2024/1772

2024.6.25.

A BIZOTTSÁG (EU) 2024/1772 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2024. március 13.)

az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-vonatkozású események és kiberfenyegetések osztályozására vonatkozó kritériumokat, a lényegességi küszöbértékeket és a jelentős eseményekkel kapcsolatos bejelentések részleteit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel 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 szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 18. cikke (4) bekezdésének harmadik albekezdésére,

mivel:

(1) Az (EU) 2022/2554 rendelet célja, hogy harmonizálja és észszerűsítse a hitelintézeteket, a pénzforgalmi intézményeket, a számlainformációs szolgáltatókat és az elektronikuspénz-kibocsátó intézményeket érintő IKT-vonatkozású, valamint a pénzforgalmi vonatkozású működési vagy biztonsági eseményekre (a továbbiakban: események) vonatkozó bejelentési követelményeket. Tekintettel arra, hogy a bejelentési követelmények 20 különböző típusú pénzügyi szervezetre vonatkoznak, a jelentős események és a jelentős kiberfenyegetések meghatározására szolgáló osztályozási kritériumokat és lényegességi küszöbértékeket egyszerű, harmonizált és egységes módon kell meghatározni, figyelembe véve valamennyi érintett pénzügyi szervezet szolgáltatásainak és tevékenységeinek sajátosságait.

(2) Az arányosság biztosítása érdekében az osztályozási kritériumoknak és a lényegességi küszöbértékeknek tükrözniük kell valamennyi pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásainak jellegét, nagyságrendjét és összetettségét. Ezenkívül a kritériumokat és a lényegességi küszöbértékeket úgy kell kialakítani, hogy méretüktől és kockázati profiljuktól függetlenül valamennyi pénzügyi szervezetre következetesen alkalmazandók legyenek, és ne jelentsenek aránytalan bejelentési terhet a kisebb pénzügyi szervezetek számára. Azon helyzetek kezelése érdekében azonban, amikor jelentős számú ügyfelet érint egy olyan esemény, amely önmagában nem haladja meg az alkalmazandó küszöbértéket, abszolút küszöbértéket kell meghatározni, amely elsősorban a nagyobb pénzügyi szervezetekre irányul.

(3) Az (EU) 2022/2554 rendelet hatálybalépése előtt meglévő eseménybejelentési keretekkel kapcsolatban biztosítani kell a folytonosságot a pénzügyi szervezetek számára. Ezért az osztályozási kritériumokat és a lényegességi küszöbértékeket össze kell hangolni az Európai Bankhatóságnak (a továbbiakban: EBH) az (EU) 2366/2015 európai parlamenti és tanácsi irányelv ([2]) szerinti, a jelentős események bejelentéséről szóló iránymutatásaival, a kereskedési adattárak által az ESMA-nak benyújtandó, az időszakos tájékoztatásról és a lényeges változásokról szóló értesítésről szóló iránymutatással, az EKB/SSM kiberbiztonsági eseményekre vonatkozó adatszolgáltatási keretrendszerével és más vonatkozó iránymutatásokkal, valamint azokból kell meríteni. Az osztályozási kritériumoknak és küszöbértékeknek megfelelőeknek kell lenniük azon pénzügyi szervezetek számára is, amelyek az (EU) 2022/2554 rendelet előtt nem tartoztak az események bejelentésére vonatkozó követelmények hatálya alá.

(4) Ami az „érintett ügyletek összege vagy száma” osztályozási kritériumot illeti, az ügyletek fogalma tág, és magában foglalja a pénzügyi szervezetekre alkalmazandó ágazati jogi aktusok különböző tevékenységeit és szolgáltatásait. Ezen osztályozási kritérium alkalmazásában a fizetési műveletekre és a pénzügyi eszközök, kriptoeszközök, áruk vagy bármely más eszköz – letét, biztosíték vagy zálogkölcsön formájában történő – cseréjének minden formájára ki kell terjednie, mind készpénz, mind pedig bármely más eszköz ellenében. Az osztályozás szempontjából minden olyan ügyletet figyelembe kell venni, amely olyan eszközöket érint, amelyek értéke pénzben kifejezhető.

([1]) HL L 333., 2022.12.27., 1. o. ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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 az 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o., ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Az osztályozási kritériumoknak biztosítaniuk kell, hogy a jelentős események valamennyi releváns típusát figyelembe vegyék. A hálózati vagy információs rendszerekbe való behatolással kapcsolatos kibertámadásokat számos osztályozási kritérium nem feltétlenül fedi le. Ezek azonban fontosak, mivel a hálózati és információs rendszerekbe való bármilyen behatolás kárt okozhat a pénzügyi szervezetnek. Ennek megfelelően az „érintett kritikus szolgáltatások" és az „adatvesztések" osztályozási kritériumait úgy kell meghatározni, hogy azok magukban foglalják az ilyen típusú jelentős eseményeket, különösen az illetéktelen behatolásokat, amelyek – még ha a hatások nem is azonnal ismertek – súlyos következményekhez, különösen adatvédelmi incidensekhez és adatszivárgásokhoz vezethetnek.

(6) Mivel a hitelintézetekre mind az eseményeknek az (EU) 2022/2554 rendelet 18. cikke szerinti osztályozási keretrendszere, mind az (EU) 2018/959 felhatalmazáson alapuló bizottsági rendelet ([3]) szerinti működési kockázati keret vonatkozik, a költségek és veszteségek kiszámításán alapuló, az események gazdasági hatásának értékelésére szolgáló megközelítésnek a lehető legnagyobb mértékben egységesnek kell lennie mindkét keretrendszerben, az összeegyeztethetetlen vagy egymásnak ellentmondó követelmények bevezetésének elkerülése érdekében.

(7) Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének c) pontjában meghatározott, az esemény földrajzi kiterjedésére vonatkozó kritériumnak az esemény határokon átnyúló hatására kell összpontosítania, mivel az eseménynek az adott joghatóságon belüli pénzügyi szervezet tevékenységeire gyakorolt hatását az említett cikkben meghatározott egyéb kritériumok fogják figyelembe venni.

(8) Tekintettel arra, hogy az osztályozási kritériumok összefüggenek egymással és kapcsolódnak egymáshoz, az (EU) 2022/2554 rendelet 19. cikkének (1) bekezdésével összhangban bejelentendő jelentős események azonosítására szolgáló megközelítésnek kritériumok kombinációján kell alapulnia úgy, hogy az IKT-vonatkozású eseménynek és a jelentős IKT-vonatkozású eseménynek az (EU) 2022/2554 rendelet 3. cikkének (8) és (10) bekezdésében meghatározott fogalommeghatározásaihoz szorosan kapcsolódó egyes kritériumoknak más kritériumoknál nagyobb hangsúlyt kell kapniuk a jelentős események osztályozásában.

(9) Annak biztosítása érdekében, hogy az illetékes hatóságok által az (EU) 2022/2554 rendelet 19. cikkének (1) bekezdése alapján a jelentős eseményekről kapott bejelentések és értesítések mind felügyeleti célokat, mind pedig a pénzügyi szektoron belüli fertőzés megelőzését szolgálják, a lényegességi küszöbértékeknek lehetővé kell tenniük a jelentős események azonosítását, többek között a szervezetspecifikus kritikus szolgáltatásokra gyakorolt hatásra, az ügyfelek vagy pénzügyi partnerek egyedi abszolút és relatív küszöbértékeire, a pénzügyi szervezetre gyakorolt lényeges hatást jelző ügyletekre, valamint a más tagállamokban gyakorolt hatás jelentőségére összpontosítva.

(10) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat vagy hálózati és információs rendszereket, illetve engedélyköteles pénzügyi szolgáltatásokat érintő eseményeket, továbbá a kritikus vagy fontos funkciókat támogató hálózati és információs rendszerekhez való rosszindulatú illetéktelen hozzáférést a pénzügyi szervezetek kritikus szolgáltatásait érintő eseményeknek kell tekinteni. A pénzügyi szervezetek kritikus vagy fontos funkcióit támogató hálózati és információs rendszerekhez való rosszindulatú illetéktelen hozzáférés súlyos kockázatot jelent a pénzügyi szervezet számára, és mivel más pénzügyi szervezeteket is érinthet, mindig bejelentendő jelentős eseménynek kell tekinteni.

(11) Az olyan ismétlődő események, amelyek hasonló nyilvánvaló kiváltó ok miatt kapcsolódnak egymáshoz, és amelyek önmagukban nem minősülnek jelentős eseménynek, jelentős hiányosságokra és gyengeségekre utalhatnak a pénzügyi szervezet esemény- és kockázatkezelési eljárásaiban. Ezért az ismétlődő eseményeket együttesen jelentősnek kell tekinteni, ha egy bizonyos időszak alatt ismétlődően előfordulnak.

(12) Tekintettel arra, hogy a kiberfenyegetések negatív hatást gyakorolhatnak a pénzügyi szervezetre és ágazatra, a pénzügyi szervezetek által a jelentős kiberfenyegetésekkel kapcsolatban tett bejelentéseknek jelezniük kell a bekövetkezés valószínűségét és a lehetséges hatás kritikusságát. Ennek megfelelően a kiberfenyegetések jelentőségének egyértelmű és következetes értékelése érdekében a kiberfenyegetés jelentősnek minősítésének egyrészt annak valószínűségétől kell függenie, hogy a fenyegetés bekövetkezése esetén a jelentős eseményekre vonatkozó osztályozási kritériumok teljesülnének-e és azok küszöbértékét elérnék-e, másrészt a kiberfenyegetés típusától és a pénzügyi szervezet rendelkezésére álló információktól.

([3]) A Bizottság (EU) 2018/959 felhatalmazáson alapuló rendelete (2018. március 14.) az 575/2013/EU európai parlamenti és tanácsi rendeletnek a működési kockázatra vonatkozó, intézmények által alkalmazott fejlett mérési módszerek illetékes hatóság általi engedélyezése során használt értékelési módszertan meghatározása tekintetében történő kiegészítéséről (HL L 169., 2018.7.6., 1. o., ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Tekintettel arra, hogy más tagállamok illetékes hatóságait értesíteni kell a joghatóságuk alá tartozó pénzügyi szervezeteket és ügyfeleket érintő eseményekről, az (EU) 2022/2554 rendelet 19. cikkének (7) bekezdésével összhangban egy másik joghatóságra gyakorolt hatás értékelésének a következőkön kell alapulnia: az esemény kiváltó oka, a harmadik fél szolgáltatókon és a pénzügyi piaci infrastruktúrákon keresztüli lehetséges átterjedés, valamint az eseménynek az ügyfelek vagy pénzügyi partnerek jelentős csoportjaira gyakorolt hatása.

(14) Az (EU) 2022/2554 rendelet 19. cikkének (6) és (7) bekezdésében említett bejelentési és értesítési eljárásoknak lehetővé kell tenniük az érintett címzettek számára az események hatásának értékelését. Ezért a közölt információknak ki kell terjedniük a pénzügyi szervezet által az illetékes hatóságnak benyújtott eseménybejelentésekben szereplő valamennyi részletre.

(15) Amennyiben egy esemény az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([4]) és a 2002/58 európai parlamenti és tanácsi irányelv ([5]) szerinti adatvédelmi incidensnek minősül, ez a rendelet nem érintheti a személyes adatok megsértésére vonatkozóan az említett uniós jogszabályokban meghatározott rögzítési és értesítési kötelezettségeket. Az illetékes hatóságoknak minden releváns kérdésben együtt kell működniük és információt kell cserélniük az (EU) 2016/679 rendeletben és a 2002/58/EK irányelvben említett hatóságokkal.

(16) Ez a rendelet az európai felügyeleti hatóságok által az Európai Uniós Kiberbiztonsági Ügynökséggel (a továbbiakban: ENISA) és az Európai Központi Bankkal (a továbbiakban: EKB) konzultálva a Bizottsághoz benyújtott szabályozástechnikai standardtervezeteken alapul.

(17) Az 1093/2010/EU európai parlamenti és tanácsi rendelet ([6]) 54. cikkében, az 1094/2010/EU európai parlamenti és tanácsi rendelet ([7]) 54. cikkében, valamint az 1095/2010/EU európai parlamenti és tanácsi rendelet ([8]) 54. cikkében említett, európai felügyeleti hatóságok vegyes bizottsága nyilvános konzultációt folytatott az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezte a javasolt standardok esetleges költségeit és hasznát, továbbá kikérte az 1093/2010/EU rendelet 37. cikkével összhangban létrehozott Banki Érdekképviseleti Csoport, az 1094/2010/EU rendelet 37. cikkével összhangban létrehozott Biztosítási és Viszontbiztosítási Érdekképviseleti Csoport és a Foglalkoztatói-nyugdíj Érdekképviseleti Csoport, valamint az 1095/2010/EU rendelet 37. cikkével összhangban létrehozott Értékpapírpiaci Érdekképviseleti Csoport tanácsát.

([4]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)(HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)(HL L 201., 2002.7.31., 37. o., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 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., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Az Európai Parlament és a Tanács 1095/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Értékpapírpiaci 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., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([9]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2024. január 24-én véleményt nyilvánított.

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

OSZTÁLYOZÁSI KRITÉRIUMOK

1. cikk

Ügyfelek, pénzügyi partnerek és ügyletek

(1) Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének a) pontjában említett, az esemény által érintett ügyfelek száma az összes olyan érintett – természetes vagy jogi személy – ügyfél számát tükrözi, aki vagy amely nem tudja vagy tudta igénybe venni a pénzügyi szervezet által nyújtott szolgáltatást az esemény során, illetve akit vagy amelyet az esemény hátrányosan érintett. Ez a szám magában foglalja azokat a harmadik feleket is, amelyekre a pénzügyi szervezet és az ügyfél mint az érintett szolgáltatás kedvezményezettje közötti szerződéses megállapodás kifejezetten vonatkozik.

(2) Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének a) pontjában említett, az esemény által érintett pénzügyi partnerek száma azon érintett pénzügyi partnerek számát tükrözi, amelyek szerződéses megállapodást kötöttek a pénzügyi szervezettel.

(3) Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének a) pontjában említett, az esemény által érintett ügyfelek és pénzügyi partnerek relevanciájával kapcsolatban a pénzügyi szervezet figyelembe veszi, hogy az ügyfélre vagy pénzügyi partnerre gyakorolt hatás milyen mértékben befolyásolja a pénzügyi szervezet üzleti célkitűzéseinek megvalósítását, valamint az esemény piaci hatékonyságra gyakorolt lehetséges hatását.

(4) Az esemény által érintett ügyleteknek az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének a) pontjában említett összege vagy száma tekintetében a pénzügyi szervezet figyelembe veszi az összes olyan érintett ügyletet, amely pénzösszeget érint, amennyiben az ügylet legalább egy részét az Unióban hajtják végre.

(5) Amennyiben az érintett ügyfelek vagy pénzügyi partnerek tényleges száma vagy az érintett ügyletek tényleges száma vagy összege nem határozható meg, a pénzügyi szervezet ezeket a számokat vagy összegeket az összehasonlítható referencia-időszakokból származó, rendelkezésre álló adatok alapján megbecsüli.

2. cikk

A hírnevet érintő hatás

(1) Az eseménynek az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének a) pontjában említett, a hírnevet érintő hatásának meghatározása céljából a pénzügyi szervezetek akkor tekintik úgy, hogy az esemény a hírnevet érintő hatással jár, ha az alábbi kritériumok közül legalább egy teljesül:

a) az esemény megjelent a sajtóban;

b) az esemény különböző ügyfelektől vagy pénzügyi partnerektől ismétlődő panaszokat eredményezett az ügyfeleknek nyújtott személyes szolgáltatások vagy a kritikus üzleti kapcsolatok vonatkozásában;

c) a pénzügyi szervezet az esemény következtében nem lesz képes vagy valószínűsíthetően nem lesz képes teljesíteni a szabályozási követelményeket;

d) a pénzügyi szervezet az esemény következtében elveszíti vagy valószínűleg elveszíti az üzleti tevékenységére jelentős hatást gyakorló ügyfeleit vagy pénzügyi partnereit.

([9]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(2) Az esemény hírnevet érintő hatásának értékelésekor a pénzügyi szervezetek figyelembe veszik az esemény láthatóságának szintjét, amelyet az esemény az (1) bekezdésben felsorolt minden egyes kritérium tekintetében elért vagy várhatóan el fog érni.

3. cikk

Időtartam és leállási idő

(1) A pénzügyi szervezetek az eseménynek az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének b) pontjában említett időtartamát az esemény bekövetkezésének pillanatától a megoldás időpontjáig mérik.

Amennyiben a pénzügyi szervezetek nem tudják meghatározni az esemény bekövetkezésének időpontját, az esemény észlelésétől számítva mérik annak időtartamát. Amennyiben a pénzügyi szervezetek tudomást szereznek arról, hogy az esemény az észlelést megelőzően következett be, az esemény hálózati vagy rendszernaplókban vagy más adatforrásokban való rögzítésétől számítva mérik az időtartamot.

Amennyiben a pénzügyi szervezetek még nem tudják, hogy az esemény mikor lesz megoldva, vagy nem tudják ellenőrizni a naplókban vagy más adatforrásokban szereplő bejegyzéseket, becsléseket alkalmaznak.

(2) A pénzügyi szervezetek az eseménynek az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének b) pontjában említett leállási idejét attól a pillanattól kezdve mérik, hogy a szolgáltatás teljesen vagy részben nem érhető el az ügyfelek, a pénzügyi partnerek vagy más belső vagy külső felhasználók számára, addig a pillanatig, amikor a rendszeres tevékenységeket vagy műveleteket visszaállították az eseményt megelőzően biztosított szolgáltatási szintre. Amennyiben a leállási idő a rendszeres tevékenységek vagy műveletek visszaállítását követően késlelteti a szolgáltatásnyújtást, a leállási időt az esemény kezdetétől addig a pillanatig kell mérni, amikor a késleltetést szenvedett szolgáltatás ismét teljeskörűen nyújtható.

Amennyiben a pénzügyi szervezetek nem tudják meghatározni a leállás kezdetének időpontját, a leállás észlelésétől számítva mérik annak időtartamát.

4. cikk

Földrajzi kiterjedés

Az esemény által érintett területek földrajzi kiterjedésének az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének c) pontjában említett meghatározása céljából a pénzügyi szervezetek értékelik, hogy az esemény hatással van vagy volt-e más tagállamokban és különösen a hatás jelentőségét az alábbiak bármelyike tekintetében:

a) ügyfelek és pénzügyi partnerek más tagállamokban;

b) a csoporton belüli, más tagállamokban tevékenységet folytató fióktelepek vagy egyéb pénzügyi szervezetek;

c) pénzügyi piaci infrastruktúrák vagy harmadik fél szolgáltatók, amelyek hatással lehetnek olyan más tagállamokban lévő pénzügyi szervezetekre, amelyeknek szolgáltatásokat nyújtanak, amennyiben ilyen információk rendelkezésre állnak.

5. cikk

Adatvesztések

Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének d) pontjában említett, az esemény által okozott adatveszteségek meghatározása céljából a pénzügyi szervezetek figyelembe veszik a következőket:

a) az adatok rendelkezésre állásával kapcsolatban azt, hogy az esemény ideiglenesen vagy tartósan hozzáférhetetlenné vagy használhatatlanná tette-e a pénzügyi szervezet, annak ügyfelei vagy partnerei által igényelt adatokat;

b) az adatok hitelességével kapcsolatban azt, hogy az esemény veszélyeztette-e az adatforrás megbízhatóságát;

c) az adatok integritásával kapcsolatban azt, hogy az esemény az adatok engedély nélküli módosítását eredményezte-e, ami pontatlanná vagy hiányossá tette azokat;

d) az adatok bizalmas jellegét illetően azt, hogy az esemény eredményeként hozzáférhetett-e az adatokhoz illetéktelen fél vagy rendszer, vagy közölték-e azokat illetéktelen féllel vagy rendszerrel.

6. cikk

Az érintett szolgáltatások kritikussága

Az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének e) pontjában említett, érintett szolgáltatások kritikusságának meghatározása céljából a pénzügyi szervezetek értékelik, hogy az esemény:

a) érinti vagy érintette-e a pénzügyi szervezet kritikus vagy fontos funkcióit támogató IKT-szolgáltatásokat, vagy hálózati és információs rendszereket;

b) érint vagy érintett-e a pénzügyi szervezet által nyújtott olyan pénzügyi szolgáltatásokat, amelyek engedélyhez vagy nyilvántartásba vételhez kötöttek, vagy amelyek az illetékes hatóságok felügyelete alá tartoznak;

c) sikeres, rosszindulatú és illetéktelen hozzáférést eredményez vagy eredményezett-e a pénzügyi szervezet hálózati és információs rendszereihez.

7. cikk

Gazdasági hatás

(1) Az eseménynek az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének f) pontjában említett gazdasági hatása meghatározása céljából a pénzügyi szervezetek figyelembe veszik – a megtérülések beszámítása nélkül – az esemény következtében felmerült közvetlen és közvetett költségek és veszteségek következő típusait:

a) kisajátított pénzeszközök vagy pénzügyi eszközök, amelyekért felelősséggel tartoznak, beleértve az eltulajdonított eszközöket is;

b) szoftver, hardver vagy infrastruktúra cseréjével, vagy áthelyezésével kapcsolatos költségek;

c) személyzeti költségek, beleértve a személyzet leváltásával vagy áthelyezésével, a további személyzet felvételével, a túlóra díjazásával és az elveszített vagy kárt szenvedett készségek helyreállításával kapcsolatos költségeket;

d) a szerződéses kötelezettségek be nem tartásából eredő díjak;

e) az ügyfeleknek nyújtott jogorvoslat és kártérítés költségei;

f) elmaradt bevételekből eredő veszteségek;

g) a belső és külső kommunikációval kapcsolatos költségek;

h) tanácsadási költségek, beleértve a jogi tanácsadással, az igazságügyi szakértői szolgáltatásokkal és a korrekciós szolgáltatásokkal kapcsolatos költségeket.

(2) Az (1) bekezdésben említett költségek és veszteségek nem foglalják magukban az üzleti tevékenység napi működéséhez szükséges költségeket, különösen a következőket:

a) az infrastruktúra, a berendezések, a hardverek és a szoftverek általános karbantartásának költségei, valamint a személyzet készségeinek naprakészen tartásával kapcsolatos költségek;

b) a biztonsági esemény bekövetkezését követően az üzleti tevékenység megerősítésére irányuló belső vagy külső kiadások, beleértve a fejlesztéseket, a javításokat és a kockázatértékelési kezdeményezéseket;

c) biztosítási díjak.

(3) A pénzügyi szervezetek az adatszolgáltatás időpontjában rendelkezésre álló adatok alapján számítják ki a költségek és veszteségek összegét. Amennyiben a költségek és veszteségek tényleges összege nem határozható meg, a pénzügyi szervezetek megbecsülik ezeket az összegeket.

(4) Az esemény gazdasági hatásának értékelésekor a pénzügyi szervezetek összesítik az (1) bekezdésben említett költségeket és veszteségeket.

II. FEJEZET

JELENTŐS ESEMÉNYEK ÉS LÉNYEGESSÉGI KÜSZÖBÉRTÉKEK

8. cikk

Jelentős események

(1) Egy esemény akkor minősül az (EU) 2022/2554 rendelet 19. cikke (1) bekezdésének alkalmazásában jelentős eseménynek, ha érintette a 6. cikkben említett kritikus szolgáltatásokat, és ha az alábbi feltételek bármelyike teljesül:

a) a 9. cikk (5) bekezdésének b) pontjában említett lényegességi küszöbértéket elérik;

b) a 9. cikk (1)–(6) bekezdésében említett egyéb lényegességi küszöbértékek közül kettőt vagy többet elérnek.

(2) Azokat az ismétlődő eseményeket, amelyek egyenként nem minősülnek az (1) bekezdés szerinti jelentős eseménynek, egyetlen jelentős eseménynek kell tekinteni, amennyiben megfelelnek az alábbi feltételek mindegyikének:

a) 6 hónapon belül legalább kétszer előfordultak;

b) az (EU) 2022/2554 rendelet 20. cikkének első albekezdésének b) pontjában említett nyilvánvaló kiváltó okuk azonos;

c) együttesen teljesítik az (1) bekezdésben meghatározott azon kritériumokat, amelyek alapján jelentős eseménynek minősülnek.

A pénzügyi szervezetek havonta értékelik az ismétlődő események előfordulását.

Ez a bekezdés nem alkalmazandó a mikrovállalkozásokra és az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében felsorolt pénzügyi szervezetekre.

9. cikk

A jelentős események meghatározásához szükséges lényegességi küszöbértékek

(1) Az „ügyfelek, pénzügyi partnerek és ügyletek” kritérium lényegességi küszöbértékét akkor érik el, ha az alábbi feltételek bármelyike teljesül:

a) az érintett ügyfelek száma meghaladja az érintett szolgáltatást igénybe vevő összes ügyfél 10 %-át;

b) az érintett szolgáltatást igénybe vevő érintett ügyfelek száma meghaladja a 100 000-et;

c) az érintett pénzügyi partnerek száma meghaladja az érintett szolgáltatás nyújtásához kapcsolódó tevékenységeket végző összes pénzügyi partner 30 %-át;

d) az érintett ügyletek száma meghaladja a pénzügyi szervezet által az érintett szolgáltatással kapcsolatban végrehajtott ügyletek napi átlagos számának 10 %-át;

e) az érintett ügyletek száma meghaladja a pénzügyi szervezet által az érintett szolgáltatással kapcsolatban végrehajtott ügyletek napi átlagos értékének 10 %-át;

f) az 1. cikk (3) bekezdésével összhangban relevánsnak minősített ügyfelek vagy pénzügyi partnerek érintettek.

Amennyiben az érintett ügyfelek vagy pénzügyi partnerek tényleges száma vagy az érintett ügyletek tényleges száma vagy összege nem határozható meg, a pénzügyi szervezet ezeket a számokat vagy összegeket az összehasonlítható referencia-időszakokból származó, rendelkezésre álló adatok alapján megbecsüli.

(2) „A hírnevet érintő hatás” kritérium lényegességi küszöbértékét akkor érik el, ha a 2. cikk a)–d) pontjában meghatározott feltételek bármelyike teljesül.

(3) Az „ügyfelek, pénzügyi partnerek és ügyletek” kritérium lényegességi küszöbértékét akkor érik el, ha az alábbi feltételek bármelyike teljesül:

a) az esemény időtartama meghaladja a 24 órát;

b) a leállási idő meghaladja a 2 órát a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások esetében.

(4) A „földrajzi kiterjedés” kritérium lényegességi küszöbértékét akkor érik el, ha az esemény a 4. cikkel összhangban két vagy több tagállamban fejt ki hatást.

(5) Az „adatvesztés” kritérium lényegességi küszöbértékét akkor érik el, ha az alábbi feltételek bármelyike teljesül:

a) az 5. cikkben említett, az adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére gyakorolt hatás hátrányosan érinti vagy fogja érinteni a pénzügyi szervezet üzleti célkitűzéseinek megvalósítását vagy a szabályozási követelményeknek való megfelelésre való képességét;

b) az a) pont hatálya alá nem tartozó sikeres, rosszindulatú és illetéktelen hozzáférés történik olyan hálózati és információs rendszerekhez, ahol ez a hozzáférés adatvesztéshez vezethet.

(6) A „gazdasági hatás” kritériumának lényegességi küszöbértékét akkor érik el, ha a pénzügyi szervezetnél az esemény következtében felmerült költségek és veszteségek meghaladták vagy valószínűleg meghaladják a 100 000 EUR-t.

III. FEJEZET

JELENTŐS KIBERFENYEGETÉSEK

10. cikk

Magas lényegességi küszöbértékek a jelentős kiberfenyegetések meghatározásához

Az (EU) 2022/2554 rendelet 18. cikke (2) bekezdésének alkalmazásában a kiberfenyegetés akkor minősül jelentősnek, ha az alábbi feltételek mindegyike teljesül:

a) a kiberfenyegetés, ha bekövetkezik, a pénzügyi szervezet rendelkezésére álló információk alapján érintheti vagy érinthette volna a pénzügyi szervezet kritikus vagy fontos funkcióit, vagy érinthet más pénzügyi szervezeteket, harmadik fél szolgáltatókat, ügyfeleket vagy pénzügyi partnereket;

b) a kiberfenyegetés nagy valószínűséggel bekövetkezik a pénzügyi szervezetnél vagy más pénzügyi szervezeteknél, figyelembe véve legalább a következő elemeket:

   i. az a) pontban említett kiberfenyegetéssel kapcsolatos alkalmazandó kockázatok, beleértve a pénzügyi szervezet rendszereinek potenciálisan kiaknázható sebezhetőségeit is;

   ii. a fenyegető szereplők képességei és szándéka, amennyiben azok a pénzügyi szervezet számára ismertek;

   iii. a fenyegetés tartóssága és a pénzügyi szervezetet vagy annak harmadik fél szolgáltatóját, ügyfeleit vagy pénzügyi partnereit érintő biztonsági eseményekkel kapcsolatban szerzett ismeretek;

c) a kiberfenyegetés – bekövetkezése esetén – az alábbiak bármelyikének megfelelhet:

   i. a szolgáltatások kritikusságára vonatkozó, az (EU) 2022/2554 rendelet 18. cikke (1) bekezdésének e) pontjában meghatározott kritérium, az e rendelet 6. cikkében meghatározottak szerint;

   ii. a 9. cikk (1) bekezdésében meghatározott lényegességi küszöbérték;

   iii. a 9. cikk (4) bekezdésében meghatározott lényegességi küszöbérték.

Amennyiben a kiberfenyegetés típusától és a rendelkezésre álló információktól függően a pénzügyi szervezet arra a következtetésre jut, hogy a 9. cikk (2), (3), (5) és (6) bekezdésében meghatározott lényegességi küszöbértékeket elérhetik, ezeket a küszöbértékeket is figyelembe lehet venni.

IV. FEJEZET

A JELENTŐS ESEMÉNYEK RELEVANCIÁJA MÁS TAGÁLLAMOK ILLETÉKES HATÓSÁGAI SZÁMÁRA ÉS A MÁS ILLETÉKES HATÓSÁGOKKAL MEGOSZTANDÓ BEJELENTÉSEK RÉSZLETEI

11. cikk

A jelentős események relevanciája más tagállamok illetékes hatóságai számára

Annak értékelése, hogy a jelentős esemény releváns-e más tagállamok illetékes hatóságai számára az (EU) 2022/2554 rendelet 19. cikkének (7) bekezdésében említettek szerint, azon alapul, hogy az eseménynek van-e egy másik tagállamból származó kiváltó oka, vagy hogy az esemény jelentős hatást gyakorol vagy gyakorolt-e egy másik tagállamban az alábbiak bármelyikével kapcsolatban:

a) ügyfelek vagy pénzügyi partnerek;

b) a pénzügyi szervezet fióktelepe vagy a csoporton belüli más pénzügyi szervezet;

c) olyan pénzügyi piaci infrastruktúra vagy harmadik fél szolgáltató, amely érintheti azokat a pénzügyi szervezeteket, amelyeknek szolgáltatásokat nyújt.

12. cikk

A más illetékes hatóságokkal megosztandó jelentős események részletei

Az illetékes hatóságok által az (EU) 2022/2554 rendelet 19. cikkének (6) bekezdésével összhangban a jelentős események részleteivel kapcsolatban más illetékes hatóságoknak benyújtandó információk, valamint az EBH, az ESMA vagy az EIOPA és az EKB által más tagállamok érintett illetékes hatóságainak az említett rendelet 19. cikkének (7) bekezdésével összhangban benyújtandó értesítések – anonimizálás nélkül – ugyanolyan szintű információkat tartalmaznak, mint a pénzügyi szervezetektől az (EU) 2022/2554 rendelet 19. cikkének (4) bekezdésével összhangban kapott, jelentős eseményekre vonatkozó bejelentések és értesítések.

V. FEJEZET

ZÁRÓ RENDELKEZÉSEK

13. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2024. március 13-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN