**A Magyar Nemzeti Bank 26/2018. (VIII.16.) számú ajánlása**

**a pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről**

## I. Az ajánlás célja és hatálya

Az ajánlás célja a pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekkel kapcsolatban a Magyar Nemzeti Bank (a továbbiakban: MNB) elvárásainak megfogalmazása, és ezzel a jogalkalmazás kiszámíthatóságának növelése, a vonatkozó jogszabályok egységes alkalmazásának elősegítése.

Az MNB jelen ajánlás közzétételével biztosítja az Európai Bankhatóságnak (EBH) az (EU) 2015/2366 irányelv (PSD2) szerinti pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről szóló, 2018. január 12-ei, EBA/GL/2017/17 számú iránymutatásoknak[1] való megfelelést.

Az ajánlás címzettjei azok a hitelintézetek, elektronikuspénz-kibocsátó intézmények, pénzforgalmi intézmények, amelyek pénzforgalmi szolgáltatási tevékenységet végeznek, valamint a Posta Elszámoló Központot működtető intézmény és a Kincstár (a továbbiakban együtt: pénzforgalmi szolgáltató).

## II. A jelen ajánlásban használt fontosabb fogalmak

Az ajánlásban a következő fogalmak az alábbi jelentéssel bírnak:

**Vezető testület:** a hitelintézetek tekintetében a hitelintézetekről és pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (a továbbiakban: Hpt.) 6. § (1) bekezdés 123. pontja szerinti testületek és személyek; a pénzforgalmi intézmények, az elektronikuspénz-kibocsátó intézmények és a Posta Elszámoló Központot működtető intézmény tekintetében a vezető tisztségviselők vagy az irányításért felelős tisztségviselők, valamint adott esetben a pénzforgalmi szolgáltatási tevékenységek irányításáért felelős tisztségviselők; a Kincstár tekintetében annak elnöke.

**Három védelmi vonal:**

A mindennapi operatív működés szintjén elhelyezkedő első védelmi vonal a folyamatba épített kontrollokat jelenti. A második védelmi vonal a bizonyos rendszerességgel és szervezeti szinten működtetett kontrollelemeket jelenti, mint például: minőség-ellenőrzés, megfelelőségi ellenőrzés, kockázatkezelés, biztonság. A harmadik védelmi vonal a független értékelést és a belső ellenőrzést jelenti, aminek a célja, hogy bizonyosságot nyújtson az első két védelmi vonalban levő kontroll elemek megfelelő működéséről. A három védelmi vonal közötti különbséget elsősorban a végrehajtástól való távolságuk jelenti, azaz a „függetlenségük” mértéke.

**Mélységi védelem:** az informatikai biztonság területén a védelem rétegzésének stratégiája. A mélységi védelem lényege, hogy a rendszert a támadásoktól a pénzforgalmi szolgáltató több különböző módszerrel egyidejűleg védje. A mélységi védelem módszerei a védelmi mechanizmusok, eljárások és irányelvek. A mélységi védelem célja az informatikai rendszer megbízhatóságának növelése; a több rétegű védelem akadályozza a kémkedést, kizárja a közvetlen támadás lehetőségét a kritikus rendszerek felé. A számítógépes hálózat védelmét tekintve a mélységi védelem nem csak megakadályozza a betörést, hanem

[1] https://www.eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_HU.pdf/8960614c-56e5-475a-b095-27c1da6deec2

időt is nyer a pénzforgalmi szolgáltató számára, hogy detektálja a támadást és válaszoljon rá, így csökkentve a támadás hátrányos következményeit.

**Működési kockázat:** az emberek szándékosságából vagy hanyagságából, a munkafolyamatok hibás lebonyolítási eljárásából, lényeges erőforrások, rendszerek hibájából, kieséséből, vagy fizikai károsodást okozó kisebb-nagyobb külső eseményekből fakadó károk veszélye (beleértve a jogszabálysértésből adódó, de ide nem értve a stratégiai, illetve reputációs kárveszélyt).

**Működési és biztonsági incidens:** a pénzforgalmi szolgáltató által előre nem tervezett olyan egyedi esemény vagy egymáshoz kapcsolódó események olyan sorozata, amelynek a fizetéshez kapcsolódó szolgáltatás sértetlenségére, rendelkezésre állására, bizalmasságára, hitelességére, illetve folyamatosságára negatív hatása van.

**Vezető állású személyek:** a hitelintézetek tekintetében a Hpt. 6. § (1) bekezdés 122. pontjában foglaltak szerinti személyek; a pénzforgalmi intézmények, az elektronikuspénz-kibocsátó intézmények a Posta Elszámoló Központot működtető intézmény és a kincstár tekintetében az intézménynél vezetői feladatot ellátó természetes személyek, akik felelősek és elszámoltathatók a vezető testület előtt a pénzforgalmi szolgáltató mindennapi vezetéséért.

**IKT rendszer:** információs és kommunikációs technológiai rendszer.

**A „legkisebb jogosultság" elve:** azt írja elő, hogy egy számítógépes környezet adott absztrakciós rétegében minden modul (mint pl. folyamat, felhasználó vagy alkalmazás) kizárólag olyan információkhoz és erőforrásokhoz fér hozzá, amelyek szükségesek a modul legitim céljainak eléréséhez. Felhasználók esetében a felhasználóknak lehetőleg mindig a lehetséges legalacsonyabb jogosultságokkal kell működniük, és a lehető legalacsonyabb jogosultsággal kell alkalmazásokat indítaniuk.

**A „szükséges ismeret" elve:** az információk elérésére, birtoklására, és azokon tevékenység végrehajtására vonatkozó jogosultságok meghatározása egy felhasználó részére a munkaköri kötelezettségei függvényében.

**Biztonsági kockázat:** a nem megfelelően kialakított vagy hibásan működő belső folyamatokból vagy külső eseményekből eredő olyan kockázat, amely negatív hatással van vagy lehet a pénzforgalmi szolgáltató IKT rendszereinek, illetve a pénzforgalmi szolgáltatások biztosításához felhasznált információk rendelkezésre állására, sértetlenségére és bizalmasságára. Ez magában foglalja a kibertámadások jelentette vagy a nem megfelelő fizikai biztonságból eredő kockázatot is.

**Kockázatvállalási hajlandóság:** A kockázat azon aggregált szintje és típusai, amelyeket a pénzforgalmi szolgáltató stratégiai céljainak megvalósítása érdekében, kockázatviselési képességének keretein belül, üzleti modelljével összhangban vállal.

## III. Általános elvárások

Az MNB elvárja, hogy a pénzforgalmi szolgáltató feleljen meg az ajánlásban foglalt valamennyi elvárásnak. A belső szabályozás részletezettségének szintje legyen arányos a pénzforgalmi szolgáltató méretével és a pénzforgalmi szolgáltató által nyújtott vagy nyújtani kívánt konkrét szolgáltatások természetével, körével, összetettségével és kockázatosságával.

## IV. Speciális elvárások

### 1. Vállalatirányítás

#### A működési és biztonsági kockázat kezelési keretrendszer

1.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató hatékony működési és biztonsági kockázatkezelési keretrendszert (a továbbiakban: kockázatkezelési keretrendszer), hozzon létre, amelyet legalább évente egy alkalommal felül kell vizsgálnia és a vezető testületnek, illetve a vezető állású személynek jóvá kell hagynia. 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.

1.2. Az MNB elvárja, hogy a kockázatkezelési keretrendszer:

a) foglalja magában az engedélyezési és nyilvántartásba vételi feltételekre vonatkozó rendelkezéseknek az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 17. § (1) bekezdésének v) pontjában, 20/A. § (1) bekezdésének g) pontjában meghatározott, a biztonsági elvek átfogó leírását tartalmazó dokumentumot;

b) legyen összhangban a pénzforgalmi szolgáltató kockázatvállalási hajlandóságával;

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

d) dolgozza ki 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.

1.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató biztosítsa a kockázatkezelési keretrendszer megfelelő dokumentáltságát, és a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján történő aktualizálását.

1.4. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az infrastruktúra, a folyamatok vagy az eljárások jelentősebb változtatása előtt és az általa nyújtott pénzforgalmi szolgáltatások biztonságát érintő valamennyi jelentős működési és biztonsági incidens után haladéktalanul vizsgálja meg, hogy szükséges-e a kockázatkezelési keretrendszer módosítása vagy fejlesztése.

#### Kockázatkezelési és ellenőrzési modellek

1.5. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a működési és biztonsági kockázatok azonosítása és kezelése érdekében „három védelmi vonalat”, vagy egy azzal egyenértékű belső kockázatkezelési és ellenőrzési modellt alakítson ki. A pénzforgalmi szolgáltatónak biztosítania 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 vezető állású személy felé is.

1.6. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az ajánlásban meghatározott biztonsági intézkedéseket vizsgáltassa felül 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

1.7. Az MNB elvárja, hogy amennyiben a pénzforgalmi szolgáltatások működési funkcióit, többek között az informatikai rendszerek működtetését a pénzforgalmi szolgáltató kiszervezi, biztosítsa az ezen ajánlásban meghatározott biztonsági intézkedések hatékony végrehajtását.

1.8. Az MNB elvárja, hogy a pénzforgalmi szolgáltató biztosítsa, 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 szolgáltató ellenőrizze és biztosítsa az említett szolgáltatók e biztonsági céloknak, intézkedéseknek és minőségi céloknak való megfelelését.

## 2. Kockázatértékelés

### Eszköz és üzleti folyamat nyilvántartás
### Üzleti funkciók, támogató folyamatok és az információs eszközök azonosítása

2.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató határozza meg, dolgozza ki és rendszeresen aktualizálja az üzleti funkciói, kulcspozíciói, és támogató folyamatainak összességét tartalmazó nyilvántartását, annak érdekében, hogy feltérképezze az egyes funkciók, feladatok és támogató folyamatok jelentőségét, valamint a működési és biztonsági kockázatokkal összefüggő kölcsönös függőségeit.

2.2. Az MNB elvárja, hogy a pénzforgalmi szolgáltató határozza meg, dolgozza ki és rendszeresen aktualizálja az információs eszközök, különösen az IKT-rendszerek, azok konfigurációi, az egyéb infrastruktúrák, valamint az egyéb belső és külső rendszerekkel való összekapcsolódások összességét tartalmazó nyilvántartásait, annak érdekében, hogy képes legyen kezelni az alapvető üzleti funkcióit és folyamatait támogató eszközöket.

### Üzleti funkciók, támogató folyamatok és az információs eszközök osztályozása

2.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató kritikusság szerint (bizalmasság, sértetlenség, rendelkezésre állás) osztályozza az azonosított üzleti funkciókat, támogató folyamatokat és információs eszközöket.

### Üzleti funkciók, támogató folyamatok és az információs eszközök kockázatértékelése

2.4. Az MNB elvárja, hogy a pénzforgalmi szolgáltató biztosítsa a fenyegetések és a sebezhető pontok folyamatos nyomon követését és rendszeresen vizsgálja felül az üzleti funkcióira, alapvető folyamataira és információs eszközeire hatással lévő kockázati forgatókönyveket. A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény (a továbbiakban: Pft.) 55/A. § (2) bekezdése alapján a pénzforgalmi szolgáltatónak – azon kötelezettsége részeként, hogy aktualizált és átfogó értékelést készítsen az általa nyújtott pénzforgalmi szolgáltatásokhoz kapcsolódó működési és biztonsági kockázatokról, valamint az e kockázatokra válaszul alkalmazott kockázatmérséklési intézkedések és ellenőrzési mechanizmusok megfelelőségéről, és azt elküldje az MNB-nek – a fő működési és biztonsági kockázatok azonosítása és értékelése érdekében évente, el kell végeznie és

dokumentálnia kell az általa azonosított és osztályozott funkciók, folyamatok és információs eszközök kockázatértékelését. Szintén elvárt, hogy ilyen kockázatértékelést végezzen a pénzforgalmi szolgáltatások biztonságát érintő infrastruktúra, folyamatok vagy eljárások minden jelentős változtatása előtt.

2.5. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a kockázatértékelések alapján határozza meg, szükséges-e a meglévő biztonsági intézkedések, az alkalmazott technológiák és az eljárások vagy a nyújtott pénzforgalmi szolgáltatások megváltoztatása, és ha igen, milyen mértékben. Az MNB elvárja továbbá, hogy a pénzforgalmi szolgáltató vegye figyelembe a változtatások végrehajtásához szükséges időt, valamint azt az időt, amely a működési és biztonsági incidensek, csalások és a pénzforgalmi szolgáltatások nyújtását zavaró esetleges hatások minimalizálását szolgáló megfelelő ideiglenes biztonsági intézkedések meghozatalához szükséges.

## 3. Védelem

3.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az azonosított működési és biztonsági kockázatokkal szembeni megelőző biztonsági intézkedéseket dolgozzon ki és hajtson végre. Ezeknek az intézkedéseknek az azonosított kockázatokkal összhangban lévő, megfelelő szintű biztonságot kell nyújtaniuk.

3.2. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a személyekre, a folyamatokra és a technológiára is kiterjedő, „mélységi védelem” megközelítésű, többszintű felügyeleti rendszert hozzon létre és vezessen be, amelyben minden egyes szint az előző szint biztonsági védőhálójaként szolgál. Az is elvárt továbbá, hogy a mélységi védelem értelmében ugyanarra a kockázatra egynél több kontrollt határozzon meg, mint például a négy szem elv, a kétfaktoros hitelesítés, a hálózatszegmentálás és a többszörös tűzfalak.

3.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató biztosítsa a kritikus logikai és fizikai eszközei, erőforrásai védelmét és a pénzforgalmi szolgáltatásait igénybe vevők érzékeny fizetési adatainak bizalmasságát, sértetlenségét és rendelkezésre állását, azok tárolása, továbbítása és használata alatt egyaránt. Ha az adatok személyes adatokat tartalmaznak, az intézkedéseket a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendeletnek, vagy ha alkalmazandó, a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló 45/2001/EK európai parlamenti és tanácsi rendeletnek megfelelően kell végrehajtani.

3.4. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy folyamatosan nyomon kövesse, hogy a 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 szolgáltató hatályos változáskezelési folyamatának részét kell képezniük, ami biztosítja a változtatások megfelelő előkészítését, tesztelését, dokumentálását és engedélyezését. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az észlelt biztonsági fenyegetések és az elvégzett változtatások alapján a releváns és ismert potenciális támadások forgatókönyveinek beépítése céljából végezzen tesztelést.

3.5. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a pénzforgalmi szolgáltatások tervezése, kialakítása és nyújtása során biztosítsa a feladatkörök szétválasztását és a „legkisebb jogosultság” elvének

alkalmazását. Elvárt, hogy a pénzforgalmi szolgáltató fordítson különös figyelmet az informatikai környezetek elkülönítésére, különös tekintettel a fejlesztési, a tesztelési és az éles környezetre.

### Adatok bizalmassága és a rendszerek integritása

3.6. Az MNB elvárja, hogy a pénzforgalmi szolgáltatások kialakításakor, fejlesztésekor és nyújtásakor a pénzforgalmi szolgáltató gondoskodjon arról, hogy a pénzforgalmi szolgáltatást igénybe vevő érzékeny fizetési adatainak összegyűjtése, továbbítása, feldolgozása, tárolása, illetve archiválása, valamint megjelenítése megfelelő és valós legyen, és csak a pénzforgalmi szolgáltatásainak nyújtásához szükséges mértékre korlátozódjon.

3.7. Az MNB elvárja, hogy a pénzforgalmi szolgáltató rendszeresen ellenőrizze, hogy a pénzforgalmi szolgáltatások nyújtásához használt szoftver – beleértve a pénzforgalmi szolgáltatást igénybe vevők fizetéshez kapcsolódó szoftverét is – naprakész legyen, és a kritikus biztonsági javítások telepítve legyenek. Azt is elvárja az MNB, hogy a pénzforgalmi szolgáltató gondoskodjon arról, hogy olyan sértetlenség-ellenőrző mechanizmusok működjenek, amik ellenőrzik a pénzforgalmi szolgáltatásuk szoftverének, firmware-ének és az adatainak sértetlenségét.

### Fizikai biztonság

3.8. Az MNB elvárja, hogy a pénzforgalmi szolgáltató olyan fizikai biztonsági intézkedéseket foganatosítson, amik megvédik a pénzforgalmi szolgáltatást igénybe vevők érzékeny fizetési adatait, valamint a pénzforgalmi szolgáltatások nyújtására használt IKT-rendszereket.

### A hozzáférések felügyelete

3.9. 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. Az MNB elvárja, hogy a pénzforgalmi szolgáltató olyan ellenőrzési rendszert vezessen be, amely az IKT-rendszerekhez való hozzáférést megbízható módon azokra korlátozza, akiknél ez valós üzleti követelmény. Elvárt, hogy a pénzforgalmi szolgáltató az adatokhoz és rendszerekhez való elektronikus hozzáférését az alkalmazások számára az adott szolgáltatás nyújtásához szükséges minimálisan elegendő szintre korlátozza.

3.10. Az MNB elvárja, hogy a pénzforgalmi szolgáltató szigorú felügyelet alatt tartsa a privilegizált (speciális jogokkal felruházott) felhasználók rendszerhozzáférését, azáltal, hogy erősen korlátozza és szorosan felügyeli a magasabb rendszerhozzáférési jogosultsággal rendelkező munkatársakat. Ilyen korlátozás/felügyelet lehet például a szerepkör alapú jogosultság kiosztás, a privilegizált felhasználók rendszertevékenységeinek naplózása és utólagos ellenőrzése, az erős hitelesítés és a szokásostól eltérő tevékenységek figyelése. A pénzforgalmi szolgáltatónak a „szükséges ismeret” elve alapján kell kezelnie az információs eszközökhöz és ezek támogató rendszereihez való hozzáférési jogokat. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a hozzáférési jogokat rendszeresen, de legalább évente egyszer vizsgálja felül.

3.11. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a hozzáférési naplókat a meghatározott üzleti funkciók, támogató folyamatok és információs eszközök kritikus jelentőségével arányos ideig őrizze meg, az iránymutatások 2.1. és 2.2. pontjának megfelelően, az uniós és nemzeti jogszabályban előírt megőrzési követelmények sérelme nélkül. Az MNB elvárja, hogy a pénzforgalmi szolgáltató ezeket az

információkat használja fel a pénzforgalmi szolgáltatások nyújtásában észlelt rendellenes tevékenységek felismerésének és kivizsgálásának megkönnyítésére.

3.12. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy 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 adjon. Elvárás továbbá, hogy a hozzáférés-kezelési folyamatokhoz kapcsolódó termékek, eszközök és eljárások üzemeltetése védje a hozzáférés-kezelési folyamatokat a kompromittálódással vagy megkerüléssel szemben. Ebbe beletartozik a megfelelő termékek, eszközök és eljárások bevezetése, fenntartása, hatályon kívül helyezése és visszavonása.

## 4. Észlelés

### Folyamatos felügyelet és észlelés

4.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a pénzforgalmi szolgáltatások nyújtásában fellépő rendellenes tevékenységek feltárása érdekében az üzleti funkciók, támogató folyamatok és információs eszközök folyamatos felügyeletéhez szükséges folyamatokat és mechanizmusokat alakítson ki és vezessen be. Elvárt továbbá, hogy a folyamatos felügyelet keretében a pénzforgalmi szolgáltató megfelelő és hatékony mechanizmusokkal rendelkezzen, hogy észlelje a fizikai vagy logikai behatolást, valamint a pénzforgalmi szolgáltatások nyújtásában használt információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának megsértését.

Az MNB elvárja, hogy a pénzforgalmi szolgáltató folyamatos felügyeleti és felderítési folyamatai térjenek ki:

a) a releváns belső és külső tényezőkre, beleértve az üzleti és IKT adminisztratív funkciókat;
b) a tranzakciókra, hogy észleljék a hozzáféréssel való visszaélést a szolgáltatók vagy más személyek részéről és
c) a potenciális belső és külső fenyegetésekre.

4.2. Az MNB elvárja, hogy a pénzforgalmi szolgáltató felderítő intézkedéseket vezessen be, hogy felismerje az információk esetleges kiszivárgását, a rosszindulatú kódokat és más biztonsági fenyegetéseket, valamint a szoftverek és hardverek közismert sérülékenységeit, és ellenőrizze az ezeknek megfelelő új biztonsági frissítéseket.

### A működési és biztonsági incidensek felügyelete és bejelentése

4.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató megfelelő kritériumokat és küszöbértékeket határozzon meg arra vonatkozóan, hogy milyen eseményt minősítsen működési vagy biztonsági incidensnek az iránymutatások „Fogalommeghatározások” részében leírtak szerint, valamint korai előrejelző mutatókat definiáljon, amelyek riasztásként szolgálnak a pénzforgalmi szolgáltató számára, így lehetővé téve a működési vagy biztonsági incidensek korai észlelését.

4.4. Az MNB elvárja, hogy a pénzforgalmi szolgáltató megfelelő folyamatokat és szervezeti struktúrákat alakítson ki, hogy biztosítsa a működési és biztonsági incidensek következetes, integrált megfigyelését, kezelését és nyomon követését.

4.5. Az MNB elvárja, hogy a pénzforgalmi szolgáltató külön eljárást alakítson ki arra, hogy az ilyen működési és biztonsági incidenseket, illetve a biztonsági vonatkozású ügyfélpanaszokat jelentse a vezető állású személy felé.

## 5. Üzletmenet-folytonosság

5.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató működőképes üzletmenet-folytonosság irányítást alakítson ki, hogy súlyos üzletviteli fennakadások esetén is maximalizálni tudja a pénzforgalmi szolgáltatások folyamatosságát és határt szabjon a veszteségeknek.

5.2. Az MNB elvárja, hogy a megbízható üzletmenet-folytonosság kezelését szolgáló terv kidolgozásához a pénzforgalmi szolgáltató gondosan elemezze a súlyos üzletviteli fennakadásoknak való kitettségét, és mennyiségileg és minőségileg értékelje azok lehetséges hatását, belső, illetve külső adatok és forgatókönyv-elemzés segítségével. Elvárt, hogy az ajánlás 2.1–2.3. pontjában foglaltaknak megfelelően azonosított és minősített kritikus funkciók, folyamatok, rendszerek, tranzakciók és kölcsönös függőségek alapján a pénzforgalmi szolgáltató kockázati alapon sorolja fontossági sorrendbe az üzletmenet-folytonossági intézkedéseket, ami az ajánlás 2. pontja szerint végzett kockázatértékeléseken alapulhat. A pénzforgalmi szolgáltató üzleti modelljétől függően ez megkönnyítheti például a kritikus tranzakciók további feldolgozását, miközben folytatódnak a helyreállító intézkedések.

5.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az ajánlás 5.2. pontja szerint végzett elemzés alapján a következőket vezesse be:

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

5.4. Az MNB elvárja, hogy a pénzforgalmi szolgáltató az őt potenciálisan érintő különböző forgatókönyvek széles körét mérlegelje, köztük a szélsőséges, de valószínűsíthető változatokat is, és mérje fel az ilyen forgatókönyvek lehetséges hatását.

5.5. Az MNB elvárja, hogy az 5.2. pont szerint végzett elemzés és az 5.4. pont szerint meghatározott valószínűsíthető forgatókönyvek alapján a pénzforgalmi szolgáltató reagálási és helyreállítási terveket dolgozzon ki, amelyek:

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

b) dokumentáltak, 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

5.6. Az MNB elvárja, hogy a pénzforgalmi szolgáltató tesztelje az üzletmenet-folytonossági terveit, és biztosítsa, hogy a kritikus funkciók, folyamatok, rendszerek, tranzakciók és kölcsönös függőségek évente legalább egyszer legyenek megvizsgálva. Ezen tervektől elvárt, hogy támogassák azon célokat, amik védik és szükség esetén újra biztosítják a napi működéshez szükséges sértetlenséget, rendelkezésre állást és az információs eszközök bizalmasságát.

5.7. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a terveket a teszteredmények, az aktuális fenyegetettségi elemzések, az információmegosztás és a korábbi incidensekből 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 frissítse. Elvárt továbbá, hogy a pénzforgalmi szolgáltató az üzletmenet-folytonossági tervei kialakítása közben konzultáljon és egyeztessen a megfelelő belső és külső érdekelt felekkel.

5.8. Az MNB elvárja, hogy a pénzforgalmi szolgáltató üzletmenet-folytonossági tervének tesztelése:

a) fedje le a forgatókönyvek megfelelően széles körét az iránymutatások 5.4. pontjában jelzettek szerint;

b) legyen úgy megtervezve, hogy tesztelje azokat a feltételezéseket, amelyeken az üzletmenet-folytonossági tervek alapulnak, beleértve az irányítási rendszereket és a válságkommunikációs terveket és

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

5.9. Az MNB elvárja, hogy a pénzforgalmi szolgáltató rendszeres időközönként ellenőrizze az üzletmenet-folytonossági tervek hatékonyságát, dokumentálja és elemezze a tesztekből eredő esetleges problémákat vagy hiányosságokat.

### Válságkommunikáció

5.10. Az MNB elvárja, hogy fennakadás vagy vészhelyzet esetén és az üzletmenet-folytonossági tervek végrehajtása során a pénzforgalmi szolgáltató gondoskodjon 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.

## 6. Biztonsági intézkedések ellenőrzése

6.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató olyan tesztelési keretrendszert alakítson ki és vezessen be, amely igazolja a biztonsági intézkedések megalapozottságát és hatékonyságát, és biztosítja, hogy a tesztelési keretrendszer igazodik a kockázatfelügyelő tevékenységek révén felismert új veszélyekhez és sérülékenységekhez.

6.2. Az MNB elvárja, hogy a pénzforgalmi szolgáltató gondoskodjon arról, hogy mindig elvégezze a teszteket az infrastruktúrát, a folyamatokat vagy az eljárásokat érintő változások esetén, illetve, ha jelentősebb működési vagy biztonsági incidensek után módosítások történnek.

Elvárt, hogy a tesztelési keretrendszer terjedjen ki:

a) a fizetési terminálokra és pénzforgalmi szolgáltatások nyújtására használt eszközökre,

b) a fizetési terminálokra és a pénzforgalmi szolgáltatást igénybe vevő hitelesítésére használt eszközökre, és

c) a pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatást igénybe vevő számára a hitelesítő kód generálásához/fogadásához biztosított eszközökre

és szoftvert érintő biztonsági intézkedésekre.

Elvárt továbbá, hogy a tesztelési keretrendszer biztosítsa, hogy a teszteket:

a) a pénzforgalmi szolgáltató érvényben levő változáskezelési folyamata keretében hajtsa végre, hogy biztosítsa 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 azonosított kockázat szintjének megfelelő sérülékenység-vizsgálatokra és behatolás-vizsgálatokra.

6.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató folyamatos és ismétlődő teszteket végezzen a pénzforgalmi szolgáltatásaikat védő biztonsági intézkedéseken. Elvárt, hogy a pénzforgalmi szolgáltató a pénzforgalmi szolgáltatások nyújtása szempontjából (a 2.2. pontban leírtak szerint) kritikus rendszerek esetében ezeket a teszteket legalább évente végezze el, a nem kritikus rendszereket pedig kockázati alapon értékelve rendszeresen, de legalább három évente tesztelje.

6.4. Az MNB elvárja, hogy a pénzforgalmi szolgáltató figyelje és értékelje az elvégzett tesztek eredményeit, és ennek megfelelően haladéktalanul frissítse a biztonsági intézkedéseit.

## 7. Helyzetismeret, biztonságtudatosság, és folyamatos tanulás

### Fenyegetettségi helyzet és kitettség értékelés

7.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató folyamatokat vezessen be és szervezeti struktúrákat alakítson ki, hogy felismerje és folyamatosan figyelemmel kísérje az olyan biztonsági és működési veszélyeket, amelyek érdemben befolyásolhatják a pénzforgalmi szolgáltatások nyújtására való képességét.

7.2. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy elemezze a szervezeten belül, illetve kívül felismert vagy megtörtént működési és biztonsági incidenseket. Elvárt, hogy a pénzforgalmi szolgáltató mérlegelje az ilyen elemzésekből származó főbb tanulságokat, és a biztonsági intézkedéseket ennek megfelelően frissítse.

7.3. Az MNB elvárja, hogy a pénzforgalmi szolgáltató aktívan figyelje a technológia fejlődését annak érdekében, hogy tisztában legyen a biztonsági kockázatokkal.

### Képzési és biztonságtudatossági programok

7.4. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy képzési programot állítson össze a munkavállalók számára, hogy azok fel legyenek készülve a feladataik és felelősségeik vonatkozó biztonsági elvekkel és eljárásokkal összhangban történő ellátására, és ezáltal csökkenjen az emberi hiba, lopás, csalás, visszaélés és veszteség esélye. Elvárt továbbá, hogy a pénzforgalmi szolgáltató gondoskodjon arról, hogy a munkavállalók legalább évente – vagy szükség esetén gyakrabban is – részt vegyenek a képzési programban.

7.5. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy biztosítsa azt, hogy a 2.1. pontban megnevezett kulcspozíciókat betöltő munkavállalók évente – vagy szükség esetén gyakrabban – célzott információbiztonsági képzésben részesüljenek.

7.6. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy rendszeres időközönként biztonságtudatosságiprogramokat dolgozzon ki és hajtson végre annak érdekében, hogy oktassa a munkavállalóit, és foglalkozzon az információbiztonsági vonatkozású kockázatokkal. Elvárt, hogy a programok keretében a pénzforgalmi szolgáltató írja elő munkatársai számára, hogy minden szokatlan tevékenységet vagy incidenst jelentsenek.

## 8. A pénzforgalmi szolgáltatást igénybe vevők ügyfélkapcsolat-kezelése

### A pénzforgalmi szolgáltatást igénybe vevő tudása a biztonsági kockázatokról és kockázatmérséklő intézkedésekről

8.1. Az MNB elvárja, hogy a pénzforgalmi szolgáltató folyamatokat alakítson ki és vezessen be annak érdekében, hogy erősítse a pénzforgalmi szolgáltatást igénybe vevőknek a pénzforgalmi szolgáltatásokkal járó biztonsági kockázatokkal kapcsolatos tudatosságát, és amihez biztosítson segítséget és útmutatást a pénzforgalmi szolgáltatást igénybe vevők számára.

8.2. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a pénzforgalmi szolgáltatást igénybe vevőknek nyújtott támogatást és útmutatást az új fenyegetések és sérülékenységek fényében aktualizálja. Elvárt továbbá, hogy a pénzforgalmi szolgáltató a változásokat közölje a pénzforgalmi szolgáltatást igénybe vevőkkel.

8.3. Az MNB elvárja, hogy ahol a termék funkcionalitása ezt megengedi, a pénzforgalmi szolgáltató tegye lehetővé, hogy a pénzforgalmi szolgáltatást igénybe vevők letiltsák a pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatást igénybe vevőknek kínált pénzforgalmi szolgáltatásokhoz kapcsolódó egyes fizetési funkciókat.

8.4. Az MNB elvárja, hogy abban az esetben, ha a Pft. 39. § (1) bekezdésének megfelelően a pénzforgalmi szolgáltató az egyes készpénz-helyettesítő fizetési eszközökkel végrehajtott fizetési műveletekre vonatkozó összeghatárokról állapodott meg a fizető féllel, a pénzforgalmi szolgáltató kínálja fel a fizető fél számára azt a lehetőséget, hogy ezeket az összeghatárokat a maximálisan elfogadott összeghatárig módosítsa.

8.5. Az MNB elvárja, hogy a pénzforgalmi szolgáltató adjon lehetőséget 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.

8.6. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy folyamatosan tájékoztassa a pénzforgalmi szolgáltatást igénybe vevőket a pénzforgalmi szolgáltatások nyújtásával kapcsolatban őket érintő biztonsági eljárások frissítéseiről.

8.7. Az MNB elvárja a pénzforgalmi szolgáltatótól, hogy a pénzforgalmi szolgáltatásokkal kapcsolatos mindenfajta kérdés, támogatáskérés és anomáliáról vagy biztonsági kérdéseket érintő ügyekről szóló értesítés esetén nyújtson segítséget a pénzforgalmi szolgáltatást igénybe vevőknek. Az MNB elvárja, hogy a pénzforgalmi szolgáltató a pénzforgalmi szolgáltatást igénybe vevőket megfelelően tájékoztassa az ilyen segítségnyújtás igénybevételének lehetőségeiről.

## V. Záró rendelkezések

9. Az ajánlás a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontja szerint kiadott, a felügyelt pénzügyi szervezetekre kötelező erővel nem rendelkező szabályozó eszköz. Az MNB által kiadott ajánlás tartalma kifejezi a jogszabályok által támasztott követelményeket, az MNB jogalkalmazási gyakorlata alapján alkalmazni javasolt elveket, illetve módszereket, a piaci szabványokat és szokványokat.

10. Az ajánlásnak való megfelelést az MNB az általa felügyelt pénzügyi szervezetek körében az ellenőrzési és monitoring tevékenysége során figyelemmel kíséri és értékeli, összhangban az általános európai felügyeleti gyakorlattal.

11. Az MNB felhívja a figyelmet arra, hogy a pénzügyi szervezet az ajánlás tartalmát szabályzatai részévé teheti. Ebben az esetben a pénzügyi szervezet jogosult feltüntetni, hogy vonatkozó szabályzatában foglaltak megfelelnek az MNB által kiadott vonatkozó számú ajánlásnak. Amennyiben a pénzügyi szervezet csupán az ajánlás egyes részeit kívánja szabályzataiban megjeleníteni, úgy az ajánlásra való hivatkozást kerülje, illetve csak az ajánlásból átemelt részek tekintetében alkalmazza.

12. Az MNB a jelen ajánlás alkalmazását 2018. november 1-jétől várja el az érintett pénzügyi szervezetektől.

Dr. Matolcsy György
a Magyar Nemzeti Bank elnöke