kell tájékoztatni. Az EU-SCICF és a tagállamok által a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv alapján a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására a más tagállamokkal és a kiberbiztonsági együttműködési csoporttal való, határokon átnyúló együttműködés biztosítása érdekében kijelölt egyedüli kapcsolattartó pontok közötti koordinációt is elő kell irányozni.

C. ajánlás – Megfelelő uniós szintű intézkedések

Ajánlott, hogy a Bizottság – az A. ajánlással összhangban elvégzett elemzések eredményei alapján – mérlegelje a rendszerszintű kiberbiztonsági események eredményes, koordinált elhárításának biztosításához szükséges megfelelő intézkedéseket.

2. SZAKASZ

VÉGREHAJTÁS

1. **Fogalommeghatározások**

Ezen ajánlás alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

a) „kiber”: személyek, folyamatok, adatok és információs rendszerek közötti interakciók összekapcsolt információs infrastruktúrájához kapcsolódó, azon belüli vagy azon keresztüli ([14]);

([14]) Lásd: „Cyber Lexicon” (Kiber lexikon), FSB, 2018. november 12., elérhető az FSB honlapján: www.fsb.org

b) „jelentős kiberbiztonsági esemény”: olyan IKT-vonatkozású biztonsági esemény, amely fokozottan káros hatással lehet a pénzügyi szervezetek kulcsfontosságú funkcióit támogató hálózati és információs rendszerekre ([15]);

c) „rendszerszintű kiberválság”: olyan jelentős kiberbiztonsági esemény, amely az uniós pénzügyi rendszerben olyan mértékű zavart okoz, amely súlyos negatív következményekkel járhat a belső piac zavartalan működésére és a reálgazdaság működésére nézve. Az ilyen válság olyan jelentős kiberbiztonsági esemény eredménye lehet, amely számos – többek között működési, bizalmi és pénzügyi – csatornában okoz sokkhatást;

d) „európai felügyeleti hatóságok” vagy „EFH-k”: az 1093/2010/EU európai parlamenti és tanácsi rendelettel ([16]) létrehozott európai felügyeleti hatóság (Európai Bankhatóság), az 1094/2010/EU európai parlamenti és tanácsi rendelettel ([17]) létrehozott európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) és az 1095/2010/EU európai parlamenti és tanácsi rendelettel ([18]) létrehozott európai felügyeleti hatóság (Európai Értékpapír-piaci Hatóság) együttesen;

e) „vegyes bizottság”: az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 54. cikkével létrehozott európai felügyeleti hatóságok vegyes bizottsága;

f) „érintett nemzeti hatóság”:

1. az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 1. cikkének (2) bekezdésében említett uniós jogi aktusokban meghatározott tagállami hatáskörrel rendelkező vagy felügyeleti hatóság, valamint az európai felügyeleti hatóságokra feladatokat ruházó uniós jogi aktusokban meghatározott bármely más illetékes nemzeti hatóság;

2. valamely tagállam illetékes hatósága, amelyet az alábbiakkal összhangban jelöltek ki:

i. a 2013/36/EU európai parlamenti és tanácsi irányelv ([19])4. cikke, az 1024/2013/EU tanácsi rendelettel ([20]) az EKB-ra ruházott külön feladatok sérelme nélkül;

ii. az (EU) 2015/2366 európai parlamenti és tanácsi irányelv ([21]) 22. cikke;

iii. a 2009/110/EK európai parlamenti és tanácsi irányelv ([22]) 37. cikke;

iv. az (EU) 2019/2034 európai parlamenti és tanácsi irányelv ([23]) 4. cikke;

([15]) Lásd a DORA rendeletre irányuló javaslat tervezett 3. cikkének 7. pontját.

([16]) Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o.).

([17]) Az Európai Parlament és a Tanács 1094/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) létrehozásáról, valamint a 716/2009/EK határozat módosításáról és a 2009/79/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 48. o.).

([18]) Az Európai Parlament és a Tanács 1095/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Értékpapír-piaci Hatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/77/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 84. o.).

([19]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.).

([20]) A Tanács 1024/2013/EU rendelete (2013. október 15.) az Európai Központi Banknak a hitelintézetek prudenciális felügyeletére vonatkozó politikákkal kapcsolatos külön feladatokkal történő megbízásáról (HL L 287., 2013.10.29., 63. o.).

([21]) Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

([22]) Az Európai Parlament és a Tanács 2009/110/EK irányelve (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (HL L 267., 2009.10.10., 7. o.).

([23]) Az Európai Parlament és a Tanács (EU) 2019/2034 irányelve (2019. november 27.) a befektetési vállalkozások prudenciális felügyeletéről, valamint a 2002/87/EK, a 2009/65/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU és a 2014/65/EU irányelv módosításáról (HL L 314., 2019.12.5., 64. o.).

v. a kriptoeszközök piacairól és az (EU) 2019/1937 irányelv módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat ([24]) 3. cikke (1) bekezdése ee) pontjának első francia bekezdése;

vi. a 909/2014/EU európai parlamenti és tanácsi rendelet ([25]) 11. cikke;

vii. a 648/2012/EU európai parlamenti és tanácsi rendelet ([26]) 22. cikke;

viii. a 2014/65/EU európai parlamenti és tanácsi irányelv ([27]) 67. cikke;

ix. a 648/2012/EU rendelet 22. cikke;

x. a 2011/61/EU európai parlamenti és tanácsi irányelv ([28]) 44. cikke;

xi. a 2009/65/EK európai parlamenti és tanácsi irányelv ([29]) 97. cikke;

xii. a 2009/138/EK európai parlamenti és tanácsi irányelv ([30]) 30. cikke;

xiii. az (EU) 2016/97 európai parlamenti és tanácsi irányelv ([31]) 12. cikke;

xiv. az (EU) 2016/2341 európai parlamenti és tanácsi irányelv ([32]) 47. cikke;

xv. az 1060/2009/EK európai parlamenti és tanácsi rendelet ([33]) 22. cikke;

xvi. a 2006/43/EK európai parlamenti és tanácsi irányelv ([34]) 3. cikkének (2) bekezdése és 32. cikke;

xvii. az (EU) 2016/1011 európai parlamenti és tanácsi rendelet ([35]) 40. cikke;

xviii. az (EU) 2020/1503 európai parlamenti és tanácsi rendelet ([36]) 29. cikke;

([24]) COM/2020/593 final.

([25]) Az Európai Parlament és a Tanács 909/2014/EU rendelete (2014. július 23.) az Európai Unión belüli értékpapír-kiegyenlítés javításáról és a központi értéktárakról, valamint 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról (HL L 257., 2014.8.28., 1. o.).

([26]) Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.).

([27]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

([28]) Az Európai Parlament és a Tanács 2011/61/EU irányelve (2011. június 8.) az alternatívbefektetésialap-kezelőkről, valamint a 2003/41/EK és a 2009/65/EK irányelv, továbbá az 1060/2009/EK és az 1095/2010/EU rendelet módosításáról (HL L 174., 2011.7.1., 1. o.).

([29]) Az Európai Parlament és a Tanács 2009/65/EK irányelve (2009. július 13.) az átruházható értékpapírokkal foglalkozó kollektív befektetési vállalkozásokra (ÁÉKBV) vonatkozó törvényi, rendeleti és közigazgatási rendelkezések összehangolásáról (HL L 302., 2009.11.17., 32. o.).

([30]) Az Európai Parlament és a Tanács 2009/138/EK irányelve (2009. november 25.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról (Szolvencia II) (HL L 335., 2009.12.17., 1. o.).

([31]) Az Európai Parlament és a Tanács (EU) 2016/97 irányelve (2016. január 20.) a biztosítási értékesítésről (HL L 26., 2016.2.2., 19. o.).

([32]) Az Európai Parlament és a Tanács (EU) 2016/2341 irányelve (2016. december 14.) a foglalkoztatói nyugellátást szolgáltató intézmények tevékenységéről és felügyeletéről (HL L 354., 2016.12.23., 37. o.).

([33]) Az Európai Parlament és Tanács 1060/2009/EK rendelete (2009. szeptember 16.) a hitelminősítő intézetekről (HL L 302., 2009.11.17., 1. o.).

([34]) Az Európai Parlament és a Tanács 2006/43/EK irányelve (2006. május 17.) az éves és összevont (konszolidált) éves beszámolók jog szerinti könyvvizsgálatáról, a 78/660/EGK és a 83/349/EGK tanácsi irányelv módosításáról, valamint a 84/253/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 157., 2006.6.9., 87. o.).

([35]) Az Európai Parlament és a Tanács (EU) 2016/1011 rendelete (2016. június 8.) a pénzügyi eszközökben és pénzügyi ügyletekben referenciamutatóként vagy a befektetési alapok teljesítményének méréséhez felhasznált indexekről, valamint a 2008/48/EK és a 2014/17/EU irányelv, továbbá az 596/2014/EU rendelet módosításáról (HL L 171., 2016.6.29., 1. o.).

([36]) Az Európai Parlament és a Tanács (EU) 2020/1503 rendelete (2020. október 7.) az európai közösségi finanszírozási üzleti szolgáltatókról, valamint az (EU) 2017/1129 rendelet és az (EU) 2019/1937 irányelv módosításáról (HL L 347., 2020.10.20., 1. o.).

3. a makroprudenciális politikai intézkedések elfogadásával és/vagy aktiválásával vagy a pénzügyi stabilitással kapcsolatos más feladatokkal, például a kapcsolódó alátámasztó elemzéssel megbízott hatóság, így többek között:

   i. a 2013/36/EU irányelv VII. címének 4. fejezete vagy az 575/2013/EU európai parlamenti és tanácsi rendelet ([37]) 458. cikkének (1) bekezdése szerinti kijelölt hatóság;

   ii. az ERKT/2011/3 európai rendszerkockázati testületi ajánlásban ([38]) meghatározott célkitűzésekkel, szabályokkal, feladatokkal, hatáskörökkel, instrumentumokkal, elszámoltathatósági követelményekkel és más jellemzőkkel rendelkező makroprudenciális hatóság;

g) „érintett hatóság”:

   1. valamely európai felügyeleti hatóság;

   2. az EKB az 1024/2013/EU rendelet 4. cikkének (1) és (2) bekezdésével, valamint 5. cikkének (2) bekezdésével összhangban rá ruházott feladatok tekintetében;

   3. valamely érintett nemzeti hatóság.

2. **Végrehajtási kritériumok**

Az ajánlás végrehajtására a következő kritériumok vonatkoznak:

a) megfelelő figyelmet kell fordítani a szükséges ismeret elvére és az arányosság elvére, figyelembe véve az egyes ajánlások célkitűzését és tartalmát;

b) teljesíteni kell az egyes ajánlások tekintetében a mellékletben meghatározott konkrét megfelelési kritériumokat.

3. **Az intézkedések elfogadására vonatkozó határidők**

Az 1092/2010/EU rendelet 17. cikkének(1) bekezdésével összhangban a címzetteknek tájékoztatniuk kell az Európai Parlamentet, a Tanácsot, a Bizottságot és az ERKT-t arról, hogy milyen intézkedéseket hoztak ezen ajánlás nyomán, vagy meg kell indokolniuk az intézkedés mellőzését. A címzettek a következő határidők betartásával nyújthatják be a tájékoztatást:

1. A. ajánlás

   a) Az EFH-knak 2023. június 30-ig, de legkorábban a DORA rendelet hatálybalépését követő hat hónapot követően időközi jelentést kell benyújtaniuk az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és az ERKT-nak az A(1) ajánlás végrehajtásáról.

   b) Az EFH-knak 2024. június 30-ig, de legkorábban a DORA rendelet hatálybalépését követő 18 hónapot követően zárójelentést kell benyújtaniuk az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és az ERKT-nak az A(1) ajánlás végrehajtásáról.

   c) Az EFH-knak 2025. június 30-ig, de legkorábban a DORA rendelet hatálybalépését követő 30 hónapot követően jelentést kell benyújtaniuk az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és az ERKT-nak az A(2) ajánlás végrehajtásáról.

2. B. ajánlás

   Az EFH-knak, az EKB-nak és a tagállamoknak 2023. június 30-ig, de legkorábban a DORA rendelet hatálybalépését követő hat hónapot követően jelentést kell benyújtaniuk az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és az ERKT-nak a B. ajánlás végrehajtásáról.

3. C. ajánlás

   a) A Bizottságnak 2023. december 31-ig, de legkorábban a DORA rendelet hatálybalépését követő 12 hónapot követően jelentést kell benyújtania az Európai Parlamentnek, a Tanácsnak és az ERKT-nak a C. ajánlás végrehajtásáról, tekintettel az EFH-k A(1) ajánlással összefüggő időközi jelentésére.

([37]) Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26) a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).

([38]) Az Európai Rendszerkockázati Testület ERKT/2011/3 ajánlása (2011. december 22.) a nemzeti hatóságok makroprudenciális felhatalmazásáról (HL C 41., 2012.2.14., 1. o.).

b) A Bizottságnak 2025. december 31-ig, de legkorábban a DORA rendelet hatálybalépését követő 36 hónapot követően jelentést kell benyújtania az Európai Parlamentnek, a Tanácsnak és az ERKT-nak a C. ajánlás végrehajtásáról, tekintettel az EFH-k A. ajánlással összefüggő jelentésére.

4. **Nyomon követés és értékelés**

1. Az ERKT titkársága:

a) támogatást nyújt a címzetteknek, biztosítva az összehangolt jelentéstételt és a megfelelő sablonok rendelkezésre bocsátását, és szükség szerint részletezve a meghozandó intézkedésekkel kapcsolatos eljárást és határidőket;

b) ellenőrzi a címzettek által hozott intézkedéseket, kérésükre segítséget nyújt, és az elfogadott intézkedésekről szóló jelentéseket nyújt be az igazgatótanácsnak. Az értékelésre az alábbiak szerint kerül sor:

i. a DORA rendelet hatálybalépését követő 12 hónapon belül az A. és B. ajánlás végrehajtása tekintetében;

ii. a DORA rendelet hatálybalépését követő 18 hónapon belül a C. ajánlás végrehajtása tekintetében;

iii. a DORA rendelet hatálybalépését követő 24 hónapon belül az A. ajánlás végrehajtása tekintetében;

iv. a DORA rendelet hatálybalépését követő 36 hónapon belül az A. ajánlás végrehajtása tekintetében;

v. a DORA rendelet hatálybalépését követő 42 hónapon belül a C. ajánlás végrehajtása tekintetében;

2. Az igazgatótanács értékelni fogja a címzettek által jelentett intézkedéseket és indokolásokat, és adott esetben határozhat úgy, hogy ezt az ajánlást nem tartották be, és a címzettek nem adtak megfelelő indokolást az intézkedés mellőzésére.

Kelt Frankfurt am Mainban, 2021. december 2-án.

az ERKT titkárságának vezetője,
az ERKT igazgatótanácsa nevében
Francesco MAZZAFERRO

MELLÉKLET

AZ AJÁNLÁSOKRA VONATKOZÓ MEGFELELÉSI KRITÉRIUMOK MEGHATÁROZÁSA

A. ajánlás – A rendszerszintű kiberbiztonsági események páneurópai koordinációs keretének (EU-SCICF) létrehozása

Az A(1) ajánlásra a következő megfelelési kritériumok vonatkoznak.

1. A pénzügyi ágazat digitális működési rezilienciájáról szóló jövőbeli európai parlamenti és tanácsi rendeletben (a továbbiakban: DORA rendelet) előirányzott hatáskör gyakorlása révén az EU-SCICF fokozatos fejlesztését magában foglaló, eredményes, koordinált uniós szintű elhárítás előkészítése során az európai felügyeleti hatóságoknak (EFH-k) a vegyes bizottságon keresztül, valamint az Európai Központi Bankkal (EKB), az Európai Rendszerkockázati Testülettel (ERKT) és az érintett nemzeti hatóságokkal együtt, és szükség esetén az Európai Uniós Hálózat- és Információbiztonsági Ügynökséggel és a Bizottsággal konzultálva meg kell fontolniuk legalább a következő szempontoknak az EU-SCICF tervezett előkészítése során történő figyelembevételét:

   a. az EU-SCICF hatékony fejlesztéséhez szükséges erőforrásigények elemzése;

   b. kibertámadási forgatókönyveket magában foglaló válságkezelési és vészhelyzeti gyakorlatok kidolgozása a kommunikációs csatornák kialakítása céljából;

   c. közös szószedet kidolgozása;

   d. a kiberbiztonsági események egységes osztályozásának kidolgozása;

   e. biztonságos és megbízható információmegosztási csatornák létrehozása, ideértve a tartalékrendszereket is;

   f. kapcsolattartó pontok létrehozása;

   g. az információmegosztás keretében a titoktartás kezelése;

   h. együttműködési és információmegosztási kezdeményezések a pénzügyi szektor kiberfelderítésével;

   i. hatékony aktiválási és eszkalációs eljárások kidolgozása helyzetismeret segítségével;

   j. a keret résztvevői felelősségi körének pontosítása;

   k. interfészek kialakítása az ágazatközi és – adott esetben – harmadik országok közötti koordinációhoz;

   l. az érintett hatóságok nyilvánosság felé irányuló egységes kommunikációjának biztosítása a bizalom megőrzése érdekében;

   m. előre meghatározott kommunikációs csatornák létrehozása az időben történő kommunikációhoz;

   n. megfelelő kerettesztelési gyakorlatok elvégzése, ideértve az országok közötti tesztelést és a harmadik országokkal való koordinációt, valamint a tanulságok levonását és a keret fejlődését eredményező értékeléseket;

   o. hatékony kommunikáció és a dezinformáció elleni intézkedések biztosítása.

B. ajánlás – Az EU-SCICF kapcsolattartó pontok létrehozása

A B. ajánlásra a következő megfelelési kritériumok vonatkoznak.

1. Az EFH-knak, az EKB-nak és az érintett nemzeti hatóságaik között az egyes tagállamoknak meg kell állapodniuk az EU-SCICF kijelölt kapcsolattartó pontjait felsoroló lista megosztására és naprakészen tartására vonatkozó közös megközelítésben.

2. Értékelni kell a kapcsolattartó pont kijelölését, figyelembe véve a tagállamok által az (EU) 2016/1148 irányelv alapján a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására a más tagállamokkal és a kiberbiztonsági együttműködési csoporttal való, határokon átnyúló együttműködés biztosítása érdekében kijelölt egyedüli kapcsolattartó pontokat.

C. ajánlás – Az uniós jogi keret módosítása

A C. ajánlásra a következő megfelelési kritérium vonatkozik.

A Bizottságnak mérlegelnie kell, hogy az A. ajánlásnak megfelelően elvégzett elemzés eredményeként szükség van-e intézkedésekre, ideértve a vonatkozó uniós jogszabályok módosítását is, annak biztosítása érdekében, hogy az EFH-k a vegyes bizottságon keresztül, az EKB-val, az ERKT-val és az érintett nemzeti hatóságokkal közösen az A(1) alajánlásnak megfelelően kidolgozhassák az EU-SCICF-et, valamint annak biztosítása érdekében, hogy az EFH-k, az EKB, az ERKT és az érintett nemzeti hatóságok, valamint más hatóságok koordinálni tudjanak és kellően részletes és következetes információcserét folytathassanak az eredményes EU-SCICF támogatásához.