2025/1190

2025.6.18.

A BIZOTTSÁG (EU) 2025/1190 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2025. február 13.)

az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek a fenyegetés alapú behatolási tesztelés elvégzésére kötelezett pénzügyi szervezetek azonosításához használt kritériumokat, a belső tesztelők igénybevételét szabályozó követelményeket és standardokat, a terjedelemre, a tesztelés egyes szakaszainak tesztelési módszertanára és megközelítésére, az eredményekre, a lezárási és korrekciós szakaszokra vonatkozó követelményeket, valamint a fenyegetés alapú behatolási tesztelés végrehajtásához és a kölcsönös elismerés megkönnyítéséhez szükséges felügyeleti és egyéb releváns együttműködés típusát 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 26. cikke (11) bekezdésének negyedik albekezdésére,

mivel:

(1) Ez a rendelettervezet a TIBER-EU kerettel összhangban készült, és az ott ismertetett fenyegetés alapú behatolási tesztelés (TLPT) módszertanát, folyamatát és szerkezetét tükrözi. A TLPT hatálya alá tartozó pénzügyi szervezetek a TIBER-EU keretre vagy annak valamely nemzeti jogban végrehajtott változatára hivatkozhatnak, és azokat alkalmazhatják, amennyiben a keret vagy annak végrehajtott változata összhangban van az (EU) 2022/2554 rendelet 26. és 27. cikkében, valamint az e rendeletben meghatározott követelményekkel. A pénzügyi ágazatban a TLPT-vel kapcsolatos ügyekért nemzeti szinten felelős egyetlen hatóságnak az (EU) 2022/2554 rendelet 26. cikkének (9) bekezdésével összhangban történő kijelölése nem sértheti az említett rendelet 46. cikkével összhangban valamely illetékes hatóságra, például a TLPT-vel kapcsolatos ügyekben a jelentős hitelintézetek tekintetében illetékesnek tekintendő Európai Központi Bankra ruházott, bizonyos pénzügyi szervezetek felügyeletére vonatkozó, uniós szintű hatáskört. Amennyiben a TLPT-kkel kapcsolatos feladatoknak csak egy részét ruházzák át az (EU) 2022/2554 rendelet 26. cikkének (10) bekezdése alapján egy másik nemzeti hatóságra a pénzügyi szektorban, a TLPT-vel kapcsolatos át nem ruházott feladatok tekintetében a pénzügyi szervezet a szóban forgó rendelet 46. cikkében említett illetékes hatóságának kell maradnia az illetékes hatóságnak.

(2) Figyelembe véve a TLPT összetettségét és a hozzá kapcsolódó kockázatokat, a TLPT alkalmazását azokra a pénzügyi szervezetekre kell korlátozni, amelyek esetében az indokolt. Ezért a TLPT-ügyekért felelős hatóságoknak (TLPT-hatóságok, akár uniós, akár nemzeti szinten) ki kell zárniuk a TLPT hatálya alól az olyan alapvető pénzügyi szolgáltatási alágazatokban működő pénzügyi szervezeteket, amelyek esetében a TLPT nem indokolt. Ez azt jelenti, hogy a hitelintézetek, a pénzforgalmi és elektronikuspénz-kibocsátó intézmények, a központi értéktárak, a központi szerződő felek, a kereskedési helyszínek, a biztosítók és a viszontbiztosítók – annak ellenére, hogy megfelelnek a mennyiségi kritériumoknak – mentesülhetnek a TLPT követelménye alól IKT-kockázati profiljuk és érettségük, a pénzügyi ágazatra gyakorolt hatásuk és a kapcsolódó pénzügyi stabilitási aggályok átfogó értékelése fényében.

(3) A TLPT-hatóságoknak az IKT-kockázati profil és érettség, a pénzügyi ágazatra gyakorolt hatás és a kapcsolódó pénzügyi stabilitási aggályok átfogó értékelése fényében fel kell mérniük, hogy a hitelintézetektől, pénzforgalmi intézményektől, elektronikuspénz-kibocsátó intézményektől, központi szerződő felektől, központi értéktáraktól, kereskedési helyszínektől, biztosítóktól és viszontbiztosítóktól eltérő bármely egyéb típusú pénzügyi szervezeteket TLPT-re kell-e kötelezni. Annak értékelése során, hogy az ilyen pénzügyi szervezetek teljesítik-e ezeket a minőségi kritériumokat, ágazatközi és objektív mutatók alkalmazásával azonosítani kell azokat a pénzügyi szervezeteket, amelyek esetében a TLPT megfelelő. Ugyanakkor annak értékelése eredményeként, hogy valamely pénzügyi szervezet megfelel-e ezeknek a minőségi kritériumoknak, a TLPT-re kötelezett szervezeteket azokra kell korlátozni,

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

amelyek esetében a tesztelés indokolt. Azt, hogy egy pénzügyi szervezet megfelel-e ezeknek a minőségi kritériumoknak, az új piaci fejlemények, valamint az új piaci szereplők – köztük az (EU) 2023/1114 európai parlamenti és tanácsi rendelet ([2]) 59. cikkével összhangban engedélyezett kriptoeszköz-szolgáltatók – pénzügyi ágazatbeli növekvő jelentősége fényében is értékelni kell.

(4) Előfordulhat, hogy a pénzügyi szervezetek ugyanazt a csoporton belüli IKT-szolgáltatót használják, vagy ugyanahhoz a csoporthoz tartoznak, és közös IKT-rendszereket használnak. Ebben az esetben fontos, hogy a TLPT-hatóságok figyelembe vegyék az adott pénzügyi szervezet szerkezetét és rendszerszintű jellegét vagy a pénzügyi ágazat szempontjából fennálló jelentőségét nemzeti vagy uniós szinten annak értékelése során, hogy a pénzügyi szervezetet TLPT-re kell-e kötelezni, és hogy a TLPT-t a szervezet szintjén vagy csoportszinten kell-e elvégezni (közös TLPT-n keresztül).

(5) A tesztelési módszertannak, hogy tükrözze a TIBER-EU keretet, a következő fő résztvevők bevonását kell biztosítania: a pénzügyi szervezet egy ellenőrzést végző csapattal (a TIBER-EU szerinti „ellenőrzést végző csapatot” tükrözve) és egy kék csapattal (a TIBER-EU szerinti „kék csapatot” tükrözve), valamint a TLPT-hatóság egy TLPT-kibercsoport (a TIBER-EU szerinti „TIBER-kibercsoportokat” tükrözve), egy fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató és tesztelők formájában (a tesztelők a TIBER-EU „vörös csapatot biztosító szolgáltatóját” tükrözik).

(6) Annak biztosítása érdekében, hogy a TLPT hasznosítsa a TIBER-EU végrehajtása keretében szerzett tapasztalatokat, valamint a TLPT elvégzésével kapcsolatos kockázatok csökkentése érdekében biztosítani kell, hogy a TLPT-hatóságok szintjén létrehozandó TLPT-kibercsoportok felelősségi köre a lehető legközelebb álljon a TIBER-EU-kibercsoportokéhoz. Ezért a TLPT-kibercsoportoknak tesztvezetőkkel kell rendelkezniük, akik felelősek az egyes TLPT-k felvigyázásáért, valamint az egyes tesztek tervezéséért és koordinálásáért. A TLPT-kibercsoportoknak egyedüli kapcsolattartó pontként kell szolgálniuk a belső és külső érdekelt felekkel a teszteléssel kapcsolatban folytatott kommunikáció, a visszajelzések és a korábban elvégzett tesztekből levont tanulságok összegyűjtése és feldolgozása, valamint azon pénzügyi szervezetek támogatása tekintetében, amelyek éppen TLPT-n esnek át.

(7) A TIBER-EU keret módszertanának tükrözése érdekében a tesztvezetőknek rendelkezniük kell a tanácsadáshoz és a tesztelők javaslatainak kétségbe vonásához szükséges készségekkel és képességekkel. A TIBER-EU keretében szerzett tapasztalatok bebizonyították, hogy hasznos, ha minden egyes teszthez legalább két tesztvezetőből álló csapatot rendelnek. Annak tükrözése érdekében, hogy a TLPT a tanulási tapasztalat ösztönzésére szolgál, valamint a tesztek titkosságának megőrzése érdekében a TLPT-hatóságokat, hacsak nem rendelkeznek erőforrásbeli vagy szakértői problémákkal, határozottan bíztatni kell annak fontolóra vételére, hogy a TLPT időtartama alatt a tesztvezetők ne végezhessenek felügyeleti tevékenységeket a TLPT-re kötelezett ugyanazon pénzügyi szervezetnél.

(8) A TIBER-EU kerettel való összhang érdekében fontos, hogy a TLPT-hatóság annak minden szakaszában szorosan figyelemmel kísérje a tesztelést. Figyelembe véve a tesztelés jellegét és az ahhoz kapcsolódó kockázatokat, alapvető fontosságú, hogy a TLPT-hatóság közreműködjön a tesztelés minden egyes szakaszában. A TLPT-hatósággal különösen a pénzügyi szervezetek azon értékeléseit és döntéseit illetően kell konzultálni, amelyek egyrészt befolyásolhatják a teszt hatékonyságát, másrészt hatással lehetnek a teszthez kapcsolódó kockázatokra, és a hatóságnak az ilyen értékeléseket és döntéseket jóvá kell hagynia. A TLPT-hatóság konkrét közreműködését igénylő alapvető lépések közé tartozik a tesztelés egyes alapvető dokumentációinak, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók és tesztelők kiválasztásának, valamint a kockázatkezelési intézkedéseknek a validálása. A TLPT-hatóságok közreműködése, különösen a validálások tekintetében, nem róhat túlzott terhet e hatóságokra, ezért azokra a dokumentációkra és döntésekre kell korlátozódnia, amelyek közvetlenül érintik a TLPT lefolytatását. A tesztelés egyes szakaszaiban való aktív részvétel révén a TLPT-hatóságok hatékonyan értékelhetik, hogy a pénzügyi szervezetek megfelelnek-e a vonatkozó követelményeknek, aminek lehetővé kell tennie az említett hatóságok számára, hogy az (EU) 2022/2554 rendelet 26. cikkének (7) bekezdése szerinti igazolásokat bocsássanak ki.

([2]) Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete (2023. május 31.) a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról (HL L 150., 2023.6.9., 40. o., ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) A TLPT titkossága rendkívül fontos annak biztosításához, hogy a tesztelés körülményei valósághűek legyenek. Ezért a tesztelésnek titkosnak kell lennie, és óvintézkedéseket kell tenni a TLPT bizalmas jellegének megőrzése érdekében, beleértve az olyan kódnevek kiválasztását, amelyek meggátolják a TLPT harmadik felek általi azonosítását. Amennyiben a pénzügyi csapat biztonságáért felelős személyzet tagjai tudomással bírnak egy tervezett vagy folyamatban lévő TLPT-ről, valószínű, hogy figyelmesebbek és éberebbek lennének, mint rendes munkakörülmények között, ami megváltoztatná a tesztelés eredményét. A pénzügyi szervezet személyzetének ellenőrzést végző csapaton kívüli tagjait ezért csak nyomós okok fennállása esetén és a tesztvezetők előzetes beleegyezésével szabad tájékoztatni valamely tervezett vagy folyamatban lévő TLPT-ről, többek között a teszt titkosságának biztosítása érdekében abban az esetben, ha a tesztet a kék csapat egy tagja észlelte.

(10) Amint azt a TIBER-EU keretében az „ellenőrzést végző csapat” tekintetében gyűjtött tapasztalatok is bizonyítják, a TLPT biztonságos lefolytatásához elengedhetetlen a megfelelő vezető kiválasztása az ellenőrzést végző csapat élére. Az ellenőrzést végző csapat vezetőjének a pénzügyi szervezeten belül rendelkeznie kell a szükséges felhatalmazással ahhoz, hogy a tesztelés valamennyi aspektusát irányítsa, anélkül, hogy ez veszélyeztetné a tesztelés bizalmas jellegét. Ugyanezen okból az ellenőrzést végző csapat tagjainak alapos ismeretekkel kell rendelkezniük a pénzügyi szervezetről, az ellenőrzést végző csapat vezetőjének munkaköréről és stratégiai pozíciójáról, rendelkezniük kell az előírt szolgálati idővel és hozzáféréssel kell rendelkezniük az igazgatótanácshoz. A TLPT veszélyeztetése kockázatának csökkentése érdekében az ellenőrzést végző csapatnak a lehető legkisebbnek kell lennie.

(11) A TLPT-hez szervesen kapcsolódnak kockázatok, mivel a kritikus funkciókat éles környezetben tesztelik, ami szolgáltatásmegtagadási eseményeket, váratlan rendszerleállásokat, a kritikus éles rendszerek károsodását vagy az adatok elvesztését, módosítását vagy közzétételét okozhatja. Ezek a kockázatok rávilágítanak arra, hogy hatékony kockázatkezelési intézkedésekre van szükség. Annak biztosítása érdekében, hogy a TLPT a tesztelés során mindvégig ellenőrzött módon folyjon, nagyon fontos, hogy a pénzügyi szervezetek minden ponton tisztában legyenek a TLPT-vel kapcsolatban felmerülő sajátos kockázatokkal, és hogy e kockázatokat csökkentsék. E tekintetben – a pénzügyi szervezet belső folyamatainak, valamint az ellenőrzést végző csapat vezetőjének már átadott felelősség és felhatalmazás sérelme nélkül – helyénvaló lehet a TLPT kockázatkezelési intézkedéseire vonatkozó információk megosztása a pénzügyi szervezet vezető testületével, vagy adott esetben az említett kockázatkezelési intézkedéseknek e vezető testület általi jóváhagyása. A hatékony és legmagasabb színvonalú szakmai szolgáltatások nyújtása és e kockázatok csökkentése érdekében az is alapvető fontosságú, hogy a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók (együttesen a TLPT-szolgáltatók) a legmagasabb szintű készségekkel, szakértelemmel és megfelelő tapasztalattal rendelkezzenek a fenyegetettséggel kapcsolatos hírszerzés és a TLPT terén a pénzügyi szolgáltatási ágazatban.

(12) A hagyományos behatolási tesztek részletes és hasznos értékelést nyújtanak gyakran egyetlen elszigetelt rendszer vagy környezet műszaki és konfigurációs sérülékenységeiről, de ellentétben a hírszerzésen alapuló, vörös csapat által végzett tesztekkel, nem értékelik az egész szervezet elleni célzott támadás teljes forgatókönyvét, beleértve a szervezet embereinek, folyamatainak és technológiáinak teljes körét. A TLPT-szolgáltatók kiválasztási folyamata során a pénzügyi szervezeteknek ezért biztosítaniuk kell, hogy ezek a szolgáltatók rendelkezzenek ne csak a behatolási tesztek, de a hírszerzésen alapuló, vörös csapat által végzett tesztek elvégzéséhez szükséges készségekkel is. Ezért átfogó kritériumokat kell megállapítani mind a belső, mind a külső tesztelők, valamint a fenyegetettséggel kapcsolatos hírszerzést nyújtó, minden esetben külső szolgáltatók számára. Amennyiben a TLPT-szolgáltatók ugyanahhoz a vállalathoz tartoznak, a TLPT-re kijelölt személyzetet megfelelően el kell különíteni.

(13) Előfordulhatnak olyan kivételes körülmények, amikor a pénzügyi szervezetek nem tudnak az átfogó kritériumoknak megfelelő TLPT-szolgáltatókkal szerződést kötni. Ezért a pénzügyi szervezetek számára lehetővé kell tenni olyan személyek bevonását, akik nem felelnek meg az összes átfogó kritériumnak, amint a számukra nyilvánvalóvá válik, hogy nem állnak rendelkezésre megfelelő fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók, feltéve, hogy megfelelően csökkentik az ebből eredő további kockázatokat, és a TLPT-hatóság értékeli mindezeket a kritériumokat.

(14) Amennyiben a TLPT-ben több pénzügyi szervezet és több TLPT-hatóság vesz részt, meg kell határozni a TLPT-folyamatban részt vevő valamennyi fél szerepét a leghatékonyabb és legbiztonságosabb teszt elvégzése érdekében. A csoportos tesztelés céljából egyedi követelményekre van szükség a kijelölt pénzügyi szervezet szerepének meghatározásához, nevezetesen arra, hogy ez a szervezet legyen felelős az összes szükséges dokumentációnak a vezető TLPT-hatóság rendelkezésére bocsátásáért és a tesztelési folyamat nyomon követéséért. A kijelölt pénzügyi szervezetnek kell felelnie a kockázatkezelési értékelés közös szempontjaiért is. A kijelölt pénzügyi szervezet szerepétől függetlenül a csoportos TLPT-folyamatban részt vevő egyes pénzügyi szervezetek kötelezettségei a csoportos teszt során változatlanok maradnak. Ugyanezt az elvet kell alkalmazni a közös TLPT-kre is.

(15) Amint azt a TIBER-EU keret végrehajtásával kapcsolatos tapasztalatok is bizonyítják, a tesztelés megfelelő elvégzése biztosításának leghatékonyabb módja az összes érintett érdekelt fél (pénzügyi szervezetek, hatóságok, tesztelők és fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók) részvételével tartott személyes vagy virtuális találkozók megtartása. Ezért személyes és virtuális találkozókat kell tartani a folyamat különböző szakaszaiban, különösen az előkészítési szakaszban a TLPT elindításakor és a terjedelmének véglegesítése érdekében, a tesztelési szakaszban a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó jelentés és a vörös csapat által végzett teszt tervének véglegesítése, valamint a heti fejlemények megosztása céljából, valamint a lezárási szakaszban a tesztelők és a kék csapat intézkedéseinek visszajátszása, a közös tesztelés és a TLPT-vel kapcsolatos visszajelzések megosztása céljából.

(16) A TLPT zökkenőmentes elvégzésének biztosítása érdekében a TLPT-hatóságnak egyértelműen be kell mutatnia a pénzügyi szervezet számára a teszteléssel kapcsolatos elvárásait. E tekintetben a tesztvezetőknek biztosítaniuk kell, hogy a pénzügyi szervezeten belül az ellenőrzést végző csapattal és a TLPT-szolgáltatókkal megfelelő információáramlás jöjjön létre.

(17) A pénzügyi szervezetnek ki kell választania azokat a kritikus vagy fontos funkciókat, amelyekre a TLPT kiterjed. E funkciók kiválasztásakor a pénzügyi szervezetnek különböző kritériumokra kell támaszkodnia, amelyek az egyes funkcióknak a pénzügyi szervezet és a pénzügyi ágazat számára uniós és nemzeti szinten betöltött fontosságával kapcsolatosak, nemcsak gazdasági szempontból, hanem a funkció szimbolikus vagy politikai státuszát is figyelembe véve. A fenyegetettséggel kapcsolatos hírszerzési szakaszba való zökkenőmentes átmenet megkönnyítése érdekében az ellenőrzést végző csapatnak részletes információkkal kell ellátnia a terjedelem meghatározására irányuló folyamatban részt nem vevő tesztelőket és fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókat a megállapodás szerinti terjedelemről.

(18) Annak érdekében, hogy a tesztelők számára biztosítva legyenek a pénzügyi szervezet kritikus vagy fontos funkcióit támogató éles rendszerek elleni életszerű és valósághű támadás szimulálásához szükséges információk, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatónak olyan információkat és adatokat kell gyűjtenie, amelyek legalább a két fő érdeklődési területet lefedik: a célpontok, a pénzügyi szervezeten belüli potenciális támadási felületek azonosítása révén, és a fenyegetések, a releváns fenyegető szereplők és a valószínű fenyegetettségi forgatókönyvek azonosítása révén. Annak biztosítása érdekében, hogy a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató a pénzügyi szervezetet érintő releváns fenyegetéseket figyelembe vegye, a tesztelőknek, az ellenőrzést végző csapatnak és a tesztvezetőknek visszajelzést kell adniuk a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó jelentés tervezetéről. Amennyiben rendelkezésre áll, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató a TLPT-hatóság által a tagállam pénzügyi ágazata számára biztosított általános fenyegetettségi helyzetet használhatja kiindulási alapként a nemzeti fenyegetettségi helyzetet illetően. A TIBER-EU keret alkalmazása alapján a fenyegetettséggel kapcsolatos hírszerzés folyamata jellemzően körülbelül 4 hétig tart.

(19) Annak érdekében, hogy a tesztelők betekintést nyerhessenek a terjedelmet meghatározó dokumentumba és a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentésbe, illetve alaposabban felülvizsgálhassák ezeket a vörös csapat által végzett tesztelés tervének véglegesítése érdekében, alapvető fontosságú, hogy a TLPT vörös csapat által végzett tesztelési szakasza előtt a tesztelők részletes magyarázatot kapjanak a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatótól a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentésről és a lehetséges fenyegetettségi forgatókönyvek elemzéséről.

(20) Annak érdekében, hogy a tesztelők valósághű és átfogó tesztelést végezhessenek, amelyben minden támadási fázist végrehajtanak és elérik a tesztcélokat, elegendő időt kell biztosítani a vörös csapat által végzett aktív tesztelési szakaszra. A TIBER-EU kerettel kapcsolatban szerzett tapasztalatok alapján az előirányzott időnek legalább 12 hétnek kell lennie, és azt az érintett felek számának, a TLPT terjedelmének, az érintett pénzügyi szervezet vagy szervezetek erőforrásainak, az esetleges külső követelményeknek és a pénzügyi szervezet által szolgáltatott alátámasztó információk rendelkezésre állásának figyelembevételével kell meghatározni.

(21) A vörös csapat által végzett aktív tesztelési szakaszban a tesztelőknek számos taktikát, módszert és eljárást kell alkalmazniuk a pénzügyi szervezet éles rendszereinek megfelelő tesztelésére. A taktikáknak, módszereknek és eljárásoknak adott esetben tartalmazniuk kell a felderítést (azaz a célponttal kapcsolatos lehető legtöbb információ összegyűjtését), a fegyverként való felhasználást (azaz az infrastruktúrára, a létesítményekre és a munkavállalókra vonatkozó információk elemzését, valamint a célpontra vonatkozó műveletekre való felkészülést), a végrehajtást (azaz a célpontra irányuló teljeskörű művelet aktív elindítását), a sebezhetőségek kihasználását (amennyiben a tesztelők célja a pénzügyi szervezet szervereinek, hálózatainak veszélyeztetése és személyzetének kihasználása pszichológiai manipuláción keresztül), az ellenőrzést és mozgást (azaz kísérlet tételét arra, hogy a már nem biztonságos rendszerekről további sérülékeny vagy nagy értékű rendszerekre jussanak el) és a célponttal kapcsolatos műveleteket (azaz további hozzáférés szerzését a már nem biztonságos rendszerekhez és hozzáférés szerzését a korábban elfogadott célinformációkhoz és -adatokhoz, a vörös csapat által végzett teszt tervében korábban elfogadottak szerint).

(22) A TLPT végrehajtása során a tesztelőknek figyelembe kell venniük a támadás végrehajtására rendelkezésre álló időt, az erőforrásokat, valamint az etikai és jogi korlátokat. Amennyiben a tesztelők nem tudnak továbbhaladni a támadás ütemterv szerinti következő szakaszába, az ellenőrzést végző csapatnak a TLPT-hatóság beleegyezésével eseti támogatást kell nyújtania „kisegítés" formájában. A kisegítések nagy vonalakban az információhoz és a hozzáféréshez kapcsolódó kisegítésként kategorizálhatók, és magukban foglalhatják az IKT-rendszerekhez vagy belső hálózatokhoz való hozzáférés biztosítását a teszt folytatása és a támadás következő lépéseire való összpontosítás érdekében.

(23) A tesztelési szakaszban a vörös csapat által végzett aktív tesztelés során – amennyiben kivételes körülmények között és az összes alternatív lehetőség kimerítését követően végső megoldásként szükséges ahhoz, hogy a TLPT folytatódhasson – együttműködésen alapuló tesztelési tevékenységet kell alkalmazni, amelyben a tesztelők és a kék csapat egyaránt részt vesznek. Az ilyen korlátozott közös teszteléssel összefüggésben a következő módszerek alkalmazhatók: „macska-egér játék", ahol a tesztelők megpróbálják folytatni a forgatókönyveket, észlelik őket, majd folytatják a tesztelést, „háborús játék", amely összetettebb forgatókönyveket tesz lehetővé a stratégiai döntéshozatal teszteléséhez, vagy „együttműködésen alapuló igazoló teszt", amely lehetővé teszi a tesztelők és a kék csapat tagjai számára, hogy ellenőrzött és együttműködésen alapuló környezetben közösen validáljanak konkrét biztonsági intézkedéseket, eszközöket vagy technikákat.

(24) A TLPT-t tanulási tapasztalatként kell felhasználni a pénzügyi szervezetek digitális működési rezilienciájának fokozása érdekében. E tekintetben a kék csapatnak és a tesztelőknek vissza kell játszaniuk a támadást, és a tesztelőkkel együttműködve felül kell vizsgálniuk a megtett lépéseket, hogy tanuljanak a tesztelési tapasztalatokból. E célból és a megfelelő előkészítés lehetővé tétele érdekében a vörös csapat tesztjelentését és a kék csapat tesztjelentését a visszajátszási tevékenységekben részt vevő valamennyi fél rendelkezésére kell bocsátani, mielőtt bármilyen visszajátszásra irányuló tevékenységet végeznének. Emellett a tanulási tapasztalat maximalizálása érdekében a lezárási szakaszban közös tesztelést kell végezni. A lezárási szakaszban a közös teszteléshez használható módszereknek magukban kell foglalniuk az alternatív támadási forgatókönyvek megvitatását, alternatív forgatókönyvek feltárását az éles rendszereken vagy az olyan tervezett forgatókönyvek újbóli feltárását az éles rendszereken, amelyeket a tesztelők a tesztelési szakaszban nem tudtak befejezni vagy végrehajtani.

(25) A TLPT-ben részt vevő valamennyi fél tanulási tapasztalatainak további megkönnyítése, a jövőbeli tesztek elősegítése, valamint a pénzügyi szervezetek digitális működési rezilienciájának előmozdítása érdekében az érintett feleknek visszajelzést kell adniuk egymásnak a teljes folyamatról és különösen meg kell határozniuk, hogy mely tevékenységek haladtak jól és melyek javíthatók, és hogy a TLPT-folyamat mely részei működtek jól és melyek javíthatók.

(26) Amennyiben eltérőek, az (EU) 2022/2554 rendelet 46. cikkében említett illetékes hatóságoknak és a TLPT-hatóságoknak együtt kell működniük annak érdekében, hogy a TLPT révén végzett fejlett tesztelést beépítsék a meglévő felügyeleti folyamatokba. E tekintetben, és hogy azonosan és helyesen értelmezzék a TLPT eredményeit – különösen a teszt összefoglaló jelentése és a korrekciós tervek tekintetében –, helyénvaló szoros együttműködést kialakítani a TLPT-ben részt vevő tesztvezetők és a felelős felügyeletek között.

(27) Az (EU) 2022/2554 rendelet 26. cikke (8) bekezdésének első albekezdése előírja a pénzügyi szervezetek számára, hogy három tesztenként külső tesztelőket bízzanak meg. Amennyiben a pénzügyi szervezetek belső és külső tesztelőket egyaránt alkalmaznak a csapatban, ezt az említett cikk alkalmazásában belső tesztelőkkel végzett TLPT-nek kell tekinteni.

(28) Ez a rendelet az Európai Bankhatóság, az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság és az Európai Értékpapírpiaci Hatóság (európai felügyeleti hatóságok) által az Európai Központi Bankkal egyetértésben a Bizottsághoz benyújtott szabályozástechnikai standardtervezeteken alapul.

(29) Az európai felügyeleti hatóságok nyilvános konzultációt folytattak az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezték az esetleges kapcsolódó költségeket és hasznot, továbbá kikérték az 1093/2010/EU európai parlamenti és tanácsi rendelet ([3]) 37. cikkével összhangban létrehozott banki érdekképviseleti csoport, az 1094/2010/EU európai parlamenti és tanácsi rendelet ([4]) 37. cikkével összhangban létrehozott biztosítási és viszontbiztosítási érdekképviseleti csoport és foglalkoztatói-nyugdíj érdekképviseleti csoport, valamint az 1095/2010/EU európai parlamenti és tanácsi rendelet ([5]) 37. cikkével összhangban létrehozott értékpapírpiaci érdekképviseleti csoport véleményét.

(30) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([6]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2024. augusztus 20-án véleményt nyilvánított,

ELFOGADTA EZT A RENDELETET:

1. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „ellenőrzést végző csapat”: a tesztelést irányító, a tesztelt pénzügyi szervezet személyzetéből és – amennyiben a TLPT terjedelmét figyelembe véve releváns – harmadik fél szolgáltatóinak és bármely más félnek a személyzetéből álló csapat;

2. „ellenőrzést végző csapat vezetője”: a pénzügyi szervezet személyzetének azon tagja, aki az adott teszttel összefüggésben a pénzügyi szervezet tekintetében a TLPT-vel kapcsolatos valamennyi tevékenység elvégzéséért felelős;

3. „kék csapat”: a pénzügyi szervezet személyzete, valamint adott esetben a pénzügyi szervezet harmadik fél szolgáltatóinak, valamint a TLPT hatókörére tekintettel relevánsnak ítélt bármely más félnek a személyzete, akik a hálózati és információs rendszerek pénzügyi szervezet általi használatát védik a szimulált vagy valós támadásokkal szembeni biztonsági helyzetének fenntartásával, és akiknek nincs tudomásuk a TLPT-ről;

4. „kék csapat feladatai”: jellemzően a kék csapat által végzendő feladatok, például a biztonsági műveleti központ (SOC) szolgáltatásai, IKT-infrastruktúra-szolgáltatások, ügyfélszolgálati szolgáltatások, operatív szintű eseménykezelési szolgáltatások;

5. „vörös csapat”: a TLPT elvégzésére szerződtetett vagy arra kirendelt belső vagy külső tesztelők;

6. „közös tesztelés”: olyan együttműködésen alapuló tesztelési tevékenység, amelyben a tesztelők és a kék csapat egyaránt részt vesznek;

([3]) 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?locale=hu).

([4]) 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?locale=hu).

([5]) 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., ELI: http://data.europa.eu/eli/reg/2010/1095/oj?locale=hu).

([6]) 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?locale=hu).

7. „TLPT-hatóság”: a következők bármelyike:

   a) a pénzügyi szektorban az (EU) 2022/2554 rendelet 26. cikkének (9) bekezdésével összhangban kijelölt egyetlen hatóság;

   b) azon hatóság a pénzügyi szektorban, amelyre a TLPT-vel kapcsolatos feladatok egy részének vagy egészének ellátását az (EU) 2022/2554 rendelet 26. cikkének (10) bekezdésével összhangban átruházták;

   c) az (EU) 2022/2554 rendelet 46. cikkében említett illetékes hatóságok bármelyike;

8. „TLPT-kibercsoport” vagy „TCT”: a TLPT-hatóságok TLPT-vel kapcsolatos ügyekért felelős személyzete;

9. „tesztvezetők”: a TLPT-hatóság adott TLPT tekintetében e rendeletnek való megfelelés nyomon követésére irányuló tevékenységeinek vezetésére kijelölt személyzet;

10. „fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató”: a pénzügyi szervezet által az egyes TLPT-k tekintetében szerződtetett, a pénzügyi szervezeten és adott esetben a csoporton belüli IKT-szolgáltatókon kívüli szakértők, akik összegyűjtik és elemzik az adott TLPT-gyakorlat hatókörébe tartozó pénzügyi szervezetek szempontjából releváns, célzott fenyegetettségi információkat, és megfelelő releváns és valósághű fenyegetettségi forgatókönyveket dolgoznak ki;

11. „TLPT-szolgáltatók”: a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók;

12. „kisegítés”: az ellenőrzést végző csapat által a tesztelőknek nyújtott támogatás vagy tájékoztatás annak érdekében, hogy a tesztelők folytathassák a támadás végrehajtását, amennyiben egyedül nem tudnak továbblépni, és nincs más észszerű alternatíva, beleértve azt is, ha egy adott TLPT-ben nem áll rendelkezésre elegendő idő vagy erőforrás;

13. „támadási útvonal”: a TLPT vörös csapat által végzett aktív tesztelési szakaszában az adott TLPT-hez meghatározott tesztcélok elérése érdekében a tesztelők által követett útvonal;

14. „tesztcélok”: a pénzügyi szervezet kritikus vagy fontos funkcióit támogató IKT-rendszerekben található kulcsfontosságú célok, amelyeket a tesztelők a teszt során megpróbálnak elérni;

15. „érzékeny információ”: olyan információ, amely könnyen felhasználható a pénzügyi szervezet IKT-rendszerei elleni támadásokhoz, szellemi tulajdon, bizalmas üzleti adatok vagy személyes adatok, amelyek közvetlenül vagy közvetve kárt okozhatnak a pénzügyi szervezetnek és ökoszisztémájának, ha rosszindulatú szereplők kezébe kerülnének;

16. „tesztcsoport”: az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdése szerinti csoportos TLPT-ben részt vevő valamennyi pénzügyi szervezet;

17. „fogadó tagállam”: a fogadó tagállam az egyes pénzügyi szervezetekre alkalmazandó uniós ágazati joggal összhangban;

18. „közös TLPT”: az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdésében említett csoportos TLPT-től eltérő olyan TLPT, amelyben ugyanazon csoporton belüli IKT-szolgáltatót igénybe vevő vagy ugyanazon csoporthoz tartozó és közös IKT-rendszereket használó több pénzügyi szervezet vesz részt.

2. cikk

A TLPT elvégzésére kötelezett pénzügyi szervezetek azonosítása

(1) A TLPT-hatóságok a pénzügyi szervezetek hatását, rendszerszintű jellegét és IKT-kockázati profilját figyelembe véve az alábbi kritériumok mindegyike alapján értékelik, hogy valamely pénzügyi szervezet köteles-e elvégezni a TLPT-t:

a) a hatáshoz és a rendszerszintű jelleghez kapcsolódó tényezők:

   i. a pénzügyi szervezet mérete, amelynek meghatározásakor alapul veszik, hogy a pénzügyi szervezet egy vagy több tagállamban nyújt-e pénzügyi szolgáltatásokat, valamint összehasonlítják a pénzügyi szervezet tevékenységeit a hasonló szolgáltatásokat nyújtó más pénzügyi szervezetek tevékenységeivel;

   ii. a pénzügyi szervezet egy vagy több tagállam pénzügyi ágazatában működő más pénzügyi szervezetekkel való összekapcsoltságának mértéke és jellege;

   iii. a pénzügyi szervezet által a pénzügyi ágazat számára nyújtott szolgáltatások kritikussága vagy jelentősége;

iv. a pénzügyi szervezet által nyújtott szolgáltatások helyettesíthetősége;

v. a pénzügyi szervezet üzleti modelljének, valamint a kapcsolódó szolgáltatásoknak és folyamatoknak az összetettsége;

vi. a pénzügyi szervezet a pénzügyi ágazatban uniós vagy nemzeti szinten rendszerszintű jellegű, közös IKT-rendszereket használó csoport tagja-e;

b) az IKT-kockázathoz kapcsolódó tényezők:

i. a pénzügyi szervezet kockázati profilja;

ii. a pénzügyi szervezet fenyegetettségi helyzete;

iii. a pénzügyi szervezet kritikus vagy fontos funkcióinak vagy azok támogató funkcióinak IKT-rendszerektől és -folyamatoktól való függőségének mértéke;

iv. a pénzügyi szervezet IKT-architektúrájának összetettsége;

v. a harmadik fél IKT-szolgáltatók által támogatott IKT-szolgáltatások és -funkciók, valamint a harmadik fél IKT-szolgáltatókkal vagy csoporton belüli IKT-szolgáltatókkal kötött szerződéses megállapodások mennyisége és típusa;

vi. a pénzügyi szervezet IKT-érettségének értékelése szempontjából releváns felügyeleti felülvizsgálatok eredményei;

vii. az IKT-üzletmenetfolytonossági tervek és IKT-reagálási és -helyreállítási tervek érettsége;

viii. az operatív IKT-biztonsághoz kapcsolódó észlelési és enyhítő intézkedések érettsége, beleértve a következőkre való képességet:

1. a pénzügyi szervezet IKT-infrastruktúrájának folyamatos nyomon követése;

2. az IKT-vel kapcsolatos események valós idejű észlelése;

3. a 2. pontban említett események elemzése;

4. időben történő és hatékony reagálás a 2. pontban említett eseményekre;

ix. a pénzügyi szervezet a pénzügyi ágazatban uniós vagy nemzeti szinten aktív, közös IKT-rendszereket használó csoport tagja-e.

Az a) pont i. alpontjának alkalmazásában a TLPT-hatóság lehetőség szerint mérlegeli a következőket:

a) a pénzügyi szervezet piaci részesedési helyzete uniós és nemzeti szinten;

b) a pénzügyi szervezet által kínált tevékenységek köre;

c) a pénzügyi szervezet által nyújtott szolgáltatások vagy az uniós és nemzeti szinten végzett tevékenységek piaci részesedése.

Az a) pont v. alpontjának alkalmazásában a TLPT-hatóság lehetőség szerint mérlegeli a következőket:

a) a pénzügyi szervezet egynél több üzleti modellt működtet-e;

b) a különböző üzleti folyamatok és a kapcsolódó szolgáltatások összekapcsoltsága.

(2) A TLPT-hatóságok előírják a következő pénzügyi szervezetek számára a TLPT elvégzését, kivéve, ha a pénzügyi szervezetre vonatkozó, az (1) bekezdésben említett értékelés azt mutatja, hogy a pénzügyi szervezet hatása, a vele kapcsolatos pénzügyi stabilitási aggályok vagy az IKT-kockázati profilja nem indokolja a TLPT elvégzését:

a) az alábbi feltételek bármelyikét teljesítő hitelintézetek:

i. a 2013/36/EU európai parlamenti és tanácsi irányelv ([7]) 131. cikkével összhangban globálisan rendszerszinten jelentős intézményként (G-SII-k) azonosították őket;

ii. a 2013/36/EU irányelv 131. cikkével összhangban egyéb rendszerszinten jelentős intézményként (O-SII-k) azonosították őket;

iii. G-SII-k vagy O-SII-k részét képezik;

([7]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások 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., ELI: http://data.europa.eu/eli/dir/2013/36/oj?locale=hu).

b) azon pénzforgalmi intézmények, amelyek a TLPT-hatóság általi értékelést megelőző két naptári év mindegyikében túllépték az (EU) 2015/2366 európai parlamenti és tanácsi irányelv ([8]) 4. cikkének 5. pontjában meghatározott fizetési műveletek tekintetében a 150 milliárd EUR összértéket;

c) azon elektronikuspénz-kibocsátó intézmények, amelyek a TLPT-hatóság általi értékelést megelőző két naptári év mindegyikében túllépték vagy az (EU) 2015/2366 irányelv 4. cikkének 5. pontjában meghatározott fizetési műveletek tekintetében a 150 milliárd EUR összértéket, vagy a kintlevő elektronikus pénz tekintetében a 40 milliárd EUR összértéket;

d) központi értéktárak;

e) központi szerződő felek;

f) az alábbi kritériumok bármelyikének megfelelő elektronikus kereskedési rendszerrel rendelkező kereskedési helyszínek:

i. a TLPT-hatóság általi értékelést megelőző két naptári év mindegyikében a forgalmat tekintve nemzeti szinten a kereskedési helyszín rendelkezik a legnagyobb piaci részesedéssel az alábbiak bármelyikében:

1. a 2014/65/EU európai parlamenti és tanácsi irányelv ([9]) 4. cikke (1) bekezdése 44. pontjának a) alpontja szerinti átruházható értékpapírok;

2. a 2014/65/EU irányelv 4. cikke (1) bekezdése 44. pontjának b) alpontja szerinti átruházható értékpapírok;

3. a 600/2014/EU európai parlamenti és tanácsi rendelet ([10]) 2. cikke (1) bekezdésének 29. pontjában meghatározott származtatott termékek;

4. a 600/2014/EU rendelet 2. cikke (1) bekezdésének 28. pontjában meghatározott strukturált pénzügyi termékek;

5. a 2014/65/EU irányelv I. melléklete C. szakaszának (11) pontjában említett kibocsátási egységek;

ii. a TLPT-hatóság általi értékelést megelőző két naptári év mindegyikében a forgalmat tekintve uniós szinten a kereskedési helyszín 5 %-ot meghaladó piaci részesedéssel rendelkezik az alábbiak bármelyikében:

1. társaságok részvényei és más – társaságok, társas vállalkozások vagy más szervezetek részvényeivel egyenértékű – értékpapírok, valamint részvények tekintetében kiadott letéti igazolások;

2. kötvények és az értékpapírosított adósság más formái, ideértve az ilyen értékpapírok tekintetében kiadott letéti igazolásokat;

3. a 600/2014/EU rendelet 2. cikke (1) bekezdésének 29. pontjában meghatározott származtatott termékek;

4. a 600/2014/EU rendelet 2. cikke (1) bekezdésének 28. pontjában meghatározott strukturált pénzügyi termékek;

5. a 2014/65/EU irányelv I. melléklete C. szakaszának (11) pontjában említett kibocsátási egységek;

([8]) 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., ELI: http://data.europa.eu/eli/dir/2015/2366/oj?locale=hu).

([9]) 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., ELI: http://data.europa.eu/eli/dir/2014/65/oj?locale=hu).

([10]) Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról (HL L 173., 2014.6.12., 84. o., ELI: http://data.europa.eu/eli/reg/2014/600/oj?locale=hu).

g) az alábbi kritériumok mindegyikének megfelelő biztosítók és viszontbiztosítók:

i. bruttó díjelőírásuk meghaladja az 1 500 000 000 EUR-t;

ii. 10 000 000 000 EUR-t meghaladó biztosítástechnikai tartalékkal rendelkeznek;

iii. olyan biztosítók, amelyek csak életbiztosítási tevékenységet folytatnak, vagy amelyek életbiztosítási és nem-életbiztosítási tevékenységet is folytatnak, és teljes eszközállományuk meghaladja a tagállamban letelepedett biztosítók és viszontbiztosítók 2009/138/EK európai parlamenti és tanácsi irányelv ([11]) 75. cikkével összhangban értékelt eszközállománya összegének 3,5 %-át;

Az f) pont ii. alpontjának alkalmazásában, amennyiben a kereskedési helyszín közös IKT-rendszereket használó vagy ugyanazon csoporton belüli IKT-szolgáltatót igénybe vevő csoport része, az értékpapírok és származtatott ügyletek tekintetében az ugyanazon csoporthoz tartozó és az Unióban letelepedett valamennyi kereskedési helyszínen elért forgalmat kell figyelembe venni.

A g) pont alkalmazásában a TLPT-hatóságok a g) pont i., ii. és iii. alpontjában lefektetett kritériumok alkalmazásával meghatározzák az összes biztosító és viszontbiztosító egy részhalmazát. Az e részhalmazba tartozó biztosítók és viszontbiztosítók akkor kötelesek elvégezni a TLPT-t, ha megfelelnek az alábbi kritériumok bármelyikének is:

a) 3 000 000 000 EUR-t meghaladó bruttó díjelőírás;

b) 30 000 000 000 EUR-t meghaladó biztosítástechnikai tartalék;

c) a tagállamban letelepedett biztosítók és viszontbiztosítók 2009/138/EK irányelv 75. cikkével összhangban értékelt eszközállománya összegének 10 %-át meghaladó eszközállomány.

(3) Amennyiben a (2) bekezdésben meghatározott kritériumokat egynél több, ugyanahhoz a csoporthoz tartozó és közös IKT-rendszereket használó pénzügyi szervezet, vagy egynél több, ugyanazon csoporton belüli IKT-szolgáltatót igénybe vevő pénzügyi szervezet teljesíti, az említett pénzügyi szervezetek TLPT-hatóságainak a 16. cikk (2) bekezdésével összhangban el kell dönteniük, hogy a TLPT egyedi alapon történő elvégzésére vonatkozó követelmény releváns-e ezen pénzügyi szervezetek tekintetében.

Amennyiben az első albekezdésben említett pénzügyi szervezetek csoportja anyavállalatának TLPT-hatósága eltér a csoport pénzügyi szervezeteinek TLPT-hatóságaitól, az adott csoporthoz tartozó pénzügyi szervezetek TLPT-hatóságainak konzultálniuk kell ezzel a hatósággal arról, hogy helyénvaló-e a TLPT egyedi alapon történő elvégzése.

3. cikk

TCT és TLPT-tesztvezetők

(1) A TLPT-hatóság a TLPT-vel kapcsolatos tevékenységek koordinálását TCT-re bízza. A TCT valamely önálló TLPT felügyeletére kijelölt tesztvezetőkből áll.

(2) A TLPT-hatóság minden teszthez kijelöl egy tesztvezetőt és legalább egy helyettest.

(3) A tesztvezetők nyomon követik, hogy teljesülnek-e az e rendeletben meghatározott követelmények, illetve biztosítják azok teljesülését.

([11]) 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., ELI: http://data.europa.eu/eli/dir/2009/138/oj?locale=hu).

(4) A tesztvezető a 9. cikk (1) bekezdésében említett értesítés útján közli a TCT elérhetőségeit a pénzügyi szervezettel.

(5) A TLPT-hatóság a TLPT valamennyi szakaszában részt vesz.

4. cikk

A pénzügyi szervezetekre vonatkozó szervezeti intézkedések

(1) A pénzügyi szervezetek kijelölik az ellenőrzést végző csapat vezetőjét, aki felel a TLPT napi irányításáért, valamint az ellenőrzést végző csapat döntéseiért és intézkedéseiért.

(2) A pénzügyi szervezetek szervezeti és eljárási intézkedéseket hoznak az alábbiak biztosítására:

a) a tervezett vagy folyamatban lévő TLPT-vel kapcsolatos információkhoz való hozzáférés a szükséges ismeret elve alapján az ellenőrzést végző csapatra, a vezető testületre, a tesztelőkre, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatóra és a TLPT-hatóságra korlátozódik;

b) az ellenőrzést végző csapat konzultál a tesztvezetőkkel, mielőtt a kék csapat bármely tagját bevonja a TLPT-be;

c) az ellenőrzést végző csapatot tájékoztatják, ha a pénzügyi szervezet vagy a harmadik fél szolgáltatói személyzete bármilyen módon észleli a TLPT-t; az eseményre való reagálás eszkalációja esetén az ellenőrzést végző csapat elszigeteli az eszkalációt, ha szükséges;

d) a TLPT titkosságára vonatkozó, a pénzügyi szervezet személyzetére, az érintett harmadik fél IKT-szolgáltatók személyzetére, a tesztelőkre és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatóra alkalmazandó szabályok vannak érvényben;

e) az ellenőrzést végző csapat kérésre a tesztvezetők rendelkezésére bocsátja a TLPT-re vonatkozó információkat;

f) amennyiben lehetséges, a TLPT-ben részt vevő felek csak kódnévvel hivatkoznak a TLPT-re.

5. cikk

A TLPT-hez kapcsolódó kockázatkezelés

(1) „(1) A 9. cikkben említett előkészítési szakaszban az ellenőrzést végző csapat értékeli a pénzügyi szervezet kritikus vagy fontos funkcióit ellátó éles rendszerek tesztelésével kapcsolatos kockázatokat, beleértve a következőkre gyakorolt lehetséges hatásokat is:

a) a pénzügyi szektor;

b) az uniós vagy nemzeti szintű pénzügyi stabilitás.

Az ellenőrzést végző csapat a tesztelés során felülvizsgálja ezeket a hatásokat.

(2) A kockázatértékelés és -kezelés céljából az ellenőrzést végző csapat legalább az alábbiakhoz kapcsolódó, következő típusú kockázatokat figyelembe veszi:

a) adott esetben hozzáférés biztosítása a pénzügyi szervezetre vonatkozó érzékeny információkhoz a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató és a külső tesztelők számára;

b) a TLPT (EU) 2022/2554 rendeletnek és e rendeletnek való meg nem felelése, amennyiben e meg nem felelés az (EU) 2022/2554 rendelet 26. cikkének (7) bekezdésében említett igazolás hiányát eredményezi, beleértve azt az esetet is, amikor a meg nem felelés a TLPT bizalmas jellegének megsértése vagy az etikus magatartás hiánya miatt áll fenn;

c) válság és események eszkalációja;

d) a vörös csapat által végzett aktív szakasz, beleértve a tesztelők tevékenysége miatt bekövetkező, a kritikus tevékenységekben fellépő zavarokkal és az adatsérüléssel kapcsolatos kockázatokat, valamint ezek harmadik felekre gyakorolt lehetséges hatásait;

e) a kék csapat tevékenysége, beleértve a tevékenységük miatt bekövetkező, a kritikus tevékenységekben fellépő zavarokkal és az adatsérüléssel kapcsolatos kockázatokat, valamint ezek harmadik felekre gyakorolt lehetséges hatásait;

f) a TLPT által érintett rendszerek hiányos visszaállítása.

6. cikk

A csoportos és közös TLPT-khez kapcsolódó kockázatkezelés

(1) Csoportos TLPT vagy közös TLPT esetében az egyes pénzügyi szervezetek ellenőrzést végző csapata saját kockázatértékelést végez és saját kockázatkezelési intézkedéseket határoz meg.

(2) Az e rendelet 16. cikke (3) bekezdésének b) pontjában említett kijelölt pénzügyi szervezet vagy az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdésével összhangban kijelölt pénzügyi szervezet ellenőrzést végző csapata értékeli a több pénzügyi szervezet TLPT-ben való részvételével kapcsolatos kockázatokat. Az érintett pénzügyi szervezetek ellenőrzést végző csapatai együttműködnek a kijelölt pénzügyi szervezet ellenőrzést végző csapatával a lehetséges közös kockázatok azonosítása érdekében.

7. cikk

A TLPT-szolgáltatók kiválasztása

(1) Az ellenőrzést végző csapat intézkedéseket hoz a TLPT-vel kapcsolatos kockázatok kezelésére és különösen a következőket biztosítja minden egyes TLPT esetében:

a) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató és a külső tesztelők az ellenőrzést végző csapat rendelkezésére bocsátanak egy részletes önéletrajzot és azon tanúsítványok másolatát, amelyek az elismert piaci szabványoknak megfelelően feljogosítják őket tevékenységeik végzésére;

b) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató és a külső tesztelő releváns szakmai felelősségbiztosítások révén megfelelően és teljeskörűen biztosítva van, többek között a szakmai kötelezettségmulasztás és a gondatlanság kockázataival szemben;

c) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató legalább három, korábbi megbízatásokból származó, behatolási teszteléssel és vörös csapat által végzett teszteléssel összefüggő referenciával szolgál;

d) a külső tesztelők legalább öt, korábbi megbízatásokból származó, behatolási teszteléssel és vörös csapat által végzett teszteléssel kapcsolatos referenciával szolgálnak;

e) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató TLPT elvégzésére kijelölt személyzete:

   i. legalább egy olyan vezetőből áll, aki legalább 5 éves tapasztalattal rendelkezik a fenyegetettséggel kapcsolatos hírszerzés terén, valamint legalább egy további tagból, aki legalább 2 éves tapasztalattal rendelkezik a fenyegetettséggel kapcsolatos hírszerzés terén;

   ii. széles körű és megfelelő szintű szakmai ismeretekkel és készségekkel rendelkezik, beleértve a következőket:

      1. hírszerzési adatgyűjtési taktikák, módszerek és eljárások;

      2. geopolitikai, műszaki és ágazati ismeretek;

      3. megfelelő kommunikációs készségek a megbízatás eredményének jól érthető bemutatásához és az arról való jelentéstételhez;

   iii. együttesen legalább három korábbi, behatolási teszteléssel és vörös csapat által végzett teszteléssel összefüggő megbízatásban vett részt a fenyegetettséggel kapcsolatos hírszerzés terén;

   iv. nem végez egyidejűleg olyan, a kék csapat által végzendő feladatokat vagy egyéb szolgáltatásokat, amelyek összeférhetetlenséget eredményezhetnek a megbízatásban szereplő TLPT-ben részt vevő pénzügyi szervezettel, harmadik fél IKT-szolgáltatóval vagy csoporton belüli IKT-szolgáltatóval szemben;

   v. elkülönül az ugyanahhoz a TLPT-hez külső tesztelőket biztosító ugyanazon TLPT-szolgáltató alkalmazottaitól, és nem ezek beosztottja;

f) külső tesztelők esetében a TLPT elvégzésére kijelölt vörös csapat:

i. legalább egy olyan vezetőből áll, aki legalább 5 éves tapasztalattal rendelkezik a behatolási tesztelés és vörös csapat által végzett tesztelés terén, valamint legalább két további tesztelőből, akik legalább 2 éves tapasztalattal rendelkeznek a behatolási tesztelés és vörös csapat által végzett tesztelés terén;

ii. széles körű és megfelelő szintű szakmai ismeretekkel és készségekkel rendelkezik, beleértve a pénzügyi szervezet üzleti tevékenységére, a felderítésre, a kockázatkezelésre, a sérülékenységek kiaknázására, a fizikai behatolásra, a pszichológiai manipulációra, a sebezhetőségek elemzésére vonatkozó ismereteket, valamint megfelelő kommunikációs készségekkel a megbízatás eredményének jól érthető bemutatásához és az arról való jelentéstételhez;

iii. együttesen legalább öt korábbi, behatolási teszteléssel és vörös csapat által végzett teszteléssel kapcsolatos megbízatásban vett részt;

iv. nem áll olyan fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató alkalmazásában, amely egyidejűleg a kék csapat feladatait végzi a TLPT-ben részt vevő pénzügyi szervezet, harmadik fél IKT-szolgáltató vagy csoporton belüli IKT-szolgáltató számára, illetve nem nyújt szolgáltatásokat ilyen számára;

v. elkülönül az ugyanahhoz a TLPT-hez fenyegetettséggel kapcsolatos hírszerzési szolgáltatásokat biztosító ugyanazon TLPT-szolgáltató alkalmazottaitól;

g) a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató a tesztelés végén visszaállítási eljárásokat végeznek, beleértve a TLPT során veszélybe került jelszavakkal, hitelesítő adatokkal és más titkos kulcsokkal kapcsolatos információk biztonságos törlését, a veszélybe került fiókok pénzügyi szervezettel való biztonságos közlését, a tesztelés során gyűjtött egyéb adatok biztonságos gyűjtését, tárolását, kezelését és ártalmatlanítását;

h) a tesztelők a tesztelés végén elvégzett, a g) pontban említett visszaállítási eljárások mellett a következő visszaállítási eljárásokat is elvégzik:

i. a támadást irányító (command and control) szerver inaktiválása;

ii. leállító kapcsolók (hatókör, időpont);

iii. a hátsó ajtók és más rosszindulatú szoftverek eltávolítása;

iv. lehetséges biztonsági sérülésekkel kapcsolatos értesítés;

v. a jövőbeli biztonsági visszaállításra vonatkozó eljárások, amelyek rosszindulatú szoftvereket vagy a teszt során telepített eszközöket érinthetnek;

vi. a kék csapat tevékenységeinek nyomon követése és az ellenőrzést végző csapat tájékoztatása a lehetséges észlelésekről;

i) a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató az alábbi tevékenységek egyikét sem végzik, illetve nem vesznek részt azokban:

i. a pénzügyi szervezet és adott esetben a harmadik fél IKT-szolgáltatója berendezéseinek engedély nélküli megsemmisítése;

ii. a pénzügyi szervezet és adott esetben a harmadik fél IKT-szolgáltatója információinak és IKT-eszközeinek ellenőrzés nélküli módosítása;

iii. a pénzügyi szervezet kritikus vagy fontos funkciói folytonosságának szándékos veszélyeztetése;

iv. olyan rendszerek engedély nélküli bevonása a tesztbe, amelyre az nem terjed ki;

v. a teszteredmények jogosulatlan közlése.

(2) Az ellenőrzést végző csapat nyilvántartást vezet a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók által az (1) bekezdés a)–f) pontjának való megfelelés igazolására benyújtott dokumentációról.

Kivételes körülmények között a pénzügyi szervezetek olyan külső tesztelőket és fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókat is megbízhatnak, akik nem felelnek meg az (1) bekezdés a)–f) pontjában meghatározott egy vagy több követelménynek, feltéve, hogy az említett pénzügyi szervezetek olyan intézkedéseket fogadnak el, amelyek alkalmasak az említett pontoknak való meg nem feleléssel kapcsolatos kockázatok csökkentésére, és nyilvántartást vezetnek ezekről az intézkedésekről.

8. cikk

A csoportos és közös TLPT-k sajátosságai

(1) Ha a vezető TLPT-hatóság másként nem határoz, amennyiben több, a 16. cikk (2) vagy (4) bekezdésével összhangban azonosított pénzügyi szervezet vesz részt egy csoportos vagy közös TLPT-ben, minden pénzügyi szervezetnek követnie kell a 9–15. cikkben meghatározott valamennyi lépést.

(2) E rendelet eltérő rendelkezése hiányában, amennyiben a 16. cikk (3) vagy (5) bekezdésében említettek szerint több TLPT-hatóság vesz részt egy közös TLPT-ben vagy egy csoportos TLPT-ben, a 9–15. cikkben a „TLPT-hatóságra” való hivatkozásokat az ilyen csoportos vagy közös TLPT vezető TLPT-hatóságára való hivatkozásként kell értelmezni.

9. cikk

Előkészítési szakasz

(1) Az (EU) 2022/2554 rendelet 26. cikke (8) bekezdésének harmadik albekezdése alapján azonosított pénzügyi szervezetnek TLPT-t kell elindítania, miután a TLPT-hatóság értesíti, hogy TLPT-t kell elvégezni.

(2) A pénzügyi szervezet az (1) bekezdésben említett értesítés kézhezvételétől számított 3 hónapon belül benyújtja a tesztvezetőknek a TLPT elindítására vonatkozó alábbi információkat:

a) a projekt magas szintű projekttervet is tartalmazó alapszabálya, amely tartalmazza az I. mellékletben meghatározott információkat;

b) az ellenőrzést végző csapat vezetőjének elérhetőségei;

c) a belső vagy külső tesztelők vagy mindkettő tervezett használatára vonatkozó információk, adott esetben a 15. cikkben részletezettek szerint;

d) a TLPT során használandó kommunikációs csatornákra vonatkozó információk;

e) a TLPT kódneve.

(3) Amennyiben a (2) bekezdés a)–e) pontjában említett információk hiánytalanok, és biztosítják a TLPT megfelelőségét és hatékony elvégzését, a TLPT-hatóság validálja a pénzügyi szervezet TLPT elindításával kapcsolatos információit, és erről értesíti a pénzügyi szervezetet.

(4) A TLPT elindítására vonatkozó információk TLPT-hatóság általi validálását követően a pénzügyi szervezet ellenőrzést végző csapatot hoz létre, hogy támogassa az ellenőrzést végző csapat vezetőjét a következő feladatok ellátásában:

a) az ellenőrzést végző csapaton belül, illetve a tesztelőkkel és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókkal a TLPT-vel kapcsolatos kérdések kapcsán folytatott kommunikáció csatornáinak és folyamatainak meghatározása;

b) a pénzügyi szervezet vezető testületének tájékoztatása a TLPT előrehaladásáról és a kapcsolódó kockázatokról;

c) a tárgyhoz kapcsolódó szakértelmen alapuló döntések meghozatala a TLPT során;

d) a TLPT végrehajtása e rendelettel összhangban;

e) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató kiválasztása a TLPT-hez;

f) a külső tesztelők, a belső tesztelők vagy mindkettő kiválasztása;

g) a terjedelmet meghatározó dokumentum elkészítése.

(5) Amennyiben a TLPT-hatóság úgy ítéli meg, hogy az ellenőrzést végző csapat kezdeti összetétele és annak bármely későbbi változása megfelelő a (4) bekezdésben említett feladatok ellátásához, a TLPT-hatóság validálja az ellenőrzést végző csapatot, és erről értesíti annak vezetőjét.

(6) A pénzügyi szervezet a TLPT-hatóság (1) bekezdésben említett értesítésének kézhezvételétől számított 6 hónapon belül benyújtja a tesztvezetőknek a II. mellékletben meghatározott valamennyi információt tartalmazó, terjedelmet meghatározó dokumentumot. A pénzügyi szervezet vezető testülete jóváhagyja a terjedelmet meghatározó dokumentumot.

(7) A pénzügyi szervezeteknek a következő kritériumokat kell figyelembe venniük, amikor meghatározzák, hogy a TLPT mely kritikus és fontos funkciókra terjedjen ki:

a) a funkció kritikussága vagy fontossága, valamint a pénzügyi ágazatra és az uniós és nemzeti szintű pénzügyi stabilitásra gyakorolt lehetséges hatása;

b) a funkció jelentősége a pénzügyi szervezet napi üzleti tevékenysége szempontjából;

c) a funkció helyettesíthetősége;

d) a más funkciókkal való összekapcsoltság;

e) a funkció földrajzi helyzete;

f) más szervezetek e funkciótól való ágazati függése;

g) amennyiben rendelkezésre áll, a funkciót illető, fenyegetettséggel kapcsolatos hírszerzés.

(8) Az ellenőrzést végző csapat megosztja a TLPT elindítására vonatkozó információkat és a terjedelmet meghatározó dokumentumot a tesztelőkkel és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókkal ezek szerződtetését követően. Az ellenőrzést végző csapat tájékoztatja a tesztelőket és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókat a követendő tesztelési folyamatról.

(9) A pénzügyi szervezet biztosítja, hogy a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók szerződtetése vagy kijelölése a tesztelési szakasz megkezdése előtt befejeződjön.

(10) A tesztelési szakasz megkezdése előtt az ellenőrzést végző csapat konzultál a tesztvezetőkkel a TLPT kockázatértékeléséről és a kockázatkezelési intézkedésekről. Az ellenőrzést végző csapat felülvizsgálja a kockázatértékelést vagy a kockázatkezelési intézkedéseket, amennyiben a TLPT-hatóság véleménye szerint azok nem megfelelőek a TLPT kockázatainak kezelésére.

(11) Az ellenőrzést végző csapat értékeli, hogy azok a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók és tesztelők, akiket be kíván vonni a TLPT-be, megfelelnek-e az (EU) 2022/2554 rendelet 27. cikkében és az e rendelet 7. cikke (1) bekezdésében meghatározott követelményeknek, és dokumentálja az értékelés eredményét. Az ellenőrzést végző csapat az említett értékeléssel és kockázatkezelési gyakorlatával összhangban választja ki a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókat. A kiválasztott fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókkal és külső tesztelőkkel való szerződéskötést megelőzően az ellenőrzést végző csapat bizonyítékot szolgáltat a tesztvezetők számára arról, hogy az említett fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók és tesztelők megfelelnek az (EU) 2022/2554 rendelet 27. cikkében és e rendelet 7. cikke (1) bekezdésében meghatározott követelményeknek. Az ellenőrzést végző csapat nem köthet szerződést a kiválasztott fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatókkal és külső tesztelőkkel, ha a TLPT-hatóság véleménye szerint a kiválasztott fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók és külső tesztelők nem felelnek meg az (EU) 2022/2554 rendelet 27. cikkében meghatározott követelményeknek vagy az e rendelet 7. cikkének (1) bekezdésében meghatározott követelményeknek, illetve az uniós joggal összhangban a nemzetbiztonsági jogszabályokból eredő további követelményeknek, vagy ha a pénzügyi szervezet nem felel meg e rendelet 7. cikke (2) bekezdése első albekezdésének, vagy ha az e rendelet 7. cikke (2) bekezdésének második albekezdésében említett körülmények nem teljesülnek.

(12) Amennyiben a terjedelmet meghatározó dokumentum teljes, és biztosítja a megfelelő és hatékony TLPT elvégzését, a TLPT-hatóság jóváhagyja a dokumentumot, és erről tájékoztatja az ellenőrzést végző csapat vezetőjét.

10. cikk

Tesztelési szakasz: fenyegetettséggel kapcsolatos hírszerzés

(1) Miután a TLPT-hatóság jóváhagyta a terjedelmet meghatározó dokumentumot, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató elemzi a pénzügyi szervezet szempontjából releváns általános és ágazatspecifikus fenyegetettségi információkat. Amennyiben a TLPT-hatóság általános fenyegetettségi helyzetet biztosított valamely tagállam pénzügyi ágazata számára, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató ezt a helyzetet használhatja kiindulási alapként a nemzeti fenyegetettségi helyzetet illetően. A fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató azonosítja a kiberfenyegetéseket és a pénzügyi szervezetet érintő meglévő vagy potenciális sérülékenységeket. Ezen túlmenően a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató a pénzügyi szervezetre vonatkozó információkat gyűjt, és elemzi a konkrét, gyakorlatban hasznosítható és kontextusba helyezett, célpontra vonatkozó és fenyegetettségi információkat, többek között az ellenőrzést végző csapattal és a tesztvezetőkkel folytatott konzultáció révén.

(2) A fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató bemutatja a releváns fenyegetéseket és a célzott fenyegetettségi információkat, és javaslatot tesz a szükséges forgatókönyvekre az ellenőrzést végző csapatnak, a tesztelőknek és a tesztvezetőknek. A javasolt forgatókönyveknek az azonosított fenyegető szereplők és a kapcsolódó taktikák, módszerek és eljárások tekintetében eltérőeknek kell lenniük, és valamennyi olyan kritikus és fontos funkciót meg kell célozniuk, amelyekre a TLPT kiterjed.

(3) Az ellenőrzést végző csapat vezetője legalább három forgatókönyvet kiválaszt a TLPT lefolytatására az alábbi elemek mindegyike alapján:

a) a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató ajánlása és az egyes forgatókönyvek fenyegetés alapú jellege;

b) a tesztvezetők által szolgáltatott adatok;

c) a javasolt végrehajtási forgatókönyvek megvalósíthatósága a tesztelők szakértői megítélése alapján;

d) a pénzügyi szervezet mérete, összetettsége és általános kockázati profilja, valamint a szolgáltatásai, tevékenységei és működése jellege, nagyságrendje és összetettsége.

(4) A kiválasztott forgatókönyvek közül csak egy lehet nem fenyegetés alapú, és alapulhat olyan előremutató és potenciálisan fiktív fenyegetésen, amely a pénzügyi szervezetet érintő fenyegetettségi helyzet várható alakulására tekintettel magas prediktív, előrejelzési, opportunisztikus vagy várható értékkel bír.

Csoportos TLPT-k esetében – a tesztelésben részt vevő pénzügyi szervezetek kritikus vagy fontos funkcióit közvetlenül célzó forgatókönyvek sérelme nélkül – legalább egy forgatókönyvnek magában kell foglalnia a harmadik fél IKT-szolgáltatónak az azon pénzügyi szervezetek kritikus vagy fontos funkcióit támogató releváns, alapul szolgáló IKT-rendszereit, -folyamatait és -technológiáit, amelyekre a TLPT kiterjed.

Amennyiben a teszt csoporton belüli IKT-szolgáltatót is érintő közös TLPT – a tesztben részt vevő pénzügyi szervezetek kritikus vagy fontos funkcióit közvetlenül célzó forgatókönyvek sérelme nélkül – legalább egy forgatókönyvnek magában kell foglalnia a csoporton belüli IKT-szolgáltatónak az azon pénzügyi szervezetek kritikus vagy fontos funkcióit támogató releváns, alapul szolgáló IKT-rendszereit, -folyamatait és -technológiáit, amelyekre a TLPT kiterjed.

(5) A fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentést az ellenőrzést végző csapat rendelkezésére bocsátja, beleértve a (3) és (4) bekezdéssel összhangban kiválasztott forgatókönyveket is. A fenyegetettséggel kapcsolatos hírszerzésre vonatkozó jelentés a III. mellékletben meghatározott információkat tartalmazza.

(6) Az ellenőrzést végző csapat jóváhagyásra benyújtja a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentést a tesztvezetőnek. Amennyiben a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentés teljes, és biztosítja a hatékony TLPT elvégzését, a TLPT-hatóság jóváhagyja a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentést, és erről tájékoztatja az ellenőrzést végző csapat vezetőjét.

11. cikk

Tesztelési szakasz: a vörös csapat által végzett teszt

(1) A fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentés TLPT-hatóság általi jóváhagyását követően a tesztelők elkészítik a vörös csapat által végzett teszt tervét, amely tartalmazza a IV. mellékletben meghatározott információkat. A tesztelők a terjedelmet meghatározó dokumentumot és a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentést veszik alapul a támadási forgatókönyvek elkészítéséhez.

(2) A tesztelők konzultálnak az ellenőrzést végző csapattal, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatóval és a tesztvezetőkkel a vörös csapat által végzett teszt tervéről, beleértve a kommunikációs, eljárási és projektirányítási megállapodást, a kisegítés aktiválásának előkészítését és eseteit, valamint az ellenőrzést végző csapat és a tesztvezetők felé történő jelentéstétellel kapcsolatos megállapodásokat.

(3) Amennyiben a vörös csapat által végzett teszt terve teljes, és biztosítja a hatékony TLPT elvégzését, az ellenőrzést végző csapat és a TLPT-hatóság jóváhagyja a vörös csapat által végzett teszt tervét, és a TLPT-hatóság erről tájékoztatja az ellenőrzést végző csapat vezetőjét.

(4) A vörös csapat által végzett teszt tervének (3) bekezdéssel összhangban történő jóváhagyását követően a tesztelők elvégzik a TLPT-t a vörös csapat által végzett aktív tesztelési szakasz során.

(5) A vörös csapat által végzett aktív tesztelési szakasz időtartamának arányosnak kell lennie a TLPT terjedelmével, a TLPT-ben részt vevő pénzügyi szervezetek és harmadik fél IKT-szolgáltatók vagy csoporton belüli IKT-szolgáltatók nagyságrendjével, tevékenységével, összetettségével és számával, és minden esetben legalább 12 hétig kell tartania. A támadási forgatókönyvek egymás után vagy egyidejűleg is végrehajthatók. Az ellenőrzést végző csapat, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató, a tesztelők és a tesztvezetők megállapodnak a vörös csapat által végzett aktív tesztelési szakasz befejezéséről.

(6) Annak biztosítása érdekében, hogy a vörös csapat által végzett teszt terve teljes maradjon, és lehetővé tegye a hatékony TLPT elvégzését, az ellenőrzést végző csapat vezetője és a tesztvezetők jóváhagyják a vörös csapat által végzett teszt tervének a jóváhagyást követő bármely módosítását, beleértve az ütemezést, a terjedelmet, a célrendszereket és a tesztcélokat érintő módosításokat is.

(7) A tesztelők a vörös csapat által végzett aktív tesztelési szakasz teljes egészében legalább hetente jelentést tesznek az ellenőrzést végző csapatnak és a tesztvezetőknek a TLPT terén elért eredményekről, a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltató pedig továbbra is az ellenőrzést végző csapat rendelkezésére áll konzultáció és fenyegetettséggel kapcsolatos további hírszerzés céljából.

(8) Az ellenőrzést végző csapat kellő időben a vörös csapat által végzett teszt terve alapján kidolgozott segítséget nyújt „kisegítés” formájában. Az ellenőrzést végző csapat és a tesztvezetők jóváhagyásával további kisegítés nyújtható vagy az módosítható.

(9) Amennyiben a pénzügyi szervezet vagy annak harmadik fél IKT-szolgáltatója vagy csoporton belüli IKT-szolgáltatója személyzetének bármely tagja észleli a tesztelési tevékenységeket, az ellenőrzést végző csapat a tesztelőkkel konzultálva és a (10) bekezdés sérelme nélkül olyan intézkedéseket javasol és nyújt be a tesztvezetők számára validálás céljából, amelyek lehetővé teszik a TLPT folytatását, ugyanakkor biztosítják annak titkosságát.

(10) Kivételes körülmények között, amelyek a pénzügyi szervezet, a harmadik fél IKT-szolgáltatói vagy csoporton belüli IKT-szolgáltatói adataira gyakorolt hatással, eszközei károsodásával és kritikus vagy fontos funkcióinak, szolgáltatásainak vagy műveleteinek megzavarásával kapcsolatos kockázatot, illetve a partnereivel vagy a pénzügyi ágazattal kapcsolatos zavarok kockázatát idézik elő, az ellenőrzést végző csapat vezetője felfüggesztheti a TLPT-t, vagy végső esetben – amennyiben a TLPT folytatása egyébként nem lehetséges –, a TLPT-hatóság előzetes jóváhagyása mellett, korlátozott terjedelmű közös teszteléssel folytathatja a TLPT-t. A korlátozott terjedelmű közös tesztelés időtartamát bele kell számítani az (5) bekezdésben említett, a vörös csapat által végzett aktív tesztelési szakasz 12 hetes minimális időtartamába.

12. cikk

Lezárási szakasz

(1) A vörös csapat által végzett aktív tesztelési szakasz végét követően az ellenőrzést végző csapat vezetője tájékoztatja a kék csapatot arról, hogy TLPT-re került sor.

(2) A vörös csapat által végzett aktív tesztelési szakasz végétől számított 4 héten belül a tesztelők benyújtják az ellenőrzést végző csapatnak a vörös csapat V. mellékletben meghatározott információkat tartalmazó tesztjelentését.

(3) Az ellenőrzést végző csapat indokolatlan késedelem nélkül megosztja a vörös csapat tesztjelentését a kék csapattal és a tesztvezetőkkel.

A tesztvezetők kérésére az első albekezdésben említett jelentés nem tartalmazhat érzékeny információkat.

(4) A vörös csapat tesztjelentésének kézhezvételét követően, azonban a vörös csapat által végzett aktív tesztelési szakasz végét követően legfeljebb 10 héten belül a kék csapat benyújtja az ellenőrzést végző csapatnak a kék csapat VI. mellékletben meghatározott információkat tartalmazó tesztjelentését. Az ellenőrzést végző csapat indokolatlan késedelem nélkül megosztja a kék csapat tesztjelentését a tesztelőkkel és a tesztvezetőkkel.

A tesztvezetők kérésére az első albekezdésben említett jelentés nem tartalmazhat érzékeny információkat.

(5) A kék csapat és a tesztelők legkésőbb 10 héttel a vörös csapat által végzett aktív tesztelési szakasz végét követően visszajátsszák a TLPT során végrehajtott támadó és védekező intézkedéseket. Az ellenőrzést végző csapat közös tesztelést is lefolytat a kék csapat és a tesztelők által közösen azonosított témákban a teszt során azonosított sérülékenységek és adott esetben olyan problémák alapján, amelyeket a vörös csapat által végzett aktív tesztelési szakaszban nem lehetett tesztelni.

(6) Az intézkedések visszajátszásának és a közös tesztelésnek a befejezését követően az ellenőrzést végző csapat, a kék csapat, a tesztelők és a fenyegetettséggel kapcsolatos hírszerzést nyújtó szolgáltatók visszajelzést adnak egymásnak a TLPT-folyamatról. A tesztvezetők is adhatnak visszajelzést.

(7) Miután a TLPT-hatóság értesítette az ellenőrzést végző csapatot arról, hogy megállapította, hogy a kék csapat tesztjelentése és a vörös csapat tesztjelentése tartalmazza az V. és VI. mellékletben meghatározott információkat, a pénzügyi szervezet az (EU) 2022/2554 rendelet 26. cikkének (6) bekezdésében említettek szerint 8 héten belül jóváhagyásra benyújtja a TLPT releváns megállapításait összefoglaló, a VII. mellékletben meghatározott elemeket tartalmazó jelentést a TLPT-hatóságnak.

A TLPT-hatóság kérésére az első albekezdésben említett jelentés nem tartalmazhat érzékeny információkat.

13. cikk

Korrekciós terv

(1) Az e rendelet 12. cikkének (7) bekezdésében említett értesítéstől számított 8 héten belül a pénzügyi szervezet benyújtja az (EU) 2022/2554 rendelet 26. cikkének (6) bekezdésében említett korrekciós terveket és dokumentációt a TLPT-hatóságnak és, amennyiben az eltér, a pénzügyi szervezet illetékes hatóságának.

(2) Az (1) bekezdésben említett korrekciós terv a TLPT keretében tett minden egyes megállapítás tekintetében tartalmazza a következőket:

a) a feltárt hiányosságok leírása;

b) a javasolt korrekciós intézkedések, valamint azok rangsorolásának és várható befejezésének leírása, beleértve adott esetben az azonosítási, védelmi, észlelési és reagálási képességek javítását célzó intézkedéseket;

c) a kiváltó okok elemzése;

d) a pénzügyi szervezetnek a javasolt korrekciós intézkedések vagy fejlesztések végrehajtásáért felelős személyzete vagy funkciói;

e) a b) pontban említett intézkedések végre nem hajtásával kapcsolatos kockázatok, valamint adott esetben az ilyen intézkedések végrehajtásához kapcsolódó kockázatok.

14. cikk

Igazolás

(1) Az (EU) 2022/2554 rendelet 26. cikkének (7) bekezdésében említett igazolás tartalmazza a VIII. mellékletben meghatározott információkat.

(2) Amennyiben egy TLPT-ben több TLPT-hatóság is részt vett, a vezető TLPT-hatóság adja ki a tesztelt pénzügyi szervezeteknek az (EU) 2022/2554 rendelet 26. cikkének (7) bekezdésében említett igazolást.

15. cikk

Belső tesztelők igénybevétele

(1) A pénzügyi szervezetek kidolgozzák a belső tesztelők igénybevételére vonatkozó alábbi intézkedések mindegyikét:

a) a TLPT-ben részt vevő belső tesztelők irányítására vonatkozó szabályzat kidolgozása és végrehajtása;

b) olyan intézkedések, amelyek biztosítják, hogy a belső tesztelők TLPT végrehajtására történő alkalmazása ne befolyásolja hátrányosan a pénzügyi szervezet IKT-vonatkozású eseményekkel kapcsolatos általános védelmi és ellenállási képességeit, és ne befolyásolja jelentős mértékben a TLPT során az IKT-vonatkozású feladatokra fordított erőforrások rendelkezésre állását;

c) olyan intézkedések, amelyek biztosítják, hogy a belső tesztelők elegendő erőforrással és kapacitással rendelkezzenek a TLPT elvégzéséhez.

Az a) pontban említett szabályzatnak meg kell felelnie az alábbiaknak:

a) tartalmaznia kell a belső tesztelők alkalmasságának, kompetenciájának és esetleges összeférhetetlenségeinek értékelésére vonatkozó kritériumokat, és meg kell határoznia a vezetői feladatok körét a tesztelési folyamaton belül;

b) dokumentálni kell és időközönként felül kell vizsgálni;

c) elő kell írnia, hogy a belső tesztelési csapatnak tartalmaznia kell egy tesztvezetőt és legalább két további tagot;

d) elő kell írnia, hogy a tesztcsapat valamennyi tagját a pénzügyi szervezetnek vagy egy csoporton belüli IKT-szolgáltatónak kellett alkalmaznia a tesztet megelőző 12 hónapban;

e) rendelkezéseket kell tartalmaznia a belső tesztelők behatolási tesztelés és vörös csapat által végzett tesztelés elvégzéséről szóló képzésére vonatkozóan.

(2) Amennyiben valamely TLPT-hatóság az (EU) 2022/2554 rendelet 27. cikke (2) bekezdésének a) pontjával összhangban jóváhagyja a belső tesztelők igénybevételét, a TLPT-hatóság figyelembe veszi az e rendelet 7. cikkének (1) bekezdésében meghatározott követelményeket.

(3) Belső tesztelők igénybevétele esetén a pénzügyi szervezet biztosítja, hogy az ilyen igénybevétel szerepeljen a következő dokumentumokban:

a) a teszt elindításával kapcsolatos, 9. cikkben említett dokumentumok;

b) a vörös csapat 12. cikk (2) bekezdésében említett tesztjelentése;

c) az (EU) 2022/2554 rendelet 26. cikkének (6) bekezdésében említett, a TLPT releváns megállapításait összefoglaló jelentés.

(4) A csoporton belüli IKT-szolgáltató által alkalmazott tesztelők a pénzügyi szervezet belső tesztelőinek tekintendők.

16. cikk

Együttműködés és kölcsönös elismerés

(1) Az egynél több tagállamban – többek között fióktelepen keresztül – szolgáltatásokat nyújtó pénzügyi szervezetekkel kapcsolatos TLPT végrehajtása céljából a TLPT-hatósága:

a) megállapítja, hogy a fogadó tagállamok mely TLPT-hatóságait kell bevonni, figyelembe véve, hogy a fogadó tagállamokban a szervezet működtet vagy megoszt-e egy vagy több kritikus vagy fontos funkciót;

b) tájékoztatja az a) ponttal összhangban azonosított TLPT-hatóságokat a pénzügyi szervezettel kapcsolatos TLPT elvégzésére vonatkozó döntésről;

c) a TLPT-hatóságok eltérő megállapodásának hiányában a pénzügyi szervezet TLPT-hatósága vezeti a TLPT-t.

A fogadó tagállamok TLPT-hatóságai a TLPT jövőbeli lefolytatására vonatkozó tájékoztatástól számított 20 munkanapon belül jelezhetik érdeklődésüket a TLPT megfigyelőként való követése iránt, vagy kijelölhetnek egy tesztvezetőt a TLPT-ben való részvételre. A vezető TLPT-hatóság a TLPT-ben megfigyelőként eljáró valamennyi TLPT-hatóság rendelkezésére bocsátja a terjedelmet meghatározó dokumentumot, a teszt összefoglaló jelentését, a korrekciós tervet és az igazolást.

A vezető TLPT-hatóság koordinálja az összes részt vevő TLPT-hatóságot a teszt során, és meghozza a TLPT megfelelő és hatékony végrehajtásához szükséges valamennyi döntést. A vezető TLPT-hatóság meghatározhatja a részt vevő TLPT-hatóságok maximális számát, ha máskülönben veszélybe kerülne a TLPT hatékony lefolytatása.

(2) Amennyiben egy pénzügyi szervezet ugyanazt a csoporton belüli IKT-szolgáltatót használja, mint más tagállamokban letelepedett pénzügyi szervezetek, vagy valamely csoporthoz tartozik, és közös IKT-rendszereket használ az ugyanazon csoporthoz tartozó, más tagállamokban letelepedett pénzügyi szervezetekkel, a pénzügyi szervezet TLPT-hatósága kapcsolatba lép az ugyanazon csoporton belüli IKT-szolgáltatót használó vagy a csoport részeként közös IKT-rendszereket használó többi pénzügyi szervezet TLPT-hatóságaival, és együtt értékelik a közös TLPT elvégzésének megvalósíthatóságát és alkalmasságát. A közös TLPT-t előnyben kell részesíteni az egyedi TLPT-vel szemben, amennyiben az kevesebb költséggel és erőforrással jár a pénzügyi szervezetek és a TLPT-hatóságok számára, feltéve, hogy ez nem sérti a tesztelés megbízhatóságát és hatékonyságát.

(3) A közös TLPT végrehajtása céljából:

a) a pénzügyi szervezetek TLPT-hatóságai megállapodnak arról, hogy mely pénzügyi szervezetet jelölik ki a TLPT elvégzésére, figyelembe véve a csoport szerkezetét és a teszt hatékonyságát;

b) a közös TLPT-ben részt vevő pénzügyi szervezetek TLPT-hatóságainak eltérő megállapodása hiányában az a) pont szerint kijelölt pénzügyi szervezet TLPT-hatósága vezeti a TLPT-t;

c) a közös TLPT vezetésére kijelölt pénzügyi szervezettől eltérő pénzügyi szervezetek TLPT-hatóságai jelezhetik érdeklődésüket a TLPT megfigyelőként való követése iránt, vagy kijelölhetnek egy tesztvezetőt az adott TLPT-hez.

A vezető TLPT-hatóság koordinálja a közös TLPT-ben részt vevő összes TLPT-hatóságot, és meghozza a közös TLPT megbízható és hatékony végrehajtásához szükséges valamennyi döntést.

(4) Amennyiben egy pénzügyi szervezet az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdésében említett olyan csoportos TLPT-t kíván lefolytatni, amely más tagállamokban letelepedett pénzügyi szervezetek bevonásával járhat, TLPT-hatósága felveszi a kapcsolatot a többi pénzügyi szervezet TLPT-hatóságaival, és az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdésével összhangban együtt értékelik a csoportos TLPT elvégzésének megvalósíthatóságát és alkalmasságát.

(5) Az (EU) 2022/2554 rendelet 26. cikkének (4) bekezdésében említett csoportos TLPT végrehajtása céljából:

a) a pénzügyi szervezetek TLPT-hatóságai megállapodnak arról, hogy mely pénzügyi szervezetet jelölik ki a csoportos TLPT lefolytatására, figyelembe véve a harmadik fél IKT-szolgáltató által a pénzügyi szervezeteknek nyújtott IKT-szolgáltatásokat és a teszt hatékonyságát;

b) a csoportos TLPT-ben részt vevő pénzügyi szervezetek TLPT-hatóságainak eltérő megállapodása hiányában az a) pont szerint kijelölt pénzügyi szervezet TLPT-hatósága vezeti a TLPT-t;

c) a csoportos TLPT vezetésére kijelölt pénzügyi szervezettől eltérő pénzügyi szervezetek TLPT-hatóságai jelezhetik érdeklődésüket a TLPT megfigyelőként való követése iránt, vagy kijelölhetnek egy tesztvezetőt az adott TLPT-hez.

A vezető TLPT-hatóság koordinálja a csoportos TLPT-ben részt vevő összes TLPT-hatóságot, és meghozza a csoportos TLPT megbízható és hatékony végrehajtásához szükséges valamennyi döntést.

(6) Amennyiben valamely TLPT elvégzésére kötelezett pénzügyi szervezet tekintetében annak TLPT-hatósága eltér az (EU) 2022/2554 rendelet 46. cikkében említett illetékes hatóságától, az említett hatóságok a TLPT-vel kapcsolatos valamennyi ügy tekintetében megosztanak minden releváns információt a TLPT végrehajtása vagy feladataiknak az említett rendelettel összhangban történő ellátása céljából.

17. 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, 2025. február 13-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

A projektterv tartalma (9. cikk (2) bekezdés a) pont)

Adat	Szükséges információk
A projekttervért felelős személy, azaz az ellenőrzést végző csapat vezetője	Név Elérhetőségek
Tesztelők	☐ belső ☐ külső ☐ mindkettő
A 9. cikk (2) bekezdésének d) pontjával és a 9. cikk (4) bekezdésének a) pontjával összhangban kiválasztott kommunikációs csatornák, beleértve a következőket: a) a használandó e-mail-titkosítás; b) a használandó online adatszobák; c) a használandó azonnali üzenetküldő alkalmazások.	
A TLPT kódneve	
A pénzügyi szervezet által más tagállamokban működtetett kritikus és fontos funkciók, ha vannak	1. a valamely más tagállamban működtetett kritikus és fontos funkciók listája 2. minden egyes kritikus és fontos funkció esetében annak a tagállamnak vagy azoknak a tagállamoknak a megjelölése, amelyben vagy amelyekben a funkciót működtetik
A harmadik fél IKT-szolgáltatók által támogatott kritikus és fontos funkciók, ha vannak	3. a harmadik fél IKT-szolgáltatók által támogatott kritikus és fontos funkciók listája 4. minden egyes funkció esetében a harmadik fél IKT-szolgáltató azonosítása
A következők befejezésének várható határideje:	
1. Előkészítési szakasz, a 9. cikkel összhangban	éééé-hh-nn
2. Tesztelési szakasz, a 10. és 11. cikkel összhangban	éééé-hh-nn
3. Lezárási szakasz, a 12. cikkel összhangban	éééé-hh-nn
4. Korrekciós terv, a 13. cikkel összhangban	éééé-hh-nn

II. MELLÉKLET

A terjedelmet meghatározó dokumentum tartalma (9. cikk (6) bekezdés)

(1) A terjedelmet meghatározó dokumentumnak tartalmaznia kell a pénzügyi szervezet által azonosított valamennyi kritikus és fontos funkció jegyzékét.

(2) Az egyes azonosított kritikus és fontos funkciókra vonatkozóan a következő információkat kell feltüntetni:

a) amennyiben a TLPT nem terjed ki az adott kritikus vagy fontos funkcióra, azon okok magyarázata, amelyek miatt nem terjed ki arra a funkcióra;

b) amennyiben a TLPT kiterjed az adott kritikus vagy fontos funkcióra:

i. azon okok magyarázata, amelyek miatt kiterjed arra a funkcióra;

ii. az adott kritikus vagy fontos funkciót támogató, azonosított IKT-rendszer(ek);

iii. az egyes azonosított IKT-rendszerek esetében:

1. kiszervezték-e, és ha igen, a harmadik fél IKT-szolgáltató neve;

2. a joghatóságok, amelyekben az IKT-rendszert használják;

3. az előzetes tesztcél(ok) magas szintű leírása, feltüntetve, hogy az egyes tesztcélok a bizalmas jelleg, az integritás, a hitelesség vagy a rendelkezésre állás mely biztonsági szempontját fedik le.

III. MELLÉKLET

A fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentés tartalma (10. cikk (5) bekezdés)

A fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentésnek a következők mindegyikére vonatkozóan információkat kell tartalmaznia:

(1) A hírszerzési kutatás általános hatóköre, amely legalább a következőket magában foglalja:

a) azon kritikus és fontos funkciók, amelyekre a TLPT kiterjed;

b) ezek földrajzi helyzete;

c) a használt hivatalos uniós nyelv;

d) a releváns harmadik fél IKT-szolgáltatók;

e) az időszak, amely alatt az információt összegyűjtik.

(2) Annak átfogó értékelése, hogy milyen konkrét, hasznosítható információk találhatók a pénzügyi szervezetről, beleértve a következőket:

a) a munkavállalók felhasználónevei és jelszavai;

b) a pénzügyi szervezet hivatalos doménjeivel összetéveszthető hasonló domének;

c) műszaki felderítés: sérülékeny vagy kihasználható szoftverek, rendszerek és technológiák;

d) a munkavállalók által az interneten közzétett, a pénzügyi szervezetre vonatkozó információk, amelyek támadás céljára felhasználhatók;

e) a „dark weben” megvásárolható információk;

f) az interneten vagy nyilvános hálózatokon rendelkezésre álló bármely egyéb releváns információ;

g) adott esetben fizikai célpontokkal kapcsolatos információk, beleértve a pénzügyi szervezet létesítményeibe való belépés módjait is.

(3) Fenyegetettséggel kapcsolatos hírszerzési elemzés, figyelembe véve az általános fenyegetettségi helyzetet és a pénzügyi szervezet sajátos helyzetét, beleértve legalább a következőket:

a) a geopolitikai környezet;

b) a gazdasági környezet;

c) technológiai trendek és a pénzügyi szolgáltatási ágazat tevékenységeihez kapcsolódó egyéb trendek.

(4) Azon rosszindulatú szereplők (konkrét egyén/csoport vagy általános osztály) fenyegetettségi profiljai, akik vagy amelyek a pénzügyi szervezetet célozhatják meg, beleértve a pénzügyi szervezet azon rendszereit, amelyeket a rosszindulatú szereplők a legnagyobb valószínűséggel veszélyeztethetnek vagy vehetnek célba, a potenciális célpontkiválasztás lehetséges motivációját, szándékát és indokait, valamint a támadók lehetséges működési módját.

(5) Fenyegetettségi forgatókönyvek: legalább három végpontok közötti fenyegetettségi forgatókönyv a 4. ponttal összhangban azonosított azon fenyegetettségi profilokat illetően, amelyek esetében a fenyegetettségi súlyossági pontszámok a legmagasabbak. A fenyegetettségi forgatókönyveknek le kell írniuk a végpontok közötti támadási útvonalat, és legalább a következőket tartalmazniuk kell:

a) egy olyan forgatókönyv, amely magában foglalja többek között a szolgáltatás rendelkezésre állásának veszélyeztetését;

b) egy olyan forgatókönyv, amely magában foglalja többek között az adatintegritás veszélyeztetését;

c) egy olyan forgatókönyv, amely magában foglalja többek között az információk bizalmas jellegének veszélyeztetését.

(6) Adott esetben a 10. cikk (4) bekezdésében említett, nem fenyegetés alapú forgatókönyv leírása.

IV. MELLÉKLET

A vörös csapat által végzett teszt tervének tartalma (11. cikk (1) bekezdés)

A vörös csapat által végzett teszt tervének a következők mindegyikére vonatkozóan információkat kell tartalmaznia:

a) kommunikációs csatornák és folyamatok;

b) a támadás során engedélyezett és nem engedélyezett taktikák, módszerek és eljárások, beleértve a pszichológiai manipuláció etikai korlátait;

c) a tesztelők által követendő kockázatkezelési intézkedések;

d) az egyes forgatókönyvek leírása, beleértve a következőket:

   i. a szimulált fenyegető szereplő;

   ii. ennek szándéka, motivációja és célja;

   iii. a célpontot jelentő funkció(k) és a támogató IKT-rendszer(ek);

   iv. a bizalmas jelleggel, integritással, hitelességgel vagy rendelkezésre állással kapcsolatos megcélzott szempontok;

   v. tesztcélok;

e) az egyes várható támadási útvonalak részletes leírása, beleértve az előfeltételeket és az ellenőrzést végző csapat által biztosítandó lehetséges kisegítéseket, beleértve az azok biztosítására és lehetséges felhasználására vonatkozó határidőket;

f) a vörös csapat által végzett tevékenységek ütemezése, beleértve az egyes forgatókönyvek végrehajtására vonatkozó ütemezést is, legalább azon három szakasz szerinti bontásban, amelyeken a tesztelő a tesztelési szakasz során végighalad, sorrendben a pénzügyi szervezetek IKT-rendszereibe való behatolás, az IKT-rendszerek bejárása, majd végső soron a tevékenységek végrehajtása a célpontokon és végezetül az IKT-rendszerekből való kivonulás (belépési, bejárási és kilépési szakaszok);

g) a pénzügyi szervezetek infrastruktúrájának sajátosságai, amelyeket a tesztelés során figyelembe kell venni;

h) adott esetben a tesztelők számára a forgatókönyvek végrehajtásához szükséges további információk vagy egyéb erőforrások.

V. MELLÉKLET

A vörös csapat tesztjelentésének tartalma (12. cikk (2) bekezdés)

A vörös csapat tesztjelentésének a következők mindegyikére vonatkozóan információkat kell tartalmaznia:

a) a végrehajtott támadásra vonatkozó információk, beleértve a következőket:

   i. a megcélzott kritikus és fontos funkciók, valamint az azokat támogató azonosított IKT-rendszerek, -folyamatok és -technológiák, a vörös csapat által végzett teszt tervében meghatározottak szerint;

   ii. az egyes forgatókönyvek összefoglalása;

   iii. az elért és el nem ért tesztcélok;

   iv. a sikeresen és sikertelenül bejárt támadási útvonalak;

   v. a sikeresen és sikertelenül alkalmazott taktikák, módszerek és eljárások;

   vi. adott esetben a vörös csapat által végzett teszt tervétől való eltérések;

   vii. adott esetben a nyújtott kisegítések;

b) a kék csapat által a támadás rekonstruálása és hatásainak enyhítése érdekében végzett minden olyan intézkedés, amelyről a tesztelők tudnak;

c) feltárt sérülékenységek és egyéb megállapítások, többek között:

   i. a sérülékenység és az egyéb megállapítás leírása, beleértve a kritikusságát is;

   ii. a sikeres támadások kiváltó okainak elemzése;

   iii. a korrekcióra vonatkozó ajánlások, beleértve a korrekció prioritásának megjelölését is.

VI. MELLÉKLET

A kék csapat tesztjelentésének tartalma (12. cikk (4) bekezdés)

A kék csapat tesztjelentésének a következők mindegyikére vonatkozóan információkat kell tartalmaznia:

(1) a tesztelők által a vörös csapat tesztjelentésében leírt minden egyes támadási lépésre vonatkozóan:
   a) az észlelt támadási cselekmények listája;
   b) az ezen észlelésekhez tartozó naplóbejegyzések;

(2) a tesztelők megállapításainak és ajánlásainak értékelése;

(3) a tesztelők támadásának a kék csapat által összegyűjtött bizonyítéka;

(4) a tesztelők által végrehajtott sikeres támadások kiváltó okainak elemzése a kék csapat részéről;

(5) a levont tanulságok és a felismert fejlesztési lehetőségek listája;

(6) a közös tesztelés keretében kezelendő témák listája.

VII. MELLÉKLET

Az (EU) 2022/2554 rendelet 26. cikkének (6) bekezdésében említett, a TLPT releváns megállapításait összefoglaló jelentésben szereplő adatok

A teszt összefoglaló jelentésének a következők mindegyikére vonatkozóan információkat kell tartalmaznia:

a) az érintett felek;

b) a projektterv;

c) a validált terjedelem, beleértve annak indokait, hogy a TLPT miért terjed vagy nem terjed ki bizonyos kritikus és fontos funkciókra, valamint az azokat támogató azonosított IKT-rendszerekre, -folyamatokra és -technológiákra;

d) a kiválasztott forgatókönyvek és a fenyegetettséggel kapcsolatos hírszerzésre vonatkozó célzott jelentéstől való bármely jelentős eltérés;

e) a végrehajtott támadási útvonalak, valamint az alkalmazott taktikák, módszerek és eljárások;

f) az elért és el nem ért tesztcélok;

g) adott esetben a vörös csapat által végzett teszt tervétől való eltérések;

h) adott esetben a kék csapat általi észlelések;

i) közös tesztelés a tesztelési szakaszban, amennyiben ilyenre sor került, és az ahhoz kapcsolódó feltételek;

j) adott esetben a felhasznált kisegítések;

k) a megtett kockázatkezelési intézkedések;

l) a feltárt sérülékenységek és egyéb megállapítások, ideértve azok kritikus jellegét is;

m) a sikeres támadások kiváltó okainak elemzése;

n) magas szintű korrekciós terv, amely összekapcsolja a sérülékenységeket és az egyéb megállapításokat, azok kiváltó okait és a korrekció prioritásait;

o) a kapott visszajelzésekből levont tanulságok.

VIII. MELLÉKLET

Az (EU) 2022/2554 rendelet 26. cikkének (7) bekezdésében említett igazolásban szereplő adatok

Az igazolásnak legalább az alábbi információk mindegyikét tartalmaznia kell:

a) az elvégzett TLPT-re vonatkozóan:

   i. a TLPT kezdő és záró időpontja;

   ii. a kritikus és fontos funkciók, amelyekre a teszt kiterjed;

   iii. adott esetben azon kritikus vagy fontos funkciókra vonatkozó információk, amelyekre a teszt kiterjed, de amelyek tekintetében a TLPT-t nem végezték el;

   iv. adott esetben a TLPT-ben részt vevő egyéb pénzügyi szervezetek;

   v. adott esetben a TLPT-ben részt vevő harmadik fél IKT-szolgáltatók;

   vi. a tesztelőkre vonatkozóan:

      1. igénybe vettek-e belső tesztelőket;

      2. a pénzügyi szervezet alkalmazta-e az 5. cikk (3) bekezdésének második albekezdését;

   vii. a vörös csapat által végzett aktív tesztelési szakasz időtartama naptári napokban;

b) amennyiben a TLPT-ben több TLPT-hatóság is részt vett, a többi TLPT-hatóság felsorolása, és hogy milyen minőségben vettek részt;

c) a TLPT-hatóság által az igazolás céljából megvizsgált dokumentumok jegyzéke.