EBA/GL/2017/17

12/01/2018

Iránymutatások

az (EU) 2015/2366 irányelv (PSD2) szerinti pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről

1. Megfelelés és beszámolási kötelezettségek

Az iránymutatások jogállása

1. Az e dokumentumban szereplő iránymutatásokat az EBH az 1093/2010/EU rendelet[1] 16. cikkének rendelkezéseivel összhangban adta ki. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése szerint az illetékes hatóságok és pénzügyi intézmények minden erőfeszítést megtesznek azért, hogy megfeleljenek az iránymutatásoknak.

2. Az iránymutatások rögzítik az EBH álláspontját azzal kapcsolatban, hogy mi a megfelelő felügyeleti gyakorlat a Pénzügyi Felügyeletek Európai Rendszerében, és miként kell alkalmazni az uniós jogot egy adott területen belül. Az 1093/2010/EU rendelet 4. cikkének (2) bekezdésében meghatározott, az iránymutatások hatálya alá tartozó illetékes hatóságok azzal tesznek eleget az iránymutatásnak, hogy megfelelően beépítik azt saját felügyeleti gyakorlataikba (pl. saját jogi kereteik vagy felügyeleti folyamataik módosításával), beleértve azokat az eseteket is, ahol az iránymutatás elsősorban intézményekre vonatkozik.

Adatszolgáltatási követelmények

3. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése értelmében az egyes illetékes hatóságok 12.03.2018-ig kötelesek értesíteni az EBH-t arról, hogy megfelelnek-e vagy meg kívánnak-e felelni ennek az iránymutatásnak, és ha nem, úgy tájékoztatniuk kell az EBH-t a meg nem felelés indokairól. Amennyiben a fenti határidőig ilyen értesítés nem érkezik, az EBH úgy tekinti, hogy a szóban forgó illetékes hatóság nem felel meg az iránymutatásnak. Az értesítéseket „EBA/GL/2017/17” hivatkozással az EBH honlapján szereplő formanyomtatványon kell megküldeni a compliance@eba.europa.eu címre. Az értesítéseket olyan személyek nyújthatják be, akik megfelelő felhatalmazással rendelkeznek arra nézve, hogy illetékes hatóságuk nevében nyilatkozzanak annak megfeleléséről. Az EBH-nak a megfeleléssel kapcsolatban bekövetkező bármely változást is be kell jelenteni.

4. Az értesítéseket a 16. cikk (3) bekezdésével összhangban közzéteszik az EBH honlapján.

[1] 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.).

2. Tárgy, alkalmazási kör és fogalommeghatározások

Tárgy és alkalmazási kör

5. Ezen iránymutatásokkal az EBH az (EU) 2015/2366/EU irányelv[2] (PSD2) 95. cikkének (3) bekezdése által rá ruházott megbízatást teljesíti.

6. Ezek az iránymutatások követelményeket határoznak meg a pénzforgalmi szolgáltatók által az (EU) 2015/2366 irányelv 95. cikkének (1) bekezdésével összhangban meghozandó, az általuk nyújtott pénzforgalmi szolgáltatásokhoz kapcsolódó működési és biztonsági kockázatok kezelését szolgáló biztonsági intézkedések kidolgozása, végrehajtása és felügyelete tekintetében.

Címzettek

7. Ezen iránymutatások címzettjei a 2015/2366 irányelv 4. cikkének (11) bekezdésében meghatározott és az (EU) 1093/2010 rendelet 4. cikke (1) bekezdésének fogalommeghatározásában „pénzügyi intézményekként” említett pénzforgalmi szolgáltatók és az említett rendelet 4. cikke (2) bekezdésének i. alpontjában a hatályon kívül helyezett 2007/64/EK irányelvre [3] (a jelenlegi (EU) 2015/2366 irányelv[4]) való hivatkozással meghatározott illetékes hatóságok.

Fogalommeghatározások

8. Eltérő rendelkezés hiányában ezen iránymutatások az (EU) 2015/2366 irányelvben használt és meghatározott fogalmakat azzal egyező módon értelmezik. Ezen túlmenően ezeknek az iránymutatásoknak az alkalmazásában a következő fogalmak az alábbi jelentéssel bírnak:

[2] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).
[3] Az Európai Parlament és a Tanács 2007. november 13-i 2007/64/EK irányelve a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről (HL L 319., 2007.12.5., 1. o.).
[4] AZ (EU) 2015/2366 irányelv 114. cikke második albekezdésének megfelelően a hatályon kívül helyezett 2007/64/EK irányelvre történő bármely hivatkozást az (EU) 2015/2366 irányelvre történő hivatkozásként kell értelmezni, az (EU) 2015/2366 irányelv II. mellékletében foglalt megfelelési táblázatnak megfelelően.

Vezető testület	– Azon pénzforgalmi szolgáltatók tekintetében, amelyek hitelintézetek, ez a meghatározás a 2013/36/EU irányelv[5] 3. cikke (1) bekezdésének 7. pontjában foglalt fogalommeghatározással megegyező jelentéssel bír; – Azon pénzforgalmi szolgáltatók esetében, amelyek pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények, ez a meghatározás a pénzforgalmi szolgáltatók vezető tisztségviselőit vagy az irányításért felelős tisztségviselőket jelenti, valamint adott esetben a pénzforgalmi szolgáltatók pénzforgalmi szolgáltatási tevékenységeinek irányításáért felelős tisztségviselőket; – Az (EU) 2015/2366 irányelv 1. cikk (1) bekezdésének c), e) és f) pontjában említett pénzforgalmi szolgáltatók tekintetében ez a meghatározás az alkalmazandó uniós vagy nemzeti jogban az e meghatározáshoz rendelt jelentéssel bír.
Működési és biztonsági esemény	A pénzforgalmi szolgáltató által előre nem tervezett olyan egyedi esemény vagy egymáshoz kapcsolódó események olyan sorozata, amelynek a fizetéshez kapcsolódó szolgáltatás integritására, rendelkezésre állására, titkosságára, hitelességére és/vagy folyamatosságára negatív hatása van.
Felső vezetés	(a) Azon pénzforgalmi szolgáltatók tekintetében, amelyek hitelintézetek, ez a meghatározás a 2013/36/EU irányelv 3. cikke (1) bekezdésének 9. pontjában foglalt fogalommeghatározással megegyező jelentéssel bír; (b) Azon pénzforgalmi szolgáltatók esetében, amelyek pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények, ez a kifejezés az intézménynél vezetői feladatot ellátó természetes személyeket jelenti, akik felelősek és elszámoltathatóak a vezető testület előtt a pénzforgalmi szolgáltató mindennapi vezetéséért; (c) Az (EU) 2015/2366 irányelv 1. cikke (1) bekezdésének c), e) és f) pontjában említett pénzforgalmi szolgáltatók tekintetében ez a meghatározás az alkalmazandó uniós vagy nemzeti jogban az e kifejezéshez rendelt jelentéssel bír.
Biztonsági kockázat	A nem megfelelő vagy hibás belső folyamatokból vagy külső eseményekből eredő olyan kockázat, amely negatív hatással van vagy lehet az információs és kommunikációs technológiai (IKT) rendszerek és/vagy a pénzforgalmi szolgáltatások biztosításához felhasznált információk rendelkezésre állására, integritására és titkosságára. Ez magában foglalja a

[5] Az Európai Parlament és a Tanács 2013/36/EU irányelve 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.).

	kibertámadások jelentette vagy a nem megfelelő fizikai biztonságból eredő kockázatot is.
Kockázatvállalási hajlandóság	A kockázat azon aggregált szintje és típusai, amelyeket valamely intézmény stratégiai céljainak megvalósítása érdekében, kockázatviselési képességének keretein belül, üzleti modelljével összhangban hajlandó vállalni.

3. Végrehajtás

Alkalmazás időpontja

9. Ezek az iránymutatások 2018. január 13-ától alkalmazandók.

4. Iránymutatások

1 Iránymutatás: Általános elvek

1.1 Minden pénzforgalmi szolgáltatónak meg kell felelnie az ezekben az iránymutatásokban foglalt valamennyi rendelkezésnek. A részletezettség szintje legyen arányos a pénzforgalmi szolgáltató méretével és a pénzforgalmi szolgáltató által nyújtott vagy nyújtani kívánt konkrét szolgáltatások természetével, körével, összetettségével és kockázatosságával.

2 Iránymutatás: Vállalatirányítás

A működési és biztonsági kockázat kezelési keretrendszer

2.1 A pénzforgalmi szolgáltatóknak hatékony működési és biztonsági kockázatkezelési keretrendszert (a továbbiakban: kockázatkezelési keretrendszer), kell létrehozniuk, amelyet a vezető testületnek és ha értelmezhető a felső vezetésnek jóvá kell hagynia és felül kell vizsgálnia, legalább évente egy alkalommal. A kockázatkezelési keretrendszernek a működési és biztonsági kockázatok mérséklését célzó biztonsági intézkedésekre kell összpontosítania, és azt teljes mértékben be kell építeni a pénzforgalmi szolgáltató általános kockázatkezelési folyamataiba.

2.2 A kockázatkezelési keretrendszernek:

a) magában kell foglalnia az (EU) 2015/2366 irányelv 5. cikke (1) bekezdésének j) pontjában meghatározott, a biztonsági elvek átfogó leírását tartalmazó dokumentumot;

b) összhangban kell lennie a pénzforgalmi szolgáltató kockázatvállalási hajlandóságával;

c) meg kell határoznia és ki kell jelölni a legfontosabb szerepeket és felelősségeket, valamint a biztonsági intézkedések végrehajtásához és a biztonsági és működési kockázatok kezeléséhez szükséges jelentéstételi csatornákat;

d) ki kell dolgoznia a pénzforgalmi szolgáltató fizetéshez kapcsolódó tevékenységeiből származó valamennyi kockázat – amelyeknek a pénzforgalmi szolgáltató ki van téve – azonosításához, felméréséhez, nyomon követéséhez és kezeléséhez szükséges eljárásokat és rendszereket, ideértve az üzletmenet-folytonossági intézkedéseket.

2.3 A pénzforgalmi szolgáltatóknak biztosítaniuk kell, a kockázatkezelési keretrendszer megfelelően dokumentáltságát, és a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján történő aktualizálását.

2.4 A pénzforgalmi szolgáltatóknak meg kell vizsgálniuk, hogy az infrastruktúra, a folyamatok vagy az eljárások jelentősebb változtatása előtt és az általuk nyújtott pénzforgalmi szolgáltatások biztonságát érintő valamennyi jelentős működési és biztonsági esemény után haladéktalanul meg kell vizsgálniuk, hogy szükséges-e a kockázatkezelési keretrendszer módosítása vagy fejlesztése.

Kockázatkezelési és ellenőrzési modellek

2.5 A pénzforgalmi szolgáltatóknak a működési és biztonsági kockázatok azonosítása és kezelése érdekében három hatékony védelmi vonalat, vagy egy azzal egyenértékű belső kockázatkezelési és ellenőrzési modellt kell kidolgozniuk. A pénzforgalmi szolgáltatóknak biztosítaniuk kell, hogy a fent említett belső ellenőrzési modell elegendő felhatalmazással, függetlenséggel és forrásokkal rendelkezzen, és közvetlen jelentéstételi csatornái legyenek a vezető testület és ha értelmezhető a felső vezetés felé is.

2.6 Az ezekben az iránymutatásokban meghatározott biztonsági intézkedéseket felül kell vizsgáltatni az informatikai biztonság és a pénzforgalom területén szaktudással rendelkező, a pénzforgalmi szolgáltatón belüli vagy a pénzforgalmi szolgáltatótól működési szempontból független ellenőrökkel. Az ellenőrzések gyakoriságát és központi elemeit a megfelelő biztonsági kockázatok figyelembe vételével kell megállapítani.

Kiszervezés

2.7 Amennyiben a pénzforgalmi szolgáltatások működési funkcióit, többek között az informatikai rendszerek működtetését kiszervezik, a pénzforgalmi szolgáltatóknak biztosítaniuk kell az ezekben az iránymutatásokban meghatározott biztonsági intézkedések hatékony végrehajtását.

2.8 A pénzforgalmi szolgáltatóknak biztosítaniuk kell, hogy a szolgáltatókkal – amelyekhez az említett funkciókat kiszervezik – kötött szerződések és szolgáltatási megállapodások megfelelő és arányos biztonsági célokat, intézkedéseket és minőségi célokat tartalmazzanak. A pénzforgalmi szolgáltatóknak ellenőrizniük és biztosítaniuk kell az említett szolgáltatók e biztonsági céloknak, intézkedéseknek és minőségi céloknak való megfelelését.

3 Iránymutatás: Kockázatértékelés

A funkciók, a folyamatok és az eszközök meghatározása

3.1 A pénzforgalmi szolgáltatóknak meg kell határozniuk, ki kell dolgozniuk és rendszeresen aktualizálniuk kell üzleti funkcióik, alapvető feladataik és támogató folyamataik összességét tartalmazó nyilvántartásukat, annak érdekében, hogy feltérképezzék az egyes funkciók, feladatok és támogató folyamatok jelentőségét, valamint a működési és biztonsági kockázatokkal összefüggő kölcsönös függőségeiket.

3.2 A pénzforgalmi szolgáltatóknak meg kell határozniuk, ki kell dolgozniuk és rendszeresen aktualizálniuk kell az információs eszközök, különösen az IKT-rendszerek, azok konfigurációi, az egyéb infrastruktúrák, valamint az egyéb belső és külső rendszerekkel való összekapcsolódások összességét tartalmazó nyilvántartásukat, annak érdekében, hogy képesek legyenek kezelni az alapvető üzleti funkcióikat és folyamataikat támogató eszközöket.

A funkciók, a folyamatok és az eszközök osztályozása

3.3 A pénzforgalmi szolgáltatóknak kritikusság szerint osztályozniuk kell az azonosított üzleti funkciókat, támogató folyamatokat és információs eszközöket.

A funkciók, a folyamatok és az eszközök kockázatértékelése

3.4 A pénzforgalmi szolgáltatóknak biztosítaniuk kell a fenyegetések és a sebezhető pontok folyamatos nyomon követését és rendszeresen felül kell vizsgálniuk az üzleti funkcióikra, alapvető folyamataikra és információs eszközeikre hatással lévő kockázati forgatókönyveket. Az (EU) 2015/2366 irányelv 95. cikkének (2) bekezdése alapján a pénzforgalmi szolgáltatóknak – azon kötelezettségük részeként, hogy aktualizált és átfogó értékelést készítsenek az általuk nyújtott pénzforgalmi szolgáltatásokhoz kapcsolódó működési és biztonsági kockázatokról, valamint az e kockázatokra válaszul alkalmazott kockázatmérséklési intézkedések és ellenőrzési mechanizmusok megfelelőségéről, és azt elküldjék az illetékes hatóságnak – a fő működési és biztonsági kockázatok azonosítása és értékelése érdekében évente, vagy az illetékes hatóság által meghatározott rövidebb időközönként el kell végezniük és dokumentálniuk kell az általuk azonosított és osztályozott funkciók, folyamatok és információs eszközök kockázatértékelését. Szintén ilyen kockázatértékelést kell végezni a pénzforgalmi szolgáltatások biztonságát érintő infrastruktúra, folyamatok vagy eljárások minden jelentős változtatása előtt.

3.5 A pénzforgalmi szolgáltatóknak a kockázatértékelések alapján meg kell határozniuk, szükséges-e a meglévő biztonsági intézkedések, az alkalmazott technológiák és az eljárások vagy a nyújtott pénzforgalmi szolgáltatások megváltoztatása, és ha igen, milyen mértékben. A pénzforgalmi szolgáltatóknak figyelembe kell venniük a változtatások végrehajtásához szükséges időt, valamint azt az időt, amely a működési és biztonsági események, csalások és a pénzforgalmi szolgáltatások nyújtását zavaró esetleges hatások minimalizálását szolgáló megfelelő ideiglenes biztonsági intézkedések meghozatalához szükséges.

4 Iránymutatás: Védelem

4.1 A pénzforgalmi szolgáltatóknak az azonosított működési és biztonsági kockázatokkal szembeni megelőző biztonsági intézkedéseket kell kidolgozniuk és végrehajtaniuk. Ezeknek az intézkedéseknek az azonosított kockázatokkal összhangban lévő, megfelelő szintű biztonságot kell nyújtaniuk.

4.2 A pénzforgalmi szolgáltatóknak „mélységi védelmi” eljárást kell kidolgozniuk és végrehajtaniuk, oly módon, hogy a személyekre, a folyamatokra és a technológiákra kiterjedő többszintű felügyeleti rendszert létesítenek, amelyben minden egyes szint az előző szint biztonsági védőhálójaként szolgál. A mélységi védelem értelmében ugyanarra a kockázatra egynél több ellenőrzést kell meghatározni, mint például a négy szem elv, a kétfaktoros hitelesítés, a hálózatszegmentálás és a többszörös tűzfalak.

4.3 A pénzforgalmi szolgáltatóknak biztosítaniuk kell az alapvető logikai és fizikai eszközeik, erőforrásaik és a pénzforgalmi szolgáltatásaikat igénybe vevők érzékeny fizetési adatainak titkosságát, integritását és rendelkezésre állását, azok tárolása, továbbítása és használata alatt egyaránt. Ha az adatok személyes adatokat tartalmaznak, az intézkedéseket az (EU) 2016/679 rendeletnek[6], vagy ha alkalmazandó, a 45/2001/EK rendeletnek[7] megfelelően kell végrehajtani.

4.4 A pénzforgalmi szolgáltatóknak folyamatosan nyomon kell követniük, hogy a az aktuális működési környezetükben bekövetkező változtatások befolyásolják-e az érvényben levő biztonsági intézkedéseket, vagy szükségessé teszik-e további intézkedések beépítését a felmerülő kockázatok mérséklése érdekében. Ezeknek a változtatásoknak a pénzforgalmi szolgáltatók hatályos változáskezelési folyamatának részét kell képezniük, ami biztosítja a változtatások megfelelő előkészítését, tesztelését, dokumentálását és engedélyezését. Az észlelt biztonsági fenyegetések és az elvégzett változtatások alapján a releváns és ismert potenciális támadások forgatókönyveinek beépítése céljából tesztelést kell végrehajtani.

4.5 A pénzforgalmi szolgáltatóknak a pénzforgalmi szolgáltatások tervezése, kialakítása és nyújtása során biztosítaniuk kell a feladatkörök szétválasztását és a „legkisebb jogosultság” elvének alkalmazását. A pénzforgalmi szolgáltatóknak különös figyelmet kell fordítaniuk az informatikai környezetek elkülönítésére, különös tekintettel a fejlesztési, a tesztelési és az éles környezetre.

Az adatok és rendszerek integritása és bizalmassága

4.6 A pénzforgalmi szolgáltatások kialakításakor, fejlesztésekor és nyújtásakor a pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy a pénzforgalmi szolgáltatást igénybe vevő érzékeny fizetési adatainak összegyűjtése, továbbítása, feldolgozása, tárolása és/vagy archiválása valamint megjelenítése megfelelő és valós legyen, és csak a pénzforgalmi szolgáltatásainak nyújtásához szükséges mértékre korlátozódjon.

4.7 A pénzforgalmi szolgáltatóknak rendszeresen ellenőrizniük kell, hogy a pénzforgalmi szolgáltatások nyújtásához használt szoftver – beleértve a pénzforgalmi szolgáltatást igénybe vevők fizetéshez kapcsolódó szoftverét is – naprakész legyen, és a kritikus biztonsági javításokat telepít. A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy olyan integritás-ellenőrző mechanizmusok működjenek, amik ellenőrzik a pénzforgalmi szolgáltatásuk szoftverének, firmwarének és az adatainak az integritását.

Fizikai biztonság

[6] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

[7] Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

4.8 A pénzforgalmi szolgáltatóknak olyan fizikai biztonsági intézkedéseket kell foganatosítaniuk, amik megvédik a pénzforgalmi szolgáltatást igénybe vevők érzékeny fizetési adatait, valamint a pénzforgalmi szolgáltatások nyújtására használt IKT-rendszereket.

A hozzáférések felügyelete

4.9 Az IKT-rendszerekhez való fizikai és logikai hozzáférést csak az engedéllyel rendelkező személyeknek szabad biztosítani. Az engedélyt csak megfelelően képzett és ellenőrzött személy számára, az adott személy feladataival és felelősségi köreivel összhangban szabad kiadni. A pénzforgalmi szolgáltatóknak olyan felügyeletet kell bevezetniük, amelyek az IKT-rendszerekhez való hozzáférést megbízható módon azokra korlátozza, akiknél ez valós üzleti követelmény. Az adatokhoz és rendszerekhez való elektronikus hozzáférését az alkalmazások számára az adott szolgáltatás nyújtásához szükséges minimálisan elegendő szintre kell korlátozni.

4.10 A pénzforgalmi szolgáltatóknak szigorú felügyelet alatt kell tartaniuk az emelt szintű rendszerhozzáféréseket azáltal, hogy erősen korlátozzák és szorosan felügyelik a magasabb rendszerhozzáférési jogosultsággal rendelkező munkatársakat. Olyan felügyeletet kell bevezetni, mint például a szerepalapú hozzáférés, az emeltszintű felhasználók rendszertevékenységeinek naplózása és utólagos ellenőrzése, az erős hitelesítés és a szokásostól eltérő tevékenységek figyelése. A pénzforgalmi szolgáltatóknak a „szükséges ismeret ” elve alapján kell kezelniük az információs eszközökhöz és ezek támogató rendszereihez való hozzáférési jogokat. A hozzáférési jogokat rendszeres időközönként felül kell vizsgálni.

4.11 A hozzáférési naplókat a meghatározott üzleti funkciók, támogató folyamatok és információs eszközök kritikus jelentőségével arányos ideig kell megőrizni, az iránymutatások 3.1. és 3.2. pontjának megfelelően, az uniós és nemzeti jogszabályban előírt megőrzési követelmények sérelme nélkül. A pénzforgalmi szolgáltatóknak ezeket az információkat a pénzforgalmi szolgáltatások nyújtásában észlelt rendellenes tevékenységek felismerésének és kivizsgálásának megkönnyítésére kell felhasználniuk.

4.12 A biztonságos kommunikáció biztosítása és a kockázat csökkentése érdekében az IKT kritikus fontosságú összetevőihez távoli rendszergazdai hozzáférést csak erős hitelesítő megoldások mellett és a szükséges ismeret elve alapján szabad adni.

4.13 A hozzáférés-kezelési folyamatokhoz kapcsolódó termékek, eszközök és eljárások üzemeltetésének védenie kell a hozzáférés-kezelési folyamatokat a kompromittálódással vagy megkerüléssel szemben. Ebbe beletartozik a megfelelő termékek, eszközök és eljárások bevezetése, fenntartása, hatályon kívül helyezése és visszavonása.

5 Iránymutatás: Észlelés

Folyamatos felügyelet és észlelés

5.1 A pénzforgalmi szolgáltatóknak a pénzforgalmi szolgáltatások nyújtásában fellépő rendellenes tevékenységek feltárása érdekében az üzleti funkciók, támogató folyamatok és információs

eszközök folyamatos felügyeletéhez szükséges folyamatokat és mechanizmusokat kell kialakítaniuk és bevezetniük.. A folyamatos felügyelet keretében a pénzforgalmi szolgáltatóknak megfelelő és hatékony mechanizmusokkal kell rendelkezniük, hogy észleljék a fizikai vagy logikai behatolást, valamint a pénzforgalmi szolgáltatások nyújtásában használt információs eszközök titkosságának, integritásának és rendelkezésre állásának megsértését.

5.2 A folyamatos felügyeleti és felderítési folyamatoknak ki kell terjedniük a :

a) a releváns belső és külső tényezőkre, beleértve az üzleti és IKT rendszergazdai funkciókat;

b) a tranzakciókra, hogy észleljék a hozzáféréssel való visszaélést a szolgáltatók vagy más személyek részéről; és

c) a potenciális belső és külső fenyegetésekre.

5.3 A pénzforgalmi szolgáltatóknak felderítő intézkedéseket kell bevezetniük, hogy felismerjék az információk esetleges kiszivárgását, a rosszindulatú kódokat és más biztonsági fenyegetéseket, valamint a szoftverek és hardverek közismert sérülékenységeit, és ellenőrizzék az ezeknek megfelelő új biztonsági frissítéseket.

A működési és biztonsági események felügyelete és bejelentése

5.4 A pénzforgalmi szolgáltatóknak megfelelő kritériumokat és küszöbértékeket kell meghatározniuk arra vonatkozóan, hogy milyen eseményt minősítenek működési vagy biztonsági eseménynek az iránymutatások „Fogalommeghatározások” részében leírtak szerint, valamint korai előrejelző mutatókat kell definiálniuk, amelyek riasztásként szolgálnak a pénzforgalmi szolgáltató számára, így lehetővé téve a működési vagy biztonsági események korai észlelését.

5.5 A pénzforgalmi szolgáltatóknak megfelelő folyamatokat és szervezeti struktúrákat kell kialakítaniuk, hogy biztosítsák a működési és biztonsági események következetes, integrált megfigyelését, kezelését és nyomon követését.

5.6 A pénzforgalmi szolgáltatóknak külön eljárást kell kialakítaniuk arra, hogy az ilyen működési és biztonsági eseményeket, illetve a biztonsági vonatkozású ügyfélpanaszokat jelentsék a felső vezetés felé.

6 Iránymutatás: Üzletmenet-folytonosság

6.1 A pénzforgalmi szolgáltatóknak működőképes üzletmenet-folytonosság irányítást kell kialakítaniuk, hogy súlyos üzletviteli fennakadások esetén is maximalizálni tudják a pénzforgalmi szolgáltatások folyamatosságát és határt szabjanak a veszteségeknek.

6.2 A megbízható üzletmenet-folytonosság kezelését szolgáló terv kidolgozásához a pénzforgalmi szolgáltatóknak gondosan elemezniük kell a súlyos üzletviteli fennakadásoknak való kitettségüket, és mennyiségileg és minőségileg értékelniük kell azok lehetséges hatását, belső és/vagy külső adatok és forgatókönyv-elemzés segítségével. Az iránymutatások 3.1–3.3. pontjának megfelelően azonosított és minősített kritikus funkciók, folyamatok, rendszerek, tranzakciók és kölcsönös

függőségek alapján a pénzforgalmi szolgáltatóknak kockázati alapon fontossági sorrendbe kell sorolniuk az üzletmenet-folytonossági intézkedéseket, ami az iránymutatások 3. pontja szerint végzett kockázatértékeléseken alapulhat. A pénzforgalmi szolgáltató üzleti modelljétől függően ez megkönnyítheti például a kritikus tranzakciók további feldolgozását, miközben folytatódnak a helyreállító intézkedések.

6.3 Az iránymutatások 6.2. pontja szerint végzett elemzés alapján a pénzforgalmi szolgáltatónak a következőket kell bevezetnie:

a) üzletmenet-folytonossági terveket, hogy megfelelően tudjon reagálni, és fenn tudja tartani a kritikus üzleti tevékenységeit; és

b) kárenyhítő intézkedéseket a pénzforgalmi szolgáltatásai megszakadásának és a meglévő szerződések felmondásának esetére, hogy elkerülje a pénzforgalmi rendszereket és a pénzforgalmi szolgáltatást igénybe vevőket érő negatív hatásokat, és biztosítsa a függőben lévő fizetési műveletek végrehajtását.

Forgatókönyveken alapuló üzletmenet-folytonossági tervezés

6.4 A pénzforgalmi szolgáltatóknak az őket potenciálisan érintő különböző forgatókönyvek széles körét kell mérlegelniük, köztük a szélsőséges, de valószínűsíthető változatokat is, és fel kell mérniük az ilyen forgatókönyvek lehetséges hatását.

6.5 Az iránymutatások 6.2. pontja szerint végzett elemzés és az iránymutatások 6.4. pontja szerint meghatározott valószínűsíthető forgatókönyvek alapján a pénzforgalmi szolgáltatóknak reagálási és helyreállítási terveket kell kidolgozniuk, amelyek:

a) a kritikus funkciók, folyamatok, rendszerek, tranzakciók és kölcsönös függőségek működését érő hatásra helyezik a hangsúlyt;

b) dokumentálva vannak, az üzleti és támogató egységek rendelkezésére állnak és vészhelyzet esetén azonnal hozzáférhetők; és

c) a tesztekből levont tanulságokkal, az újonnan felismert kockázatokkal és fenyegetésekkel és a megváltozott helyreállítási célokkal és prioritásokkal összhangban frissítve vannak.

Az üzletmenet-folytonossági tervek tesztelése

6.6 A pénzforgalmi szolgáltatóknak tesztelniük kell az üzletmenet-folytonossági terveiket, és gondoskodniuk kell arról, hogy a kritikus funkciók, folyamatok, rendszerek, tranzakciók és kölcsönös függőségek működését legalább évente teszteljék. A terveknek támogatniuk kell a műveleteik integritásának és rendelkezésre állásának és az információs eszközeik titkosságának védelmére és szükség esetén helyreállítására vonatkozó célkitűzéseket.

6.7 A terveket a teszteredmények, az aktuális fenyegetettségi elemzések, az információmegosztás és a korábbi eseményekből levont tanulságok, a változó helyreállítási célok, valamint a még be nem következett, működési és technikai szempontból valószínűsíthető forgatókönyvek elemzése

alapján, illetve adott esetben a rendszerekben és folyamatokban történt módosítások után legalább évente frissíteni kell. A pénzforgalmi szolgáltatóknak az üzletmenet-folytonossági terveik kialakítása közben konzultálniuk és egyeztetniük kell a megfelelő belső és külső érdekelt felekkel.

6.8 A pénzforgalmi szolgáltatók üzletmenet-folytonossági terveinek tesztelése:

a) fedje le a forgatókönyvek megfelelően széles körét, az iránymutatások 6.4. pontjában jelzettek szerint;

b) legyen úgy megtervezve, hogy kihívást jelentsen azoknak a feltételezéseknek, amelyeken az üzletmenet-folytonossági tervek alapulnak, beleértve az irányítási rendszereket és a válságkommunikációs terveket; és

c) olyan eljárások tartalmazzon, amivel igazolni lehet a személyzet és a folyamatok azon képességét, hogy megfelelően tudnak reagálni a fenti forgatókönyvekre.

6.9 A pénzforgalmi szolgáltatóknak rendszeres időközönként ellenőrizniük kell az üzletmenet-folytonossági terveik hatékonyságát, dokumentálniuk és elemezniük kell a tesztekből eredő esetleges problémákat vagy hiányosságokat.

Válságkommunikáció

6.10 Fennakadás vagy vészhelyzet esetén és az üzletmenet-folytonossági terveik végrehajtása során a pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy hatékony válságkommunikációs intézkedések legyenek érvényben, annak érdekében, hogy minden érintett belső és külső érdekelt fél időben és megfelelő módon kapjon tájékoztatást, a külső szolgáltatókat is ideértve.

7 Iránymutatás: A biztonsági intézkedések tesztelése

7.1 A pénzforgalmi szolgáltatóknak olyan tesztelési keretrendszert kell kialakítaniuk és bevezetniük, amely bizonyosságot nyújt a biztonsági intézkedések megalapozottságára és hatékonyságára, és biztosítja, hogy a tesztelési keretrendszer igazodik a kockázatfelügyelő tevékenységek révén felismert új veszélyekhez és sérülékenységekhez.

7.2 A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy mindig elvégezzék a teszteket az infrastruktúrát, a folyamatokat vagy az eljárásokat érintő változások esetén, illetve ha jelentősebb működési vagy biztonsági események után módosítások történnek.

7.3 A tesztelési keretrendszernek ki kell terjednie i. a fizetési terminálokat és pénzforgalmi szolgáltatások nyújtására használt eszközöket, ii. a fizetési terminálokat és a pénzforgalmi szolgáltatást igénybe vevő hitelesítésére használt eszközöket, iii. a pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatást igénybe vevő számára a hitelesítő kód generálásához/fogadásához biztosított eszközöket és szoftvert érintő biztonsági intézkedésekre.

7.4 A tesztelési keretrendszernek biztosítania kell, hogy a teszteket:

a) a pénzforgalmi szolgáltató érvényben levő változáskezelő folyamata keretében hajtsák végre, hogy biztosítsák azok megalapozottságát és hatékonyságát;

b) független tesztelő személyek végezzék el, akik a pénzforgalmi szolgáltatások biztonsági intézkedéseinek tesztelésében kellő ismeretekkel, szaktudással és szakértelemmel rendelkeznek, és nem érintettek a tesztelendő pénzforgalmi szolgáltatások vagy rendszerek biztonsági intézkedéseinek fejlesztésében, legalábbis a biztonsági intézkedések hatálybalépése előtti végső tesztek esetében; és

c) kiterjesszék a pénzforgalmi szolgáltatásoknál felismert kockázat szintjének megfelelő sérülékenységi ellenőrzésekre és behatolásvizsgálatokra.

7.5 A pénzforgalmi szolgáltatóknak folyamatos és ismétlődő teszteket kell végezniük a pénzforgalmi szolgáltatásaikat védő biztonsági intézkedéseken. A pénzforgalmi szolgáltatásaik nyújtása szempontjából (az iránymutatások 3.2. pontjában leírtak szerint) kritikus rendszerek esetében ezeket a teszteket legalább évente el kell végezni. A nem kritikus rendszereket kockázati alapon értékelve rendszeresen, de legalább háromévente tesztelni kell.

7.6 A pénzforgalmi szolgáltatóknak figyelniük és értékelniük kell az elvégzett tesztek eredményeit, és ennek megfelelően kell frissíteniük a biztonsági intézkedéseiket, a kritikus rendszerek esetében indokolatlan késedelem nélkül.

8 Iránymutatás: Helyzetismeret és folyamatos tanulás

Fenyegetettség és helyzetismeret

8.1 A pénzforgalmi szolgáltatóknak folyamatokat és szervezeti struktúrákat kell kialakítaniuk és bevezetniük, hogy felismerjék és folyamatosan figyelemmel kísérjék az olyan biztonsági és működési veszélyeket, amelyek érdemben befolyásolhatják a pénzforgalmi szolgáltatások nyújtására való képességüket.

8.2 A pénzforgalmi szolgáltatóknak elemezniük kell a szervezeten belül és/vagy kívül felismert vagy megtörtént működési és biztonsági eseményeket. A pénzforgalmi szolgáltatóknak mérlegelniük kell az ilyen elemzésekből származó főbb tanulságokat, és a biztonsági intézkedéseket ennek megfelelően kell frissíteniük.

8.3 A pénzforgalmi szolgáltatóknak aktívan figyelniük kell a technológia fejlődését, hogy tisztában legyenek a biztonsági kockázatokkal.

Képzési és biztonságismereti programok

8.4 A pénzforgalmi szolgáltatóknak képzési programot kell összeállítaniuk a személyzet minden tagja számára, hogy fel legyenek készülve a feladataikra és felelősségeikre vonatkozó biztonsági elvekkel és eljárásokkal összhangban történő ellátására, és ezáltal csökkenjen az emberi hiba, lopás, csalás, visszaélés vagy veszteség esélye. A pénzforgalmi szolgáltatóknak gondoskodniuk kell arról, hogy a képzési program a személyzet tagjai számára legalább évente – vagy szükség esetén gyakrabban is – biztosítsa a képzést.

8.5 A pénzforgalmi szolgáltatóknak biztosítaniuk kell, hogy a személyzetnek az iránymutatások 3.1. pontjában megnevezett kulcspozíciókat betöltő tagjai évente – vagy szükség esetén gyakrabban – célzott információbiztonsági képzésben részesüljenek.

8.6 A pénzforgalmi szolgáltatóknak rendszeres időközönkénti biztonságismereti programokat kell kidolgozniuk és végrehajtaniuk, hogy felvilágosítsák a munkatársaikat, és foglalkozzanak az információbiztonsági vonatkozású kockázatokkal. E programok keretében a pénzforgalmi szolgáltatók munkatársai számára elő kell írni, hogy minden szokatlan tevékenységet vagy eseményt jelentsenek.

9 Iránymutatás: A pénzforgalmi szolgáltatást igénybe vevők ügyfélkapcsolat-kezelése

A pénzforgalmi szolgáltatást igénybe vevő tudomása a biztonsági kockázatokról és kockázatmérséklő intézkedésekről

9.1 A pénzforgalmi szolgáltatóknak folyamatokat kell kialakítaniuk és bevezetniük, hogy erősítsék a pénzforgalmi szolgáltatást igénybe vevőknek a pénzforgalmi szolgáltatásokkal járó biztonsági kockázatokkal kapcsolatos tudatosságát, amihez segítséget és útmutatást kell biztosítaniuk a pénzforgalmi szolgáltatást igénybe vevők számára.

9.2 A pénzforgalmi szolgáltatást igénybe vevőknek nyújtott támogatást és útmutatást az új fenyegetések és sérülékenységek fényében aktualizálni kell, és a változásokat közölni kell a pénzforgalmi szolgáltatást igénybe vevőkkel.

9.3 Ahol a termék funkcionalitása ezt megengedi, a pénzforgalmi szolgáltatóknak lehetővé kell tenniük, hogy a pénzforgalmi szolgáltatást igénybe vevők letiltsák a pénzforgalmi szolgáltatók által a pénzforgalmi szolgáltatást igénybe vevőknek kínált pénzforgalmi szolgáltatásokhoz kapcsolódó egyes fizetési funkciókat.

9.4 Ha az (EU) 2015/2366 irányelv 68. cikke (1) bekezdésének megfelelően egy pénzforgalmi szolgáltató az egyes készpénz-helyettesítő fizetési eszközökkel végrehajtott fizetési műveletekre vonatkozó összeghatárokról állapodott meg a fizető féllel, a pénzforgalmi szolgáltatónak fel kell kínálnia a fizető fél számára azt a lehetőséget, hogy ezeket az összeghatárokat a maximálisan elfogadott összeghatárig módosítsa.

9.5 A pénzforgalmi szolgáltatóknak lehetőséget kell adniuk arra, hogy a pénzforgalmi szolgáltatást igénybe vevők értesítést kapjanak a fizetési műveletek indítására tett megkezdett/sikertelen kísérletekről, ami lehetővé teszi a számlájuk csalárd vagy rosszindulatú használatának észlelését.

9.6 A pénzforgalmi szolgáltatóknak folyamatosan tájékoztatniuk kell a pénzforgalmi szolgáltatást igénybe vevőket a pénzforgalmi szolgáltatások nyújtásával kapcsolatban őket érintő biztonsági eljárások frissítéseiről.

9.7 A pénzforgalmi szolgáltatóknak a pénzforgalmi szolgáltatásokkal kapcsolatos mindenfajta kérdés, támogatáskérés és anomáliáról vagy biztonsági kérdéseket érintő ügyekről szóló értesítés esetén

segítséget kell nyújtaniuk a pénzforgalmi szolgáltatást igénybe vevőknek. A pénzforgalmi szolgáltatást igénybe vevőket megfelelően tájékoztatni kell az ilyen segítségnyújtás igénybevételének lehetőségeiről.