H-JÉ-IV-B-52/2020. számú határozat

A **Pannónia Nyugdíjpénztárnál** (székhely: 1068 Budapest, Benczúr utca 11.) (**Pénztár**) hivatalból folytatott célvizsgálat megállapításai alapján a **Magyar Nemzeti Bank** (székhelye: 1054 Budapest, Szabadság tér 9., telephelye: 1013 Budapest, Krisztina krt. 39.) (**MNB**) az alábbi

h a t á r o z a t o t

hozza.

1. Felszólítja a Pénztárat, hogy az informatikai tárgyú szabályzatait mindenkor tartsa összhangban a jogszabályi elvárásokkal és a gyakorlati működésével.

   A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

2. Az informatikai környezetének határvédelmével kapcsolatosan felszólítja a Pénztárat, hogy
   a) a jogszabályi követelményeket figyelembe véve biztosítsa a kockázatokkal arányosan az informatikai hálózatának szeparálását más jogi entitásoktól, valamint a belső hálózatának további szeparálását az éles - és tesztrendszerek megfelelő szétválasztása érdekében;
   b) vizsgálja felül a tűzfalszabály kezelési-, felülvizsgálati-, és nyilvántartási eljárásait, gyakorlatát és a kockázatokkal arányosan gondoskodjon olyan szabályozásról és folyamatokról, melyek biztosítják a tűzfalszabályok rendszeres érdemi felülvizsgálatát és az ellenőrzések teljeskörűségét; a tűzfalszabályok létrehozásakor rendeljen minden tűzfalszabályhoz egy egyedi azonosítót, és azt tüntesse fel mind a kérelemben, mind a felvitt szabálynál a tűzfalon;
   c) vizsgálja felül és a kockázatokkal arányosan erősítse a határvédelmi funkciók használatát, beleértve az IDS/IPS védelmet és DDoS elleni támadások elleni védelmet;
   d) gondoskodjon a hitelesítési adatok bizalmasságának teljeskörű biztosításáról, valamint a hálózati forgalom sértetlenségének és hitelességének kockázatokkal arányos védelméről.

   A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

3. Felszólítja a Pénztárat, hogy az adatbázisai esetében a kockázatokkal arányosan hozzon létre és tartson naprakészen a biztonsági beállítások erősítésére, egységesítésére szolgáló „hardening" eljárásokat és ellenőrzési folyamatot, és biztosítsa azok alkalmazását adatbáziskörnyezeteiben; továbbá gondoskodjon arról, hogy a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenységek naplózása megvalósuljon.

   A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

4. Az informatikai biztonsági rendszer védelmével kapcsolatosan felszólítja a Pénztárat, hogy
   a) folyamatosan biztosítsa az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az Internet irányából elérhető szolgáltatásai esetében;
   b) végezze el az újonnan bevezetett portál rendszerének sérülékenységi vizsgálatát;
   c) a kockázatokkal arányosan hozzon létre és tartson naprakészen a biztonsági beállítások erősítésére, egységesítésére szolgáló „hardening" eljárásokat és ellenőrzési folyamatot a hálózati eszközei, operációsrendszerei, adatbázisai és alkalmazásai esetében.

A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

5. A felhasználói jogosultságokkal kapcsolatosan felszólítja a Pénztárat, hogy
   a) biztosítsa a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációját;
   b) ennek keretében vizsgálja felül jogosultságkezelési gyakorlatát és szabályozását, valamint
   c) erősítse a jogosultságok nyilvántartásának, összeférhetetlenségek meghatározásának és kezelésének, visszavonásának és ellenőrzésének folyamatait, illetve
   d) gondoskodjon a szükségtelen jogosultságok visszavonásáról;
   e) az informatikai rendszerhozzáférésekben csak névhez rendelt egyedi azonosítókat alkalmazzon;
   f) valamint gondoskodjon a jogosultság felülvizsgálatok elvárások szerinti rendszeres elvégzéséről.

   A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

6. A naplózási funkciókkal kapcsolatosan felszólítja a Pénztárat, hogy
   a) a biztonsági kockázattal arányosan tartson fent olyan biztonsági környezetet, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is;
   b) gondoskodjon arról, hogy a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenység naplózása megvalósuljon, a naplófájlok sérthetetlensége és rendelkezésre állása biztosított legyen, valamint a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódjanak;
   c) a fentiek érdekében vizsgálja felül a naplóelemzési eljárásait, szabályozza a tevékenységet, majd készítsen tervet és valósítsa meg az infrastruktúra elemek, szerverek, alkalmazások, adatbázisok biztonsági naplózását, azok naplóállományainak gyűjtését, valamint kockázatokkal arányosan alakítsa ki a központi automatikus biztonsági naplóelemzési- és riasztási képességeit.

   A Pénztár a jelen pontban foglaltak teljesítését legkésőbb 2021.06.30. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

7. Kötelezi a Pénztárat a határozat rendelkező részének 1-6. pontjaiban foglalt jogszabálysértésekre tekintettel 1.200.000, - Ft, azaz egymillió-kettőszázezer forint összegű felügyeleti bírság megfizetésére.

A kiszabott felügyeleti bírságot a határozat jogerőre emelkedésétől számított 30 (harminc) napon belül kell az MNB hatósági bírság és költségtérítés fizetése bankszámlájára (19017004-01678000-30900002) – „felügyeleti bírság” megjelöléssel, valamint a határozat számának feltüntetésével – befizetni. A bírság önkéntes befizetésének elmaradása esetén azokat az MNB megkeresésére az állami adóhatóság hajtja be. A bírság befizetésére meghatározott határidő elmulasztása esetén, a be nem fizetett bírságösszeg után késedelmi pótlék felszámolására kerül sor, amelynek mértéke minden naptári nap után a felszámítás időpontjában érvényes jegybanki alapkamat kétszeresének 365-öd része. A késedelmesen megfizetett késedelmi pótlék után nem számítható fel késedelmi pótlék. A késedelmi pótlékot az MNB hivatkozott számú számlájára kell befizetni, a határozat számának feltüntetésével, „késedelmi pótlék” megjelöléssel. Ha a kötelezett a bírságfizetési kötelezettségének határidőben nem tesz eleget, a fizetési kötelezettséget az MNB rendeli el, és a végrehajtást az adóhatóság foganatosítja.

8. Felszólítja a Pénztárat, hogy az Igazgatótanács elnöke e határozatot az Igazgatótanács és az Ellenőrző Bizottság ülésén a közléstől számított 15 (tizenöt) napon belül, a pénztártagokkal a következő küldöttközgyűlésen ismertesse.

Az MNB felhívja a Pénztár figyelmét, hogy amennyiben jelen határozati felszólításoknak, illetve felhívásoknak nem, vagy nem teljeskörűen, illetve késedelmesen tesz eleget, az MNB-nek jogszabályban biztosított intézkedések alkalmazására van lehetősége, ideértve magasabb összegű bírság kiszabását is.

Az MNB eljárása során eljárási költség nem merült fel.

A határozat ellen fellebbezésnek nincs helye, ugyanakkor az, akinek jogát vagy jogos érdekét a közigazgatási tevékenység közvetlenül érinti, a határozat ellen annak közlésétől számított 30 (harminc) napon belül jogszabálysértésre hivatkozással közigazgatási pert indíthat.

A keresetlevelet a Fővárosi Törvényszékhez címezve − az MNB-nél − kell benyújtani a következők szerint:
A perben a jogi képviselet kötelező, a keresetlevelet űrlapbenyújtás támogatási szolgáltatás igénybevételével kell benyújtani. (Az űrlapbenyújtás támogatási szolgáltatás elérhetősége: https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/hatarozatok-es-vegzesek-keresese).

A keresetlevél benyújtásának a határozat végrehajtására, illetve hatályosulására nincs halasztó hatálya, az ügyfél azonban azonnali jogvédelmet kérhet.

A bíróság a pert főszabály szerint tárgyaláson kívül bírálja el. Tárgyalás tartását az ügyfél a keresetlevélben kérheti. A tárgyalás tartása iránti kérelem elmulasztása miatt igazolásnak nincs helye.

I n d o k o l á s

I. A VIZSGÁLAT CÉLJA ÉS LEFOLYTATÁSA

Az MNB a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény (**MNB tv.**) 62. §-a, a 64. § (1) bekezdés b) pontja, a 64. § (2) bekezdés d) pontja alapján 2020. január 21-én hivatalból indított felügyeleti ellenőrzési eljárás keretében célvizsgálatot (**Vizsgálat**) folytatott le a Pénztárnál. A Vizsgálat részeként az MNB az MNB tv. 67. § (1) bekezdésére figyelemmel 2020. január 21. és 2020. január 29. napja között helyszíni ellenőrzést tartott a Pénztár székhelyén. A Vizsgálat alá vont időszak (**Vizsgált Időszak**) 2019. január 1. napjától a helyszíni ellenőrzés lezárásának napjáig terjedt.

Az MNB a Vizsgálat megállapításait a 2020. május 7-én kelt vizsgálati jelentésben (**Jelentés**) foglalta össze, és azt nyilatkozattételre megküldte a Pénztár részére, harminc napos határidő tűzésével. A Pénztár 2020. május 21-én vette kézhez a Jelentést.

A Pénztár az MNB-hez 2020. június 22-én érkezett beadványában tájékoztatta az MNB-t a Jelentésben foglalt megállapításokkal kapcsolatos észrevételeiről (**Észrevételek**). Az Észrevételeket az MNB áttekintette, kiértékelte és a jelen határozat meghozatala során figyelembe vette.

II. A VIZSGÁLAT MEGÁLLAPÍTÁSAI, A MEGÁLLAPÍTÁSOK MINŐSÍTÉSE, AZ ÉSZREVÉTELEK ÉRTÉKELÉSE

1. Informatikai tárgyú szabályzatok

1.1. Megállapítás

A Vizsgálat megállapította, hogy a Pénztár „IBU-07 Rendszerhozzáférések” elnevezésű informatikai biztonsági utasítása **(IBU-07-es utasítás)** a 3.3-as pont alatt az alábbiakat tartalmazza: „A jogosultság kiadását, módosítását vagy visszavonását a felhasználó vagy a felettese igényli a Felhasználói jogosultságkezelő bizonylat kitöltésével, módosításával. Amennyiben erre megfelelő elektronikus rendszer van kialakítva, az is használható, ha utólag is ellenőrizhető és szabályozott a kommunikációs csatorna (pl. levelezés, Helpdesk rendszer).” Az IBU-07-es utasítás idézett rendelkezésében megfogalmazott szabályok nem pontosan rögzítik a gyakorlatot, mivel a Pénztár a jogosultság igénylést, engedélyezést a Mantis workflow elnevezésű rendszerben dokumentálja, így tehát a jogosultságkezelő rendszer megnevezése nem szerepel a szabályzatban.

A Vizsgálat megállapította továbbá, hogy az „IBU-02 ADATOK OSZTÁLYOZÁSA, RENDSZEREK BESOROLÁSA” elnevezésű informatikai biztonsági utasítás **(IBU-02-es utasítás)** utolsó dokumentált – az IBU-02-es utasítás fedlapján is feltüntetett – módosítása 2011.05.24-én történt. Az IBU-02-es utasítás nem határozza meg az informatikai rendszer elemeinek a Pénztár által alkalmazott biztonsági osztályokba történő sorolása rendszerének konkrét végrehajtható módszertanát, továbbá nem határozza meg a besorolási osztályokat bizalmasság, rendelkezésre állás

és sértetlenség szempontjából. A Pénztár által alkalmazott négy biztonsági osztály definícióját az IBU-02-es utasítás helyett a Pénztár IT-25 Adatvédelmi szabályzata **(Adatvédelmi Szabályzat)** tartalmazza.

A Vizsgálat megállapította azt is, hogy a Pénztár a javítások és biztonsági javítások telepítésének folyamatát (patch management), valamint a biztonsági naplózás és naplóelemzés folyamatát nem szabályozta.

A Vizsgálat megállapította továbbá, hogy a Pénztár Informatikai Biztonsági Szabályzata **(IBSZ)** 6.7.4 számú, Jelszókezelés pontjában előírt jelszókövetelmények (min 6 karakter, a jelszavakat rendszeres időközönként - legfeljebb 90 naponként - cserélni kell) eltérnek az Active Directory központi címtárszolgáltatásában jól beállított (Minimális 8 karakter, maximális élettartam 60 nap) értékektől.

A Vizsgálat megállapította azt is, hogy a Pénztár nem az Informatikai szabályzatában rögzíti az egyes munkakörök betöltéséhez szükséges informatikai ismeretek körét, hanem az adott személyek konkrét munkaköri leírásában.

[INF.01] [IT.0 - 23_Szabalyozas\IBU_07_Rendszerhozzáférések_v2.4.pdf; IBU_02_Adatok osztályozása, Rendszerek besorolása_v2.0.pdf; IT.011; IT.015; IT.024]

1.2. A Megállapítás minősítése

Az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény **(Öpt)** 40/C. § (1) bekezdése szerint: „A pénztárnak ki kell alakítania a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről, amely kiterjed a bűncselekményekkel kapcsolatos kockázatok kezelésére is. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén."
Az Öpt 40/C. § (1) bekezdése szerint: „A pénztár belső szabályzatában meg kell határozni az egyes munkakörök betöltéséhez szükséges informatikai ismeretet."

Az 1.1. pontban megállapított hiányosságok azt eredményezik, hogy a Pénztár informatikai szabályzatai nehezen áttekinthetőek, illetve bizonyos funkciókat nem szabályoznak, a gyakorlatot nem követik, vagy attól eltérő szabályokat tartalmaznak. A Pénztár ebből következően megsértette az Öpt. 40/C. § (1) bekezdésében foglaltakat.
A Pénztár azzal, hogy nem az Informatikai szabályzatában rögzíti az egyes munkakörök betöltéséhez szükséges informatikai ismeretek körét, hanem az adott személyek konkrét munkaköri leírásában, megsértette az Öpt. 40/C. § (9) bekezdésében foglaltakat.

1.3. Az Észrevételek és egyéb nyilatkozatok

A Pénztár az Észrevételekben előadta, hogy az IBU-07-es utasítás szövegezését pontosította a jelenlegi gyakorlat alapján, melynek alátámasztására dokumentumot is csatolt (IBU_07_Rendszerhozzáférések_v2 3.3-as fejezet).

A Pénztár az IBU-02-es utasítás kapcsán előadta, hogy annak szövegében valóban nem történt módosítás a megállapításokban jelzett dátum óta, de ennek oka az, hogy a Pénztár a módosítás szükségességét nem is tartotta indokoltnak sem az IBU-02-es utasítás felülvizsgálatakor a kockázatelemzés során, sem a Pénztárnál lefolytatott GDPR projekt során felmerülő felülvizsgálatkor. (A Pénztár megemlítette, hogy az IBSZ dokumentum történetiségét rögzítő fedlapján látható, hogy az IBSZ-ben az adatosztályozással kapcsolatos változtatás is történt az Adatvédelmi Szabályzattal történő GDPR célzatú összehangoláskor). Az IBU-02-es utasítás tartalmazza az adatosztályozással kapcsolatos felelősségeket, feladatokat, a dokumentálás helyét, a szükséges forrásokat. Az IBU-02-es utasítás hivatkozása alapján az IBSZ 6.2-es fejezete tartalmazza az adatbesorolások kategóriával szemben támasztott alapvető informatikai elvárásokat, az Adatvédelmi Szabályzat (melyet az INF.01_IT-25 Adatvedelmi_szabalyzat_20190426_korr.docx néven csatolt a Pénztár) 15-ös fejezete pedig bemutatja milyen jellegű adatok tartoznak az adott kategóriákba. (a Pénztár megjegyezte, hogy az Adatvédelmi Szabályzatot azonosító kódban az "IT" megjelölés az azt elfogadó Igazgatótanácsot jelöli, és nem az informatikát.) A Pénztár álláspontja szerint az említett rendelkezések megfelelő támpontot adnak az adatbesorolás elvégzéséhez, melyet a BA_bizonylati album tartalmaz. A Pénztár előadta továbbá, hogy a BA_Bizonylati albumban pontosította az „Adatgazda kijelölése, adatok besorolása" részt az egyértelműbb megfelelőség érdekében (a Pénztár az említett dokumentumot a BA_Bizonylati album v4.2 név alatt csatoltan megküldte az MNB részére). Az adatgazdákkal szemben támasztott

egyéb elvárásokat elsősorban az Adatvédelmi Szabályzat tartalmazza, mint például, de nem kizárólagosan az adatkatalógus frissen tartása. (Lásd Adatvédelmi Szabályzat 10-es fejezet).

A Pénztár előadta, hogy a frissítésekkel, biztonsági javításokkal kapcsolatos szabályozás az időközben bevezetett WSUS rendszerrel összhangban elkészült és kiadásra került, és a Pénztár ennek alátámasztása céljából megküldte az MNB részére a IÜU_04_Szoftvergazdálkodás_v2.3 dokumentumot.

A Pénztár előadta továbbá, hogy biztonsági naplózás/naplózási folyamat szabályozással rendelkezik. Az ezzel kapcsolatos szabályozásokat az IÜU_01_Rendszermonitorozás és a IBU_07_Rendszerhozzáférések szabályzatok tartalmazzák. A Pénztár előadta, hogy a releváns dokumentációt már korábban átadta az MNB részére; a vonatkozó részek az IBU_07: VPN és INGRID naplózási elvárások 3.2-es fejezete, IÜU_01: 3.1, 3.2, 3.3-as fejezetek: szerver, biztonsági mentés, VPN, hálózati forgalom, fizikai védelem riasztó be/kilépési naplók, napló megőrzési idő.
A Pénztár továbbá a naplóellenőrzések elvégzéséről evidenciát csatolt (INF.01 Naplóelemzések.docx).

A Pénztár előadta továbbá, hogy az új székházában jelenleg „7/24" élőerős őrzés működik, és az egyéb fizikai biztonsági eszközök pilot üzemmódú alkalmazása során nyert tapasztalatok alapján az eljárásrendek kialakítása folyamatban van (beléptető kártyák, kulcskiadás, riasztó rendszer). Az élőerős őrzés miatt a riasztó naplók ellenőrzése 2020. áprilistól feleslegessé vált.
A Pénztár előadta, hogy az intézkedési tervben is szereplő naplózási rendszer fejlesztésével összhangban kerül majd sor a naplózási szabályzatok gyakorlathoz történő igazítására is. A dedikált/profi naplózással kapcsolatos ajánlat elkészült és a döntés szerint a következő pénzügyi év tervében kerül majd jóváhagyásra a Pénztár oldaláról a szükséges forrás, amelynek várható elfogadása a 2020. decemberben tartandó küldöttközgyűlésen történik meg. A tervezett megvalósítási határidő: 2021.06.30.

A Pénztár előadta, hogy a jelszókezelés kapcsán az IBSZ törzsdokumentum elsősorban alap- és irányelveket fogalmaz meg: a jelszókezeléssel kapcsolatos konkrét és gyakorlati szabályozást a IBU-07-es utasítás 3.4-es fejezete tartalmazza, ami megfelel a jelenleg alkalmazott jelszókezelési gyakorlatnak. A Pénztár álláspontja szerint emiatt nem indokolt az IBSZ törzsdokumentum módosítása.

A pénztár előadta továbbá, hogy az egyes munkakörök betöltéséhez szükséges ismereteket a Pénztár az IÜU_04_Szoftvergazdálkodás_v2.3 szabályzatban fogalmazta meg és fogadta el (mely dokumentumot a IÜU_04_Szoftvergazdálkodás_v2.3 néven megküldte az MNB részére).

1.4. Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a megállapítást részben vitatta, illetve az Észrevételekben megtett és tervezett intézkedésekről számolt be.

A Pénztár az IBU-07-es utasítást a jogosultság igénylés és az INGRID rendszer naplózási követelmények részével aktualizálta, a Pénztár a bizonylati albumát kiegészítette. Az MNB a Pénztár által a szabályozás felülvizsgálata érdekében megtett intézkedéseket kockázatcsökkentő intézkedésként figyelembe veszi. Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítás ezen részét az 1.1. pontban szereplő tartalommal fenntartja.

A Pénztár vitatta az IBU-02-es utasítás módosításának szükségességét. Az IBU-02-es utasítás nem határoz meg konkrét módszertant az adatok osztályozására és a rendszerek besorolására, hanem hivatkozást tesz arra, hogy az IBSZ-ben vannak definiálva a biztonsági osztályokhoz előírt védelmi intézkedések, továbbá az IBSZ tovább hivatkozik az Adatvédelmi Szabályzatra, ahol a biztonsági osztályokba tartozó adatok köre rögzített. A fenti hivatkozások bonyolult struktúrája nehezíti a szabályok átláthatóságát, és ennélfogva hátráltatja az adatgazdákat az adatosztályozás végrehajtásában. Tekintetbe véve, hogy az IBSZ és az Adatvédelmi Szabályzat tartalmazza a konkrét módszertant, ennélfogva célszerű az IBSZ-be beépíteni az IBU-02-es utasításban meghatározott "adatosztályozással kapcsolatos felelősségeket, feladatokat, a dokumentálás helyét". Az MNB a Pénztár ezen Észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, a megállapítás ezen részét fenntartja az 1.1. pontban foglaltaknak megfelelően.

A Pénztár az operációs rendszer és alkalmazott szoftverek biztonsági javításának telepítési szabályozásával a IÜU_04_Szoftvergazdálkodás szabályzatát kiegészítette. Az MNB a Pénztár által a szabályozás felülvizsgálata érdekében megtett intézkedéseket kockázatcsökkentő intézkedésként figyelembe veszi. Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítás ezen részét az 1.1. pontban szerepelő tartalommal fenntartja.

A Pénztár észrevételében felsorolt biztonsági naplózásra vonatkozó IÜU_01_Rendszermonitorozás szabályzás 3.1, 3.2. és 3.3 pontjai csak az naplózott események körét rögzítik, azok biztonsági elemzésének eszköz általi támogatását, riportálás gyakoriságát és a naplóelemzés részleteit nem tartalmazzák. Az MNB a Pénztár ezen Észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, a megállapítás ezen részét fenntartja az 1.1. pontban foglaltaknak megfelelően.

A Pénztár álláspontja szerint az IBSZ törzsdokumentum elsősorban alap- és irányelveket fogalmaz meg a jelszókezeléssel kapcsolatban, azonban az IBSZ 6.7.4-es pontjában előírt jelszókövetelmények eltérnek a gyakorlati beállítástól és az IBU-07-es utasítás 3.4-es fejezetében leírtaktól. Az MNB álláspontja szerint a szabályozásban leírtak és a gyakorlat összhangjának biztosítása minden szabályzatra vonatkozik. Az MNB a Pénztár ezen Észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, a megállapítás ezen részét fenntartja az 1.1. pontban foglaltaknak megfelelően.

A Pénztár az egyes munkakörök betöltéséhez szükséges informatikai ismeretet az IÜU_04_Szoftvergazdálkodás szabályzatában rögzítette. Az MNB a Pénztár által a szabályozás felülvizsgálata érdekében megtett intézkedéseket kockázatcsökkentő intézkedésként figyelembe veszi. Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítás ezen részét az 1.1. pontban szerepelő tartalommal fenntartja.

1.5. Az MNB által alkalmazott intézkedés

A fentiek alapján a jelen határozat rendelkező részének 1. pontjában az MNB felszólította a Pénztárat, hogy az informatikai tárgyú szabályzatait mindenkor tartsa összhangban a jogszabályi elvárásokkal és a gyakorlati működésével.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 1. pontjában foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

2. Informatikai környezet határvédelme

2.1 Megállapítás (tényállás)

A Vizsgálat megállapította, hogy a Pénztár IT hálózata nem teljeskörűen szegmentált. A Pénztár élesüzemi szerverei és teszt szerverei, valamint a munkaállomásai közös hálózati szegmenst használnak. A szerverek képernyőin a szerver üzemmódja (éles-teszt) látható. Ugyanezen a hálózati szegmensben találhatóak a Pénztár vagyonkezelőjének, az MKB Pannónia Alapkezelő Zrt. **(Alapkezelő)** szerverei (élesüzemi és teszt), valamint munkaállomásai is. A két intézmény szerverei és munkaállomásai nincsenek külön VLAN-ban, hálózati forgalmuk közös. Szintén közös a tűzfaluk és a hálózati mentési tárhelyük.

Az internetet elválasztó MikroTik tűzfalon a Pénztárból kimenő adatforgalmon a Pénztár port- és protokoll szintű szűrést nem végez. Az egyes jóváhagyott tűzfalszabálykérelmeket nem lehet egyértelműen nyomon követni a beállított tűzfalszabályokban. A Pénztár által bemutatott éves tűzfalszabály-felülvizsgálatok nem teljeskörűek, nem került minden érvényes szabály felülvizsgálatra.

A Pénztár az MNB IT.32 számú adatkérésére adott nyilatkozata alapján a munkaállomásokat leszámítva IDS/IPS (behatolásmegelőző/-detektáló) megoldással nem rendelkezik, továbbá DDoS (Distributed Denial of Service/Elosztott szolgálatás megtagadás) támadás elleni védelmi megoldással sem rendelkezik.
A Pénztár több, a belsőhálózatából elérhető webes alkalmazásának, így például az INGRID nyilvántartórendszer (éles: http://192.168.0.92:8080/ingrid/, teszt: http://192.168.0.93/ingrid), valamint az üzemeltetési monitorozásra használt Icinga adminisztrátori felülete (http://192.168.254.13/icingaweb2/) esetében a kommunikáció nem titkosított protokoll (http) használatával valósul meg, így a szerver és a kliensek között közlekedő adatok

bizalmassága, sértetlensége és hitelessége, többek közt a belépési adatok (azonosítók, jelszavak) esetén sem biztosított.

[INF.03], [IT.0 - 23_Szabalyozas], [IT.0 - 41_Uzemeltetes], [IT.0 - 42_Nyilvantartasok], [IT.0 - 44_Halozat], [IT.0 - [52_IBF], [IT.16], [IT.29 – IT.35]

2.2 A Megállapítás minősítése

Az Öpt 40/C. § (5) bekezdése szerint: „A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
(…)
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról,
(…)
e) a távadatátvitel, valamint a kizárólag elektronikus úton megvalósuló pénzügyi tranzakciók bizalmasságáról, sértetlenségéről és hitelességéről, (…)"
Az Öpt 40/C. § (6) bekezdése szerint: „A pénztárnak tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
(…)
d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását,"

Az élesüzemi és a teszt környezet elkülönítés nélküli használata növelheti annak a kockázatát, hogy a tesztkörnyezet egyes folyamatai előre nem látható negatív hatást váltanak ki az élesüzemi környezetben.
Egy, a Pénztártól eltérő, idegen intézmény (jelen esetben az Alapkezelő) szervereinek a működtetése a saját hálózatban kockázatot jelenthet a saját adatok bizalmasságára és sértetlenségére nézve. Az idegen intézménnyel (Alapkezelő) közös használatú szerverek pedig a fentieken kívül növelhetik az adatok rendelkezésre állás elvesztésének a kockázatát.
A tűzfalszabályok kezelésének gyakorlata miatt az igénylési folyamat end-to-end ellenőrzése, valamint tűzfalszabályok ellenőrzések végrehajtása nem biztosítható egyértelműen, ezáltal szükségtelen tűzfalszabályok kerülhetnek beállításra, illetve maradhatnak érvényben, melyek biztonsági kockázatot növelő tényezők.
A Pénztárat elhagyó adatforgalom port- és protokollszűrés nélküli kiengedése az internetre megnövelheti az adatszivárgás- az adatvesztés-, valamint az ártalmas webhelyekhez való csatlakozás kockázatát.
A hálózati forgalom során a hitelesítési adatok nem kikényszerített titkosítása nagymértékben növelheti annak a kockázatát, hogy a hitelesítési adatokhoz illetéktelen személyek hozzáférhetnek. A nem titkosított hitelesítési adatok, valamint az a tény, egy másik jogi entitásnak a forgalma is ugyanazon a hálózati szegmensen zajlik -hálózati behatolásjelző (IDS/IPS) használat nélkül-, igen magas adatbiztonsági kockázatot jelenthet.

A Pénztár a fentiekben leírt hiányosságokkal megsértette az Öpt. 40/C. § (5) bekezdés b) és e) pontjában, valamint a (6) bekezdés d) pontjában foglalt rendelkezéseket.

2.3 Az Észrevételek és egyéb nyilatkozatok

A Pénztár az Észrevételekben az Alapkezelővel közös hálózati szegmens kapcsán előadta, hogy a közös hálózat mindkét fél részéről már korábban is ismert és felvállalt kockázat volt. A Pénztár az alábbi érveket jelölte meg a kockázat felvállalás okaiként (többek között):

- Mindkét szervezet IT infrastruktúráját a Pannónia Pénztárszolgáltató üzemelteti. A fizikai szerverek, a tűzfal és a LAN valóban közös, de minden más szempontból logikailag szétválasztottak a rendszerek.
- Mindkét szervezet, sőt a virtuális hostok is külön-külön Active Directory-ban vannak, a szervezetek nem használnak semmi olyan logikai szervert/rendszert közösen, amelyben adatok vagy felhasználói loginok lennének.
- A két szervezet szerverei minden szempontból hasonló szinten vannak, az üzemeltetésük és a biztonsági szabályzataik is egyenszilárdságúak.
- A felhasználói fluktuáció elhanyagolható szintű.
- A két szervezet között tulajdonosi kapcsolat is van.

A Pénztár előadta, hogy a biztonsági mentések a helyi mentési tárhelyen jól elkülönített könyvtárakban vannak, sőt a szintén napi mentésű Offsite helyen mindkét szervezetnek saját backup szervere is van, külön-külön szerverhoteli elhelyezési szerződéssel. A Pénztár ugyanakkor arról tájékoztatta az MNB-t, hogy a hálózat szétválasztását tervbe vette, és már az intézkedési tervben szerepel; a Pénztár 1 (egy) éven belül tervezi megvalósítani a két hálózat szétválasztását.

A Pénztár arról is tájékoztatta az MNB-t, hogy a kimenő forgalom port- és protokoll szintű szűrését a 2020 év végéig esedékes kockázatelemzésben megvizsgálja, és a kockázat elemzés függvényében dönt róla.

A Pénztár 2019 novemberében az üzleti igényekkel egyeztetett, vezető által jóváhagyott tűzfal szabály dokumentumban leírt, akkor aktuális szabályozást elfogadta, és a Mantis Helpdesk rendszerben minden tűzfalváltoztatásról kérelem és jóváhagyás készül. A Pénztár álláspontja szerint ez a szabályokkal összeegyeztethető eljárás (a Pénztár példaként csatolta az INF.03 Tűzfal igények és szabályok dokumentumot).

A Pénztár az IPS/IDS kapcsán előadta, hogy a 2020 év végéig esedékes kockázatelemzésben megvizsgálja, és a kockázat elemzés függvényében dönt róla.

A Pénztár előadta továbbá, hogy az Icinga, INGRID rendszerek https protokollal történő használatára való átállás részben megtörtént; ennek bizonyítása céljából csatolta az INF.3 https dokumentumot.
A Pénztár előadta, hogy a belső hálózatából elérhető webes alkalmazások (INGRID nyilvántartórendszer (éles: http://192.168.0.92:8080/ingrid/, teszt: http://192.168.0.93/ingrid)) esetében megkezdte a titkosított protokoll alkalmazásának tesztelését.
A Pénztár továbbá arról tájékoztatta az MNB-t, hogy 2020.06.18-án a Teszt rendszeren (https://nyp-ingrid-app-test.vit2000.hu:8443/ingrid) az új protokoll már átállításra került. Az éles rendszeren az új protokollt a Pénztár a teszt rendszer tapasztalatai alapján legkésőbb a 2020.07.07-ei tervezett frissítés keretein belül élesíti.

2.4 Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a hálózati szegmentáció hiányát nem vitatta, hanem magyarázatot kívánt adni a hiányosság tudatos felvállalásának okaira. Az MNB álláspontja szerint a Pénztár által felsorolt okok, mint például a Pénztár és az Alapkezelő szervezet közös hálózati szegmensen lévő szerverei egyenszilárdsága, illetve a közös szervereken lévő elkülönített könyvtárak használata nem helyettesítik a hálózati szegmensek teljes fizikai vagy logikai szétválasztást. A részbeni közös tulajdonosi struktúra nem minősül olyan kivételnek, ami mentességet adna a jogszabályban meghatározott kötelezettségek végrehajtása alól. A Pénztár a megállapításhoz kapcsolódó tervezett intézkedésről számolt be, de a tervezett intézkedést alátámasztó dokumentumot nem csatolt. Az MNB a Pénztár ezen Észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, a megállapítás ezen részét fenntartja a 2.1. pontban foglaltaknak megfelelően.

A Pénztár a tűzfalon kimenő forgalom port- és protokollszűréssel kapcsolatosan tett megállapítást nem vitatta. A megállapításhoz kapcsolódóan tervezett, feltételes jövőbeli intézkedésről számolt be, ahhoz alátámasztó dokumentumokat nem csatolt. Az MNB a megállapítás ezen részét fenntartja a 2.1. pontban foglaltaknak megfelelően.

A Pénztár a tűzfalszabálykérelmek nyomonkövethetőségének hiányosságára tett megállapítást vitatta. A Pénztár által példaként csatolt INF.03 Tűzfal igények és szabályok dokumentumban szereplő NYP-DMZ-WEBSRV-TEST gépen létrehozott szabály és annak magyarázó része szerepel mind a Mantis Helpdesk rendszerben, mind a tűzfalszabályok megjegyzés mezőjében, ugyanakkor nem szerepel egy egyedi azonosító, ami egyértelműen hozzárendeli a felvitt tűzfalszabályt annak kérelméhez. Az MNB a Pénztár ezen Észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, a megállapítás ezen részét fenntartja a 2.1. pontban foglaltaknak megfelelően.

A Pénztár az IPS/IDS megoldás hiányára tett megállapítást nem vitatta. A megállapításhoz kapcsolódóan tervezett, feltételes jövőbeli intézkedésről számolt be, ahhoz alátámasztó dokumentumokat nem csatolt. Az MNB a megállapítás ezen részét fenntartja a 2.1. pontban foglaltaknak megfelelően.

A Pénztár az ICINGA és az INGRID rendszerei elérésénél a titkosított HTTPS protokoll hiányára tett megállapítást nem vitatta. Az ICINGA szerver (https://192.168.254.13/icingaweb2/) és a INGRID teszt rendszereinek (https://nyp-ingrid-

app-test.vit2000.hu:8443/ingrid) HTTPS protokolra való átállást az INF.03 https nevű dokumentummal bizonyította, melyet az MNB kockázatcsökkentő tényezőként figyelembe vesz. A megállapításokhoz kapcsolódó további tervezett intézkedésről számolt be, ahhoz alátámasztó dokumentumokat nem csatolt. Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítás ezen részét a 2.1. pontban szereplő tartalommal fenntartja.

2.5. Az MNB által alkalmazott intézkedés

Fentiek alapján a jelen határozat rendelkező részének 2. pontjában az informatikai biztonsággal kapcsolatban az MNB felszólította a Pénztárat, hogy

d) a jogszabályi követelményeket figyelembe véve biztosítsa a kockázatokkal arányosan az informatikai hálózatának szeparálását más jogi entitásoktól, valamint a belső hálózatának további szeparálását az éles és tesztrendszerek megfelelő szétválasztása érdekében;
e) vizsgálja felül a tűzfalszabály kezelési-, felülvizsgálati-, és nyilvántartási eljárásait, gyakorlatát és a kockázatokkal arányosan gondoskodjon olyan szabályozásról és folyamatokról, melyek biztosítják a tűzfalszabályok rendszeres érdemi felülvizsgálatát és az ellenőrzések teljeskörűségét; a tűzfalszabályok létrehozásakor rendeljen minden tűzfalszabályhoz egy egyedi azonosítót, és azt tüntesse fel mind a kérelemben, mind a felvitt szabálynál a tűzfalon;
f) vizsgálja felül és a kockázatokkal arányosan erősítse a határvédelmi funkciók használatát, beleértve az IDS/IPS védelmet és DDoS elleni támadások elleni védelmet;
g) gondoskodjon a hitelesítési adatok bizalmasságának teljeskörű biztosításáról, valamint a hálózati forgalom sértetlenségének és hitelességének kockázatokkal arányos védelméről.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 2. pontjában foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

3. Adatbázisok kezelése

3.1. Megállapítás (tényállás)

A Vizsgálat megállapította, hogy az INGRID rendszert kiszolgáló Oracle 18.6.0.0.190416 Standard „NYP-INGRID-DB" adatbázisszerveren a Vizsgálat helyszíni szakasza alatt is aktív adatbázis adminisztrátori jogosultsággal rendelkező „Setup" felhasználóhoz tartozó alapértelmezett jelszó nem került megváltoztatásra, továbbá a Pénztár az egyes felhasználói profilok esetében nem alkalmaz megfelelő jelszókövetelményeket, így több profil esetében a „PASSWORD_LIFE_TIME", „PASSWORD_REUSE_MAX", „PASSWORD_REUSE_TIME" paraméterek beállításai gyengék vagy alapértelemezettek. A „sec_protocol_error_trace_action" paraméter értéke az üzemszerű működés során nem indokolt, az felesleges tárhely töltődéssel járhat egy támadás során.

A Vizsgálat megállapította továbbá, hogy az éles INGRID adatbázisban több, nem az éles működéshez szükséges felhasználói azonosító is aktív volt a Vizsgálat helyszíni szakasza alatt, így például a „Teszt", „Teszt2" azonosítók, valamint a Vizsgálat helyszíni szakasza alatt már kilépett adatbázis adminisztrátori jogosultsággal bíró felhasználó „HorvathM" azonosítója.

A Vizsgálat megállapította azt is, hogy az auditing beállítások közül a Pénztár az objektumok auditálási lehetőségét nem használja (DBA_OBJ_AUDIT_OPTS), valamint az Oracle adatbáziskezelő új, „Unified Auditing" funkcióját sem alkalmazza.

A Vizsgálat szintén megállapította, hogy az éles TRASSET adatbázist kiszolgáló „INGRID-SERVER" Oracel 11.2 adatbázis szerver esetében is az egyes profilokhoz tartozó „PASSWORD_LIFE_TIME", „PASSWORD_REUSE_MAX", „PASSWORD_REUSE_TIME", „PASSWORD_LOCK_TIME" paraméterek beállításai gyengék vagy alapértelemezettek, valamint egyik profil esetében sem biztosítanak megfelelő jelszó ellenőrzést, mivel a „PASSWORD_VERIFY_FUNCTION" paraméter értéke „NULL".

A Vizsgálat megállapította, hogy az éles TRASSET adatbázis esetében is a „remote_login_passwordfile" paraméter értéke alapján jelszófájlok használata nem tiltott, illetve a „sec_case_sensitive_logon" beállítás tiltott, így jelszavak kis- és nagybetűk érzékenysége nem kerül alkalmazásra, továbbá a „sec_protocol_error_trace_action" és a „sec_protocol_error_further_action" paraméterek értéke az üzemszerű működés során nem indokolt, azok egyes

támadási módok esetén felesleges tárhely töltődéssel járhatnak. Továbbá az éles TRASSET adatbázisszerveren az „audit_sys_operations” paraméter tiltott, így a SYSOPER és a SYSDBA fiókok alatt végzett összes felhasználói tevékenység auditálása nem biztosított.

A vizsgált Oracle adatbázisok alapján a Vizsgálat megállapította, hogy a Pénztár az adatbázisainak kezelésével kapcsolatban nem definiált eljárást, elvárt követelményeket az adatbázis konfigurációs- és hardening beállításokra, így az adatbázisok biztonsági paramétereinek, felhasználó- és jelszó követelményeinek, naplózási beállításainak az elvárható legjobb gyakorlatnak való folyamatos megfeleltetése sem biztosítható egyértelműen.

[INF.08], [IT.0 - 23_Szabalyozas], [IT.0 - 41_Uzemeltetes], [IT.0 - 42_Nyilvantartasok], [IT.0 - 44_Halozat], [IT.86], [IT.87]

3.2 A Megállapítás minősítése

Az Öpt 40/C. § (5) bekezdése szerint: „A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
(…)
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról,
(…)
d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére, (…)”

A megállapításban foglaltak alapján az adatbáziskezelőkre érvényes egységes hardening szabályozás, az adatbáziskezelő paraméterek, naplózási beállításainak hiányában illetéktelenül végrehajtott események maradhatnak felderítetlenül; továbbá az érvényes adatbázis profil beállítások miatt az azonosítókkal és jelszavakkal való visszaélés kockázata magasabb; ennélfogva a Pénztár a fentiekben leírtakkal megsértette az Öpt. 40/C. § (5) bekezdése b) és d) pontjaiban foglalt rendelkezéseket.

3.3 Az Észrevételek és egyéb nyilatkozatok

A Pénztár az észrevételekben megtett intézkedésekről számolt be.

A Pénztár előadta, hogy a sec_protocol_error_trace_action paraméter értékét TRACE értékről ALERT -re állította, így protokoll hiba esetén kap figyelmeztetést az alert.log állományba, de nem keletkezik feleslegesen nagy méretű trace állomány.

A Pénztár előadta, hogy az unified auditing beállítási lehetőség az Oracle 12c verziótól kezdve érhető el. Az INGRID rendszer korábban Oracle 11g verzión működött és a 18c upgrade során a Pénztár nem érezte szükségességét az addig is beállított audit trail módosításának. A Pénztár vállalta, hogy az unified audit beállítását az éles rendszer soron következő leállása alkalmával beállítja (amikor a https-t is konfigurálja).

A Pénztár előadta továbbá, hogy az Észrevételek tételének idején nem auditálja külön az adatbázis objektumokat, ezért nem található semmi a DBA_OBJ_AUDIT_OPTS-ban. Jelenleg a ki és bejelentkezések, illetve az objektumok létrehozása, módosítása (DDL utasítások) vannak auditálva Oracle szinten. Az adatbázis táblákban történő módosításokat az Észrevételek tételének idején a Pénztár csak alkalmazás szinten logolja és a log információk megváltoztatására alkalmazás szinten nincs lehetőség. A Pénztár vállalta, hogy az auditálás megerősítésére a következő módosításokat bevezetését teszi meg:

(i) A rendszert olyan módon fogja korlátozni, hogy az INGRID rendszer felhasználói ezentúl kizárólag az INGRID alkalmazáson keresztül tudjanak hozzáférni az adatokhoz, az adatbázishoz közvetlen hozzáféréssel ne rendelkezzenek. Az adatbázishoz közvetlen hozzáféréssel rendelkező felhasználók pedig az adatbázis hozzáféréshez engedélyezett felhasználónévvel ne tudjanak belépni az INGRID alkalmazásba. Ezt adatbázis LOGON triggerekkel tervezi a Pénztár megvalósítani.

(ii) Az INGRID programon keresztül csatlakozó felhasználók műveletei az INGRID rendszerben naplózásra kerülnek már az Észrevételek tételének idején is. Az INGRID programon keresztül nincs semmilyen lehetőség a naplók manipulálására, törlésére. Ezek a logok az INGRID programon keresztül ellenőrizhetők.
(iii) A közvetlen adatbázis hozzáférés kockázatát úgy tervezi csökkenteni a Pénztár, hogy azoknak a felhasználóknak, akik nem az INGRID alkalmazáson keresztül jelentkeznek be az adatbázisba, valamennyi műveletét naplózza az Oracle audit lehetőségével.
(iv) Minden felhasználó bejelentkezését, kilépését, hibás bejelentkezési próbálkozását, akár az INGRID, akár más alkalmazáson keresztül történik, a Pénztár szintén naplózza az Oracle audit lehetőségével.

A Pénztár jelezte, hogy a fenti pontokban felsorolt intézkedések megvalósítására az INF.14-hez becsatolt Ingrid jogosultsági és naplózási koncepció megvalósításával egyidejűleg kerül majd sor.

A Pénztár előadta, hogy az éles Ingrid rendszerben a HORVATHM, a TESZT és a TESZT2 felhasználók tiltásra kerültek mind az ügyintézői felületen, mind adatbázis szinten; továbbá mellékelte a tiltásról készült képernyőképeket (INF.08 Fiókok.doc) és a friss felhasználói listát (INF.08_Ingrid_felhasználói lista.xls).

A Pénztár jelezte továbbá, hogy megrendelésre került a Trasset kiszolgálók cseréje, melynek során az MNB által hiányolt beállításokat is elvégezni tervezi. A Pénztár csatolt a megrendelő lapot (INF.08_TRASUPP_15534_feladatlap.pdf).

3.4 Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a megállapítást nem vitatta, Észrevételében megtett, folyamatban lévő és tervezett intézkedésekről számolt be.
A Pénztár a megtett intézkedések igazolására csatolta az Ingrid Oracle adatbázis beállításainak erősítését igazoló képernyőképeket, melyeket az MNB kockázatcsökkentő tényezőként figyelembe vesz.
A Pénztár által csatolt az Oracle adatbázisok erősítésére szolgáló terveit az MNB támogatja, azok eredményéről visszajelzést vár.
A Pénztár a Trasset adatbázisa kapcsán csak jövőbeni tervezett intézkedésekről számolt be.
A Pénztár észrevétele a megállapítás szükségességét és tényszerűségét nem befolyásolja, az MNB a megállapítást a 3.1. pontban foglaltak szerint fenntartja.

3.5 Az MNB által alkalmazott intézkedés

Fentiek alapján a jelen határozat rendelkező részének 3. pontjában az MNB felszólította a Pénztárat, hogy a kockázatokkal arányosan hozzon létre és tartson naprakészen a biztonsági beállítások erősítésére, egységesítésére szolgáló „hardening" eljárásokat és ellenőrzési folyamatot az adatbázisai esetében, és biztosítsa azok alkalmazását adatbáziskörnyezeteiben; továbbá gondoskodjon arról, hogy a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenységek naplózása megvalósuljon.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 3. pontjában foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

4. Az informatikai biztonsági rendszer önvédelmére

4.1 Megállapítás (tényállás)

A Pénztár az MNB IT.77 és IT.79 számú adatkéréseire adott nyilatkozatai alapján „A szervezet [a Pénztár] nem rendelkezik sérülékenységvizsgálatot szabályozó dokumentummal.", valamint az MNB IT.81 számú adatkérése adott nyilatkozata szerint „A Pénztár hardening guide-dal, illetve vonatkozó ellenőrzési gyakorlattal nem rendelkezik."
A Pénztár által bemutatott dokumentumok alapján a külső betörési és sérülékenységi vizsgálatok nem terjedtek ki minden releváns szolgáltatásra és IP címre, így például a "portal.pannonianyp.hu (89.135.50.146)" Webes ügyfélportált kiszolgáló szerverre nem történt sérülékenységvizsgálat.
[INF.10] [IT.0 - 23_Szabalyozas], [IT.0 - 41_Uzemeltetes], [IT.0 - 42_Nyilvantartasok], [IT.0 - 44_Halozat], [IT.0 – 52_IBF], [IT.77 – IT.81]

4.2 A Megállapítás minősítése

Az Öpt. 40/C. § (5) bekezdése szerint: „A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
(…)
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról (…)".

Az Internet irányából elérhető szolgáltatások teljeskörű biztonsági tesztelésének rendszeres végrehajtása hiányában alkalmazásbeli sérülékenységek maradhatnak felfedezetlenül, illetve javítatlanul. Emiatt előfordulhat, hogy egy támadó a sérülékenység kihasználásával illetéktelenül férhet hozzá ügyfelek adataihoz.
A biztonsági vizsgálatok folyamatának, hatókörének, a felelősségek, a kockázatok kezelésének és felvállalásának részletes szabályozása nélkül a Pénztár nem tudja a kockázatokkal arányosan kezelni az informatikai rendszereinek kitettségét a kártékonykód és egyéb biztonsági fenyegetettségekkel szemben.
A fentiek miatt a Pénztár megsértette az Öpt. 40/C. § (5) bekezdésének b) pontjában foglalt rendelkezéseket.

4.3 Az Észrevételek és egyéb nyilatkozatok

A Pénztár az Észrevételekben megtett intézkedésekről számolt be.

A Pénztár előadta, hogy a sérülékenység vizsgálattal kapcsolatos szabályozás kiadásra került az eddigi gyakorlatoknak megfelelően, ezzel kapcsolatban csatolva megküldte az MNB számára az IBU-07-es utasítás aktualizált verzióját, megjelölve, hogy annak 3.5-ös fejezete rendelkezik a sérülékenységvizsgálatokról.

A Pénztár továbbá előadta, hogy a sérülékenységi vizsgálat a kimaradt IP címre megtörtént (melynek bizonyítására csatolta az S2_PannoniaNyp_1IP_Infra_Jelentes_200206 nevű dokumentumot). A Pénztár továbbá arról tájékoztatta az MNB-t, hogy a sérülékenységi vizsgálat után az érintett IP címet le is váltotta a Pénztár által újonnan bevezetett portálrendszer. A sérülékenység vizsgálat során talált kockázatok a port átirányítás megszüntetések miatt megszűntek.

4.4 Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a megállapítást nem vitatta, az Észrevételében megtett intézkedésekről számolt be.
A Pénztár a megtett intézkedések igazolására csatolta a sérülékenységi vizsgálatok elvégzésének szabályozását is magában foglaló módosított IBU-07-es utasítást, valamint a kimaradt IP címre történt sérülékenységi vizsgálat jegyzőkönyvét (S2_PannoniaNyp_1IP_Infra_Jelentes_200206). A Pénztár az általa említett újonnan bevezetett portálrendszer sérülékenységi vizsgálatának jegyzőkönyvét nem csatolta.
A Pénztár által csatolt szabályzatot és jegyzőkönyvet az MNB kockázatcsökkentő tényezőként figyelembe veszi.

Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítást a 4.1. pontban szerepelő tartalommal fenntartja.

4.5 Az MNB által alkalmazott intézkedés

Fentiek alapján a jelen határozat rendelkező részének 4. pontjában az informatikai biztonsági rendszer védelmével kapcsolatosan az MNB felszólította a Pénztárat, hogy

a) folyamatosan biztosítsa az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az Internet irányából elérhető szolgáltatásai esetében;
b) végezze el az újonnan bevezetett portál rendszerének sérülékenységi vizsgálatát;
c) a kockázatokkal arányosan hozzon létre és tartson naprakészen a biztonsági beállítások erősítésére, egységesítésére szolgáló „hardening" eljárásokat és ellenőrzési folyamatot a hálózati eszközei, operációsrendszerei, adatbázisai és alkalmazásai esetében.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 4. pontjában foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

5. Felhasználói jogosultságok

5.1. Megállapítás (tényállás)

A Vizsgálat megállapította, hogy az éles INGRID rendszerben nem névhez kötött felhasználói profilokat (például: IRF, illetve a helyszíni vizsgálat alkalmával tiltásra került TESZT és TESZT2) is használ a Pénztár, amelyek esetében a naplóbejegyzésekben a felhasználó egyértelmű azonosítása nem elvégezhető. Az IRF felhasználói profilt az IRF Szoftverház Kft. 9 különböző munkatársa használja, amelyek közül 6 fő fejlesztő. (A Pénztár INGRID nevű informatikai rendszerének üzemeltetését és fejlesztését az IRF Szoftverház Kft. végzi.)
Az Online IT Consulting Kft. által a Pénztári rendszerek távoli adminisztrálására használt „Inforservice Tavadmin" azonosítót szintén több felhasználó használja, így az általuk végzett tevékenységek egyértelmű személyhez kötése csak áttételesen és nehezen biztosítható. (Az Online IT Consulting Kft. a Pénztár informatikai külső tanácsadója, IT üzemeltetője, amely informatikai biztonsági funkciókat is ellát.)
A Vizsgálat megállapította továbbá, hogy a Pénztár nem rendelkezik konkrét összeférhetetlenségi mátrixxal a TRASSET és az INGRID rendszerre vonatkozóan. Az INGRID rendszer jogosultsági rendszerében 15 olyan felhasználó dolgozik, akinek a szerepköreinek a száma 6-nál is több. A Pénztár a 2019 év folyamán az INGRID rendszer jogosultságainak belső vizsgálata során megállapította, hogy az INGRID jogosultságrendszere felülvizsgálatra szorul, aminek elvégzését a 2020-as évre feladatként a Pénztár kitűzte.
A Pénztár az MNB IT.22 számú adatkérésére a következő nyilatkozatot tette: „A Pénztár az IBSZ 6.7 pontjának megfelelő ellenőrzést nem végzett, azonban az IT.022 pontban bemutatott módon végzett felülvizsgálatokat, és azok eredménye alapján a szükséges intézkedéseket meg is tette. A Pénztár felül fogja vizsgálni az IBSZ vonatkozó pontját, hogy a gyakorlatnak megfelelő szabályozást alakítson ki."

A FABI és HorvathM felhasználói profilokhoz tartozó munkavállalók a Pénztárnak az IT13.-as adatkérésre adott válasza alapján a Vizsgálat helyszíni szakaszának időpontjában már nem voltak munkavállalói a Pénztárnak. Ennek ellenére a FABI és HorvathM felhasználói profilok nem kerültek megszüntetésre/tiltásra a Panda Security és a Tűzfal rendszerben, valamint a HorvathM felhasználói profil esetében az Active Directory Domain adminisztrátori jogosultsággal bíró azonosítója is aktív volt. A Vizsgálat megállapította továbbá, hogy az éles INGRID adatbázisban több, nem az éles működéshez szükséges felhasználói azonosító is aktív volt a Vizsgálat helyszíni szakasza alatt, így például a „Teszt", „Teszt2" azonosítók, valamint, a Vizsgálat helyszíni szakasza alatt már kilépett adatbázis adminisztrátori jogosultsággal bíró felhasználó „HorvathM" azonosítója.

A Pénztár munkavállalói listáján (IT.017) szerepelnek az „sferenczi", „vicsapi" felhasználói profilok, mint a TF System Kft. munkatársai (a „vicsapi" felhasználói profil a VPN engedéllyel rendelkezők között is szerepel IT.019), azonban a TF Systems KFt. nyilatkozata (IT.007) ezen felhasználókat már nem tünteti fel, mint a Pénztárhoz rendelt munkatársak. (A TF Systems KFt. a TRASSET nyilvántartórendszer fejlesztését, üzemeltetési támogatását látja el.)
A helyszínen ellenőrzött technikai felhasználókhoz tartozó jelszóborítékok nyilvántartása átalakításra szorul, mivel az egyes jelszavak különálló, sorszámozott borítékolása nem biztosított, valamint a borítékok felvételéhez nem vezetnek egyértelmű nyilvántartást.
[INF.11] [IT.0 - 23_Szabalyozas], [IT.0 - 46_Jogosultsag], [IT.15 – IT.27], [IT.86]

5.2 A Megállapítás minősítése

Az Öpt. 40/C. § (5) bekezdése szerint: „A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
(…)
c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események) (…)".

A hozzáférési jogosultságok nem megfelelő kezelése, ellenőrzése azt eredményezheti, hogy a felhasználók a rendszerekben nem a minimálisan szükséges jogosultsággal rendelkeznek; ez a körülmény pedig az adatokhoz való illetéktelen hozzáférés kockázatát hordozza.
A nem névhez kötött felhasználói profilok révén végzett tevékenységek növelik a csalás kockázatát, továbbá a jogosultságok felülvizsgálatának hiányában nem válik nyilvánvalóvá a napi működés során, hogy az egyes felhasználók a munkájukhoz szükséges és elégséges jogosultságoknál magasabb hozzáférési jogokkal rendelkeznek; ez a körülmény pedig növeli az engedély nélküli adatmódosítás kockázatát.

A technikai azonosítók jelszavainak nem dokumentált felvétele megnehezíti a jelszóval való esetleges visszaélés kivizsgálását.
A fentiekben leírt hiányosságok miatt a Pénztár megsértette az Öpt. 40/C. § (5) bekezdésének c) pontjában foglalt rendelkezéseket.

5.3 Az Észrevételek és egyéb nyilatkozatok

A Pénztár az Észrevételekben arról számolt be, hogy az éles Ingrid rendszerben az IRF, a TESZT és a TESZT2 felhasználók tiltásra kerültek mind az ügyintézői felületen, mind adatbázis szinten. Az IRF munkatársai a frissített kirendelt munkavállalói lista alapján kerültek nevesítve a rendszerben, melynek bizonyítása céljából csatolta az INF.08_Ingrid_felhasználói lista.xls nevű dokumentumot.
A tiltásról készült képernyőképeket a Pénztár az INF.11 Fiókok csatolmányban mutatta be, illetve mellékelten megküldte a módosított listát a kirendelt felhasználókról: INF.11_IRF_KirendeltMunkavállalókListája_20200615.pdf, valamint a FABI és HorvathM fiók jogosultságaival kapcsolatos válaszokat az INF.11 Fiókok nevű dokumentumban megküldte az MNB részére.
A Pénztár előadta továbbá, hogy a Trasset rendszer esetében is felülvizsgálatra és frissítésre került a kirendelt munkavállalók listája, melynek bizonyítása céljából az INF.11_TFSYS_munkavállalói_lista.pdf nevű dokumentumot megküldte az MNB részére.

A Pénztár az Észrevételekben az Infoservice tavadmin felhasználó személyhez kötése kapcsán arra hivatkozva, hogy az IT027 vizsgálati kérdésre bizonyosságot adó nyilatkozatot tett, kérte az erre vonatkozó megállapítás törlését.

A Pénztár végezetül előadta, hogy a jelszó borítékok szeparálása megtörtént, melynek bizonyítása céljából csatolta az INF.11 Boríték nevű dokumentumot.

5.4 Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a megállapítást részben vitatta, az Észrevételekben megtett intézkedésekről is beszámolt.

A Pénztár a megtett intézkedések igazolására csatolta a jelszóborítékok kapcsán megtett intézkedéseit igazoló dokumentumot, az éles Ingrid rendszerből a megállapításban taglalt azonosítók kezelésére vonatkozó dokumentumot, és a felülvizsgálatok dokumentumát. A Pénztár által csatolt dokumentumokat az MNB kockázatcsökkentő tényezőként figyelembe veszi. Tekintettel arra, hogy a hiányosságok a Vizsgált Időszakban fennálltak, az MNB a megállapítás ezen részét az 5.1. pontban szerepelő tartalommal fenntartja.

A Pénztár az Észrevételekben vitatta az "Infoservice tavadmin" azonosító személyhez kötése kapcsán tett megállapítást, hivatkozva az IT.027 számú MNB-s helyszíni adatkérésre adott nyilatkozatára. Az MNB a Pénztár ezen észrevételét ugyanakkor nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, mert az nem ad választ a feltárt kockázatra, vagyis arra, hogy az Online IT Consulting Kft. által a Pénztári rendszerek távoli adminisztrálására használt „Inforservice Tavadmin” azonosítót több felhasználó használja, így az általuk végzett tevékenységek egyértelmű személyhez kötése csak áttételesen és nehezen biztosítható.
Mivel az MNB a Pénztár ezen észrevételét nem találta alkalmasnak a jogszabálysértés hiányának megállapításához, illetve a Pénztár észrevétele a megállapítás szükségességét és tényszerűségét nem befolyásolja, ezért az MNB a megállapítás ezen részét az 5.1. pontban szerepelő tartalommal fenntartja.

5.5 Az MNB által alkalmazott intézkedés

Fentiek alapján a jelen határozat rendelkező részének 5. pontjában a felhasználói jogosultságokkal kapcsolatosan az MNB felszólította a Pénztárat, hogy

a) biztosítsa a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációját;
b) ennek keretében vizsgálja felül jogosultságkezelési gyakorlatát és szabályozását, valamint
c) erősítse a jogosultságok nyilvántartásának, összeférhetetlenségek meghatározásának és kezelésének, visszavonásának és ellenőrzésének folyamatait, illetve
d) gondoskodjon a szükségtelen jogosultságok visszavonásáról;
e) az informatikai rendszerhozzáférésekben csak névhez rendelt egyedi azonosítókat alkalmazzon;

f) valamint gondoskodjon a jogosultság felülvizsgálatok elvárások szerinti rendszeres elvégzéséről.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 5. pontjában foglaltak teljesítését legkésőbb 2021.02.28. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

6. Naplózási rendszer

6.1 Megállapítás (tényállás)

A Vizsgálat megállapította, hogy a Pénztár által használt naplógyűjtő szerver (Kiwi Syslog Server) csak a tűzfal naplóbejegyzéseit fogadja az 514-es UDP porton, de az onnan begyűjtött naplókra nincs beállított vizsgálat, riasztás.
A Vizsgálat megállapította továbbá, hogy a Pénztár egyes rendszereiben nem végez naplózást, így például az MNB IT.84 számú adatkérésére adott nyilatkozata szerint „A Pénztárnál a Linux kiszolgálók esetében nem történik naplózás".
A naplózás sok esetben hiányos és működése szigetszerű még azokban a rendszerekben, helyeken is, ahol be van állítva; így például az Active Directory Domain Controller kiszolgálóin érvényes naplózási beállítások (Audit policy) értelmében a naplózott események köre korlátozott (egyedül a „Fiókkezelés" naplózott), nincsen összhangban a kockázatokkal, ugyanis más fontos elemek (ideértve például, de nem kizárólagosan a „Címtárszolgáltatás-hozzáférést") naplózása nem biztosított.

A Vizsgálat megállapította továbbá, hogy a naplóbejegyzések ellenőrzése több helyen (pl: INGRID rendszer) alkalmi jellegű, és csak az utólagos vizsgálatok segítségére korlátozódik. A naplóvizsgálatokról riportok nem készülnek.
A naplók gyűjtése során, valamint a begyűjtött naplóbejegyzések sértetlensége nem garantált, mivel többek között a gyűjtés az 514-es UDP porton történik. Az UDP 514-es adatkapcsolat sajátossága miatt nem biztosított a sértetlenség (UDP esetében a felek semmilyen, a kommunikáció állapotára vonatkozó információt nem tartanak nyilván, nincs kapcsolatkiépítés, nyugtázás, újra adás stb., és ennek megfelelően nincs kapcsolat hitelesítés sem. Ezek körülmények miatt nagyobb a veszélye - például - az IP forráscím esetleges meghamisításának. Az UDP514-es kapcsolat ezenfelül nyílt, nem titkosított kommunikációs csatornát jelent.) A begyűjtött naplóbejegyzéseket az adminisztrátor utólag visszakereshető bejegyzés nélkül módosíthatja, vagy akár törölheti is.
Az INGRID rendszer naplói a fájlszerveren található – integritásvédelmet nem biztosító – Excel táblázatokba kerülnek exportálásra.
[INF.14] [IT.0 - 23_Szabalyozas], [IT.0 - 54_Naplozas], [IT.24], [IT.82 – IT.85]

6.2 A Megállapítás minősítése

Az Öpt. 40/C. § (5) bekezdése szerint: „A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
(…)
d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére (…)".

A 6.1. pontban szereplő megállapítások alapján a Pénztár a biztonsági naplózást, a biztonsági naplógyűjtést és biztonsági naplóelemzés tevékenységét nem szabályozta megfelelően. A biztonsági naplóelemzés megfelelő szabályozása hiányában, valamint az IT infrastruktúra elemek, a kapcsolódó alkalmazás- és adatbázis megfelelő naplózása és naplóiknak központi gyűjtése hiányában a központi érdemi naplóelemzés teljessége nem biztosítható; ezáltal egy esetleges biztonsági incidens feltárásához szükséges események és összefüggések elemzése nem biztosítható egyértelműen; az egyes biztonsági incidensek, valamint rendszerhibák észlelése időben elhúzódhat, mely biztonsági kockázatot növelő tényező.
A fentiekben foglalt körülmények alapján a Pénztár megsértette az Öpt. 40/C. § (5) bekezdésének d) pontjában foglaltakat.

6.3 Az Észrevételek és egyéb nyilatkozatok

A Pénztár az Észrevételekben előadta, hogy a naplózási szabályozás részletesebb kidolgozása az Ingrid naplózási átalakítás során fog megvalósulni. A Kiwi syslog szerver leváltása professzionális logelemző megoldásra az

intézkedési tervben szerepel, mely átütemezésre került 2021.06.30-as határidővel. A linux kiszolgálók közül csak egy van, amin kritikus rendszer fut, de annak az Oracle naplózása mindig is működött. Az Ingrid jogosultság és naplózási folyamat teljes átalakítás alatt van, melyet egy éven belül tervez bevezetni a Pénztár; ezzel kapcsoltban csatoltan megküldte az MNB részére az INF.14_Ingrid_jogosultság_naplózás_koncipcio.pdf nevű dokumentumot.
A Pénztár előadta továbbá, hogy a kritikus rendszerekre (tűzfal, Active directory, INGRID, TRASSET) vonatkozóan egy éven belül tervezi a naplózások kialakítását.

6.4 Az Észrevételek és egyéb nyilatkozatok értékelése

A Pénztár a megállapítást nem vitatta, az Észrevételekben tervezett intézkedésekről számolt be.
A Pénztár észrevétele a megállapítás szükségességét és tényszerűségét nem befolyásolja, az MNB a megállapítást a 6.1. pontban szerepelő tartalommal fenntartja.

6.5 Az MNB által alkalmazott intézkedés

Fentiek alapján a jelen határozat rendelkező részének 6. pontjában a naplózási funkciókkal kapcsolatosan az MNB felszólította a Pénztárat, hogy

a) a biztonsági kockázattal arányosan tartson fent olyan biztonsági környezetet, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is;
b) gondoskodjon arról, hogy a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenység naplózása megvalósuljon, a naplófájlok sérthetetlensége és rendelkezésre állása biztosított legyen, valamint a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódjanak;
c) a fentiek érdekében vizsgálja felül a naplóelemzési eljárásait, szabályozza a tevékenységet, majd készítsen tervet és valósítsa meg az infrastruktúra elemek, szerverek, alkalmazások, adatbázisok biztonsági naplózását, azok naplóállományainak gyűjtését, valamint kockázatokkal arányosan alakítsa ki a központi automatikus biztonsági naplóelemzési- és riasztási képességeit.

Az MNB felszólította továbbá a Pénztárat, hogy az a jelen határozat rendelkező részének 6. pontjában foglaltak teljesítését legkésőbb 2021.06.30. napjáig – dokumentumokkal alátámasztva – igazolja az MNB részére.

III. Az MNB által alkalmazott intézkedések

Az intézkedések jogalapja

Az MNB tv. 75. § (1) bekezdés a) pontja alapján, ha az MNB a 62. § (2) bekezdése szerinti ellenőrzés – mint a Vizsgálat – végén vagy az általa hivatalosan ismert tények alapján megállapítja a Pénztár működésére és tevékenységére vonatkozó jogszabályokban meghatározott kötelezettségek megszegését, elkerülését, elmulasztását, késedelmes vagy hiányos teljesítését – ha törvény eltérően nem rendelkezik – az Öpt. szerinti intézkedést, kivételes intézkedést alkalmazza, illetve bírságot szab ki.

A Pénztár kötelezettségeinek teljesítése, a pénztártagok érdekeinek védelme, valamint a pénztártevékenységre vonatkozó jogszabályi előírások betartása érdekében az MNB az Öpt. 65. § (3) bekezdése alapján az ott meghatározott intézkedéseket – akár együttesen is – alkalmazhatja.

1. Felszólítás a jogszabályoknak való megfelelésre (jelen határozat 1-6. pontja)

Az Öpt. 65. § (3) bekezdésének a) pontja alapján az MNB az Öpt.-ben és a pénztártevékenységre vonatkozó más jogszabályban meghatározott feltételeknek való megfelelésre, valamint a jogsértő magatartás abbahagyására – esetleg határidő kitűzésével – felszólíthat.

Az MNB tv. 75. § (4) bekezdése szerinti mérlegelési jogkörében eljárva az MNB úgy ítélte meg, hogy a Vizsgálat által feltárt jogsértések esetén a Pénztár jogszabályszerű működésének helyreállításához szükséges a Pénztár rendelkező rész szerinti, a vonatkozó jogszabályi előírások betartására vonatkozó felszólítása, illetve a feltárt jogsértések és hiányosságok orvoslásához a kidolgozandó és végrehajtandó intézkedések nélkülözhetetlenek. Ezen túlmenően a felszólítás alkalmazását az MNB szükségesnek tartotta azon jogalkalmazói cél eléréséhez is, hogy a Pénztár a jövőben tartózkodjon a hasonló típusú jogsértések megvalósításától, továbbá ösztönözve legyen a jogszabálysértéseket megvalósító körülményei megváltoztatására.

Fentiekre tekintettel az MNB a jelen határozat rendelkező részének 1-6. pontjában előírt felügyeleti intézkedésekről határozott, figyelemmel arra is, hogy a Pénztár több esetben vállalta a jogsértés megszüntetését. Az intézkedések alkalmazása során az MNB az MNB tv. 75. § (4) bekezdésében meghatározott körülmények közül az a), b), c), e), és f) pontok alapul vételével tekintettel volt a szabályok megsértésének, illetőleg a hiányosságoknak a súlyosságára, a cselekménynek a biztonságos működésre, valamint az ügyfelekre gyakorolt hatására.

Az MNB tv. 48. § (4) bekezdése alapján az MNB felhívására az MNB tv. 39. § (1) bekezdésében meghatározott törvények hatálya alá tartozó személy és szervezet – így a Pénztár is – köteles az MNB feladatellátásához kért, a tevékenységére vonatkozó tájékoztatást megadni, a hatósági eljárás tárgyával összefüggő adatot, továbbá az előbbiekben fel nem sorolt egyéb kimutatást az MNB által meghatározott formában elkészíteni és rendelkezésére bocsátani.

Az MNB fokozottan figyelemmel kívánja kísérni a határozat rendelkező részében foglalt egyes intézkedések teljes körű végrehajtását, ezért az MNB tv. 75. § (4) bekezdése szerinti mérlegelési jogkörében eljárva a határozat rendelkező részének 1-6. pontjában foglaltakhoz kapcsolódóan – egyúttal annak teljesítési határidejét is meghatározva – adatszolgáltatási kötelezettségek előírásáról is határozott.

2. AZ MNB ÁLTAL KISZABOTT BÍRSÁG (7. PONT)

2.1. A felügyeleti bírság kiszabása

2.1.1.A bírság jogalapja

Az MNB tv. 75. § (1) bekezdés a) pontja alapján, ha az MNB a Vizsgálat végén vagy az általa hivatalosan ismert tények alapján megállapítja a pénztárak működésére és tevékenységre vonatkozó jogszabályok, vagy az MNB hatósági határozatában meghatározott kötelezettség megszegését, elkerülését, elmulasztását, késedelmes vagy hiányos teljesítését, – ha törvény eltérően nem rendelkezik – a Pénztár esetén az Öpt. fentebb már hivatkozott 65. § (3) bekezdésének a) pontja szerinti intézkedés alkalmazása mellett bírságot szabhat ki.

Az Öpt. 65. § (3) bekezdés f) pontja alapján a Pénztár kötelezettségeinek teljesítése, a pénztártagok érdekeinek védelme, valamint a pénztártevékenységre vonatkozó jogszabályi előírások betartása érdekében az MNB felügyeleti bírság megfizetésére kötelezhet.

2.1.2. A bírság kiszabásának indoka

Az MNB célja – figyelemmel az MNB tv. 4. § (9) bekezdés c) és d) pontjára – az egyes pénzügyi szervezeteket, illetve egyes szektorokat fenyegető, nemkívánatos üzleti és gazdasági kockázatok feltárása, a már kialakult egyedi vagy szektoriális kockázatok csökkentése vagy megszüntetése, illetve az egyes pénzügyi szervezetek prudens működésének biztosítása érdekében megelőző intézkedések alkalmazása, valamint a pénzügyi szervezetek által nyújtott szolgáltatásokat igénybevevők érdekeinek védelme, a pénzügyi közvetítőrendszerrel szembeni közbizalom erősítése. E törvényi célok elérése érdekében az MNB határozottan, következetesen és szigorúan fel kíván lépni az ellenőrzési eljárásai során feltárt, vagy az általa hivatalosan ismert tények alapján tudomására jutott minden olyan magatartással szemben, amely sérti vagy veszélyezteti a pénztári tevékenységet végző szervezetek ügyfeleinek az érdekeit, illetve alkalmas a pénzügyi közvetítőrendszerrel – így az önkéntes és magánnyugdíjpénztári piaccal – szembeni közbizalom gyengítésére, valamint az átlátható, hatékony és prudens működés megzavarására. Ebben a tekintetben az MNB ellenőrzési tevékenysége akkor tekinthető hatékonynak, ha betölti a jogszabályi rendeltetését, azaz felfedi – többek között – az önkéntes és magánnyugdíjpénztári tevékenységet végző szervezetek és személyek által elkövetett jogszabálysértéseket, és azok miatt arányos, következetes és kiszámítható jogkövetkezményt,

megfelelő jellegű és mértékű intézkedést, illetve szankciót alkalmaz. Ezáltal tud hatékonyan megfelelni az MNB a pénzügyi közvetítőrendszer feletti felügyeletet gyakorló hatósági jogkörében a megelőző (preventív) szerepének, és lehet képes megakadályozni a pénzügyi piacok zavarait.

Az MNB előbbiekben említett célkitűzéseit a Vizsgálat lezárása során a Pénztárral szemben alkalmazandó megfelelő felügyeleti intézkedés, illetve szankció kiválasztása, illetőleg annak szükséges és arányos mértékének a megállapítása során is következetesen érvényre kívánta juttatni. Ennek mérlegelése során a szükséges és arányos jogkövetkezményként a Pénztárral szemben alkalmazott felszólítás intézkedés mellett a határozat indokolásának 1-6. pontjában megállapított jogszabálysértések miatt az MNB a bírságszankció alkalmazását is szükségesnek tartotta. A bírság kiszabásának szükségességéről ezen jogsértések esetében az MNB arra tekintettel döntött, hogy az alkalmazott jogkövetkezménynek egyszerre kell szolgálnia mind az egyedi (speciális), mind az általános (generális) – a többi önkéntes és magánnyugdíjpénztári piaci szereplőre informatív, figyelem felhívó erővel ható – prevenciós célokat. Az MNB megítélése szerint a jogszabályi megfelelésre való felhívás önmagában nem elegendő annak a kívánt joghatásnak az érvényre juttatására, hogy a Pénztárat rábírja a feltárt kockázatok kezelésére, illetve megszüntetésére, egyúttal a határozatban foglaltak határidőben történő, pontos és teljes körű teljesítésére.

2.1.3 A bírság kiszabása során mérlegelt körülmények és a bírság összegének megállapítása

Az MNB tv. 76. § (1) bekezdése alapján a pénztárakkal szemben kiszabható felügyeleti bírság összege százezer forinttól kétmilliárd forintig terjedhet.

Az MNB hangsúlyozza, hogy a bírság összegének meghatározásakor megvizsgálta a jelen határozatban értékelt jogsértések szempontjából releváns valamennyi – többek között az MNB tv. 75. § (4) bekezdésében is nevesített – mérlegelési szempontot, és amelyek megítélése szerint a jelen ügy szempontjából a bírságkiszabás körében enyhítő, vagy súlyosító körülményként értékelhetők, azokat alább részletezi. Tekintettel arra, hogy az MNB tv. 75. § (4) bekezdése nem taxatív felsorolást tartalmaz az MNB által figyelembe vehető körülményekről, tehát az MNB a mérlegelése során olyan szempontokat is értékelés tárgyává tehet, amelyek az adott ügy egyedi sajátosságaiból fakadnak, így az MNB kizárólag a bírságkiszabás során figyelembe vehető és ténylegesen figyelembe vett körülményeket rögzíti.

(i) A jelen határozat 1. pontjában az MNB azt állapította meg, hogy a Pénztár informatikai szabályzatai nehezen áttekinthetőek, illetve bizonyos funkciókat nem szabályoznak, a gyakorlatot nem követik, vagy attól eltérő szabályokat tartalmaznak, továbbá a Pénztár nem az Informatikai szabályzatában rögzíti az egyes munkakörök betöltéséhez szükséges informatikai ismeretek körét. Az MNB a fent leírt körülményeket az MNB tv. 75. § (4) bekezdés a) pontja alapján (a szabályszegés, mulasztás súlyossága) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott – részben már megtett, részben pedig tervezett – intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

(ii) A jelen határozat 2. pontjában az MNB azt állapította meg, hogy a Pénztár működésében az informatikai környezet határvédelmével kapcsolatosan számos hiányosság fedezhető fel (nem különítette el az éles és a teszt környezetet; a Pénztártól eltérő, idegen intézmény szervereit a saját hálózatában működtette, a kimenő adatforgalommal kapcsolatban elmulasztotta a port- és protokollszűrés megtételét, illetve a hitelesítési adatok titkosításának kikényszerítését, illetve a tűzfalszabályokkal kapcsolatban voltak mulasztásai). Az MNB a fent leírt körülményeket az MNB tv. 75. § (4) bekezdés a), b), c), és e) pontja alapján (a szabályszegés, mulasztás súlyossága, a cselekménynek a Pénztár biztonságos működésére gyakorolt hatása, a cselekménynek a Pénztárra és a pénztártagokra gyakorolt hatása, és a szabályszegéssel előidézett kockázatok) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott – részben már megtett, részben pedig tervezett – intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

(iii) A jelen határozat 3. pontjában az MNB azt állapította meg, hogy a Pénztár az adatbázisok kezelésével kapcsolatosan több ponton mulasztást követett el (az adatbáziskezelőkre érvényes egységes hardening szabályozás, az adatbáziskezelő paraméterek, naplózási beállításainak hiányában illetéktelenül végrehajtott események maradhatnak felderítetlenül; továbbá az érvényes adatbázis profil beállítások miatt az azonosítókkal és jelszavakkal való visszaélés kockázata magasabb). Az MNB a fent leírt körülményeket az MNB

tv. 75. § (4) bekezdés a), b), c), és e) pontja alapján (a szabályszegés, mulasztás súlyossága, a cselekménynek a Pénztár biztonságos működésére gyakorolt hatása, a cselekménynek a Pénztárra és a pénztártagokra gyakorolt hatása, és a szabályszegéssel előidézett kockázatok) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott – részben már megtett, részben folyamatban lévő, részben pedig tervezett – intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

(iv) A jelen határozat 4. pontjában az MNB azt állapította meg, hogy a Pénztár informatikai biztonsági rendszereinek önvédelme nem megfelelő (teljeskörű biztonsági tesztelésének rendszeres végrehajtása hiányzik, alkalmazásbeli sérülékenységek maradhatnak felfedezetlenül, illetve javítatlanul; emiatt előfordulhat, hogy egy támadó a sérülékenység kihasználásával illetéktelenül férhet hozzá ügyfelek adataihoz; a Pénztár nem tudja a kockázatokkal arányosan kezelni az informatikai rendszereinek kitettségét a kártékonykód és egyéb biztonsági fenyegetettségekkel szemben). Az MNB a fent leírt körülményeket az MNB tv. 75. § (4) bekezdés a), b), c), és e) pontja alapján (a szabályszegés, mulasztás súlyossága, a cselekménynek a Pénztár biztonságos működésére gyakorolt hatása, a cselekménynek a Pénztárra és a pénztártagokra gyakorolt hatása, és a szabályszegéssel előidézett kockázatok) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott megtett intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

(v) A jelen határozat 5. pontjában az MNB azt állapította meg, hogy a felhasználói jogosultságok kezelése a Pénztár részéről nem megfelelő (fennáll az adatokhoz való illetéktelen hozzáférés és a csalás, illetve az adatok engedély nélküli módosításának kockázata; a technikai azonosítók jelszavainak nem dokumentált felvétele megnehezíti a jelszóval való esetleges visszaélés kivizsgálását). Az MNB a fent leírt körülményeket az MNB tv. 75. § (4) bekezdés a), b), c), és e) pontja alapján (a szabályszegés, mulasztás súlyossága, a cselekménynek a Pénztár biztonságos működésére gyakorolt hatása, a cselekménynek a Pénztárra és a pénztártagokra gyakorolt hatása, és a szabályszegéssel előidézett kockázatok) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott megtett intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

(vi) A jelen határozat 6. pontjában az MNB azt állapította meg, hogy a naplózással kapcsolatosan számos hiányosság fedezhető fel (a biztonsági naplózás, a biztonsági naplógyűjtés és naplóelemzés nem megfelelően szabályozott; ennek következtében és az IT infrastruktúra elemek, a kapcsolódó alkalmazás- és adatbázis megfelelő naplózása és naplóiknak központi gyűjtése hiányában a központi érdemi naplóelemzés teljessége nem biztosítható; ezáltal egy esetleges biztonsági incidens feltárásához szükséges események és összefüggések elemzése nem biztosítható egyértelműen; az egyes biztonsági incidensek, valamint rendszerhibák észlelése időben elhúzódhat, mely biztonsági kockázatot növelő tényező). Az MNB a fent leírt körülményeket az MNB tv. 75. § (4) bekezdés a), b), c), és e) pontja alapján (a szabályszegés, mulasztás súlyossága, a cselekménynek a Pénztár biztonságos működésére gyakorolt hatása, a cselekménynek a Pénztárra és a pénztártagokra gyakorolt hatása, és a szabályszegéssel előidézett kockázatok) súlyosító körülményként vette figyelembe. Az MNB a Pénztár által az Észrevételekben bemutatott tervezett intézkedéseket az MNB tv. 75. § (4) bekezdés f) pontja alapján (MNB-vel kapcsolatban tanúsított együttműködés) enyhítő körülményként értékelte.

A Pénztár vagyona 2020. június 30-án elérte a 114,4 Milliárd Ft-ot; taglétszáma pedig 34.067 fő volt.
A Pénztár vagyona alapján piaci részesedése a 2020. év második negyedévére vetítve mintegy 7,68 %-os; míg a taglétszám alapján mintegy 3,07 %-os.
Annak érdekében, hogy az intézkedés a speciális prevenciós hatását elérje, a bírság összegének megállapítása során az MNB figyelembe vette azt is, hogy a Pénztár működési eredménye 2020. év második negyedévében 217,6 millió Ft volt, illetve, hogy a Pénztár működési és likvidítási tartaléka (vagyis a működés céljára felhasználható tartalékok) együttes összege 2020. június 30-án 2.098,5 millió Ft volt.

A fentiek alapján a Pénztár erős hatású piaci szereplőnek minősül, amit az MNB tv. 75. (4) bekezdés b) pontja alapján értékelt a bírság összegének meghatározása során.

Az MNB enyhítő körülményként értékelte, hogy a megállapított jogszabálysértéseknek nincs negatív hatása a pénzügyi intézményrendszer tagjaira (MNB tv. 75. § (4) bekezdés d) pont), továbbá azt is, hogy a Pénztár az Észrevételekben több esetben a jogszabálysértés megszüntetéséről, illetve jövőbeli orvoslásáról számolt be (MNB tv. 75. § (4) bekezdés f) pont).

A fentiek alapján a határozat indokolásának 1-6. pontjaiban foglalt jogszabálysértésekre tekintettel kiszabott bírság összegét az MNB – figyelemmel az MNB tv. 76. § (1) bekezdésében rögzített, százezer forinttól kétmilliárd forintig terjedő bírságkeretre, és tekintettel az MNB tv. 75. § (4) bekezdésében foglalt mérlegelési szempontok fentiek szerinti értékelésére – a jelen határozat rendelkező részének 7. pontjában írt összegben állapította meg. Ezen összegű felügyeleti bírság kiszabásával látta elérhetőnek azt a jogalkalmazói célt, hogy a Pénztárt a jövőre nézve visszatartsa a hasonló típusú jogsértések megvalósításától, továbbá ösztönözze a Pénztárt a jogszabálysértést megvalósító körülményei megváltoztatására. Ezen bírságösszeg kiszabását tartotta továbbá alkalmasnak az MNB arra, hogy a többi piaci szereplő számára jelezze azt, hogy az MNB a jelen határozatban feltárt jogsértések elkövetését – figyelembe véve a fent kifejtett súlyosító és enyhítő körülményeket – megfelelő nyomatékú felügyeleti bírság kiszabásával szankcionálja.

3. Tájékoztatás (8. pont)

A jelen határozat rendelkező részében előírt tájékoztatás a Pénztár jogi és ténybeli helyzete tekintetében elsőrendű fontosságú, hiszen a megfelelő tájékoztatás hiányában a Pénztár Igazgatótanácsa és Ellenőrző Bizottsága, illetve a küldöttközgyűlés az Öpt.-ben meghatározott jogköreit nem tudná teljességében gyakorolni, és ez sértené a pénztártagok jogait. A Pénztár Igazgatótanácsa, illetve az Ellenőrző Bizottsága tagjainak feladatait és hatáskörét az Öpt. 24–27. §-ai egyetemleges felelősségüket feladatkörükben kötelezettségeik megszegésével okozott kárért az Öpt. 20. §-a rögzíti.

***

A határozat a már hivatkozott jogszabályhelyeken, valamint az MNB tv. 49/C. § (1)-(2) bekezdésén alapul.

A határozat meghozatalára az MNB nevében, az MNB tv. 4. § (9) bekezdésében és 39. § (1) bekezdés a) pontjában biztosított hatáskörben, az MNB tv. 13. § (1) bekezdésére és a (11) bekezdés a) pontjára figyelemmel, a Magyar Nemzeti Bank egyes hatósági döntéseivel kapcsolatos hatáskörgyakorlás, valamint a hatáskör gyakorlója helyettesítésének részletes szabályairól szóló 45/2019 (XII. 18.) MNB rendelet (MNB rendelet) 2. § (9) bekezdése, továbbá helyettesítés esetén a 7. § (1) bekezdés c) pontja, illetve (2) bekezdése alapján került sor. A határozat aláírására az MNB rendelet 5. §-ában foglaltak alapján került sor.

A határozat elleni jogorvoslatról szóló tájékoztatás az MNB tv. 46. § (2) bekezdés 18. pontján, az Ákr. 112. §-án, a 113. § (1) bekezdés a) pontján, a 114. § (1) bekezdésén, a közigazgatási perrendtartásról szóló 2017. évi I. törvény 13. § (3) bekezdés ad) pontján, a 17. §-án, a 27. § (1) bekezdésén, a 29. § (1) bekezdésén, a 39. § (1) és (6) bekezdésein, az 50. § (1) bekezdésén, a 77. § (1)-(2) bekezdésén, a polgári perrendtartásról szóló 2016. évi CXXX. törvény 608. § (1) bekezdésén, valamint az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 9. § (1) bekezdés a), illetve b) pontján alapul.

Az MNB tv. 77. § (1) bekezdése szerint a bírságot a kiszabásáról hozott döntés jogerőre emelkedésétől számított harminc napon belül kell a döntésben megjelölt számlára befizetni.

A késedelmi pótlék MNB általi felszámításának lehetőségét az MNB tv. 55/A. §-a alapján az Ákr. 135. §-a biztosítja. Az MNB által kiszabott bírságnak az állami adóhatóság útján történő foganatosításának lehetősége az Ákr. 134. § (1) bekezdésén alapul.

A határozat az MNB tv. 49/C. § (7) bekezdése alapján alkalmazandó Ákr. 82. § (1) bekezdése értelmében annak közlésével végleges.

Budapest, 2020. szeptember 14.

A Magyar Nemzeti Bank nevében eljáró
Nagy Koppány
igazgató
Biztosítás-, pénztár- és közvetítők felügyeleti igazgatóság
ELEKTRONIKUSAN ALÁÍRT IRAT