PRAUDIT

INFORMATIKAI BIZTONSÁGI MEGÁLLAPÍTÁSOK A MAGYAR NEMZETI BANK 2018/2019. ÉVI HATÁROZATAI TEKINTETÉBEN

PR-AUDIT KFT.

TARTALOMJEGYZÉK

CÉLKITŰZÉSEK

A Magyar Nemzeti Bank (a továbbiakban: MNB) a jegybanktörvény alapján folyamatos felügyeletet gyakorol a pénzügyi ágazati törvények hatálya alá tartozó szervezetek és személyek felett. Az MNB felügyeleti tevékenységének része az ellenőrzési eljárás, melyet egyrészt az adatszolgáltatásból származó adatok, másrészt a részére átadott dokumentumok, információk, illetve a hivatalosan ismert információk ellenőrzésével és elemzésével valósít meg. A vizsgálatok gyakoriságát törvényi előírások határozzák meg: banknál, szakosított hitelintézetnél, biztosítónál, viszontbiztosítónál, befektetési vállalkozásnál, alapkezelőnél – kivéve kockázati-tőkealap kezelők –, elektronikuspénz-kibocsátó intézménynél, pénzforgalmi intézménynél legalább három évente, pénztárnál, illetve kisbiztosítónál legalább öt évente kell helyszíni vizsgálatot lefolytatni.[1]

Jelen dokumentum célja az MNB ellenőrzési eljárásainak megállapításai alapján hozott határozatok áttekintése és összefoglalása, így segítségével átfogó kép alkotható, mely

- segíti megérteni az MNB joggyakorlatát, ellenőrzési metodikáját és súlypontjait,
- segíti az informatikai szakembereket (piaci szereplőket) az MNB ajánlások értelmezésében,
- segítséget nyújt az MNB ellenőrzésre való felkészülésben, az MNB ellenőrzésnek való megfelelés elérésében,
- segítségül szolgál az üzleti (beszerzési) döntések meghozatalában.

Jelen dokumentum elkészítése során a vizsgált időszakba eső MNB határozatok informatika és információbiztonság területével összefüggő megállapításai kerültek összegyűjtésre az alkalmazott módszertannak megfelelő módon.

[1] https://www.mnb.hu/felugyelet/felugyeleti-keretrendszer/ellenorzesi-terv-es-jelentes

RÖVID CÉGBEMUTATÓ

A PR-AUDIT Professzionális Informatikai Audit Kft. (a továbbiakban: PR-Audit) a hazai információbiztonsági piac megkerülhetetlen szereplője 2003 óta. A magyar tulajdonú kis-és középvállalkozás az információbiztonság különböző területein bír jelentős kompetenciával.

IT BIZTONSÁGI TANÁCSADÁS

Cégünk hosszú évek óta végez főként a pénzügyi szervezetek részére információbiztonsági, informatikai átvilágításokat és célauditokat, IT biztonsági kockázatelemzéseket és alakít ki átfogó szabályozó környezetet. Több szervezetnél kiszervezés keretében töltünk be információ biztonsági felelősi pozíciót, ahol mind a kialakítás, mind az ellenőrzés oldaláról látjuk az információbiztonság megfelelőség kérdéseit. Tanácsadási szolgáltatásunk keretében több helyen alakítottunk ki teljes üzletmenet-folytonossági keretrendszereket, melyet 2011-től saját fejlesztésű szoftveres támogatással (PCP alkalmazás) tettünk még teljesebbé. 2008 óta rendelkezünk ISO 27001 tanúsítvánnyal, amelyet évről évre sikerrel megújítunk. Ezen tapasztalatunkat és tudásunkat felhasználva több ügyfelünket készítettünk fel a tanúsítvány megszerzésére és a biztonsági keretrendszer későbbi folyamatos működtetésére.

TECHNOLÓGIAI VIZSGÁLATOK

Etikus hacker csapatunk évente számos betörési tesztet, sérülékenységi vizsgálatot, alkalmazásbiztonsági auditot és forráskód elemzést végez. Ügyfeleink a kis cégektől a nagy multinacionális cégekig minden szegmensből hosszú évek óta visszatérő partnereink. Sikerünk titka, hogy az esetleges hiányosságok széles körű feltárásán túl javaslataink megfelelő támogatást jelentenek a hibák kijavítása során.

A mély technológiai vizsgálatok terén szerzett felkészültségünket és tapasztalatunkat jelzi, 2010 szeptemberében cégünk csapata nyerte meg a Hacktivity CTF versenyét, ezzel elnyerve az év legjobb hackercége díjat, melyet 2011. évben sikeresen megvédett. 2012-ben a PRAUDITORS az EC-Council szervezésében megrendezésre kerülő CyberLympics 2012 Hacker Olimpiának számító európai versenyen európai első helyezést, az ezt követő világversenyen hatodik helyezést ért el, 2013-ban pedig európai bronzérmes lett. Szakály Tamás kollégánk 2015-ben, 2016-ban és 2018-ban is előadóként vett részt a DefCon-n, a világ legszakmaibb hacker konferenciáján.

SAJÁT FEJLESZTÉSŰ ALKALMAZÁSAINK

LOGNESS

LOGNESS all-in-one megoldásként megvalósítja a naplóállományok gyűjtését, feldolgozását és azok értékelését. PR-AUDIT az elmúlt évek sikerprojektjeinek tapasztalatait integrálta SIEM platformjába, mely know-how a magyar piacon egyedülálló és évek óta sikerrel alkalmazott naplóelemzési szolgáltatáson alapul. Az új generációs LOGNESS Boxer termékünk bevezetése 10 lépésben végrehajtható, így a naplóállományok érdemi elemzése

bármilyen képzettséggel és információbiztonságitapasztalattal rendelkező felhasználó számára akár órákon belül megkezdhető.

A PR-AUDIT 2008 óta folyamatosan foglalkozik naplóelemzéssel, melynek első sikerköve a 2010 márciusában Budapesten megrendezett az informatikai audit és biztonság területén a világ vezető konferenciájának számító EuroCACS volt, ahol hazánkat előadóként a PR-AUDIT képviselte.
Az előadás témája a központosított naplógyűjtés- és naplóelemzés volt. A 2010-2011. évben végrehajtott integrált naplógyűjtési- és naplóelemzési projektjével cégünk elnyerte az ITBN Biztonsági Díj 2011 - Legjobb IT Biztonsági referencia projekt díját, mely a termék és a kapcsolódó szolgáltatások legkiemelkedőbb szakmai elismerése. Jelen pillanatban a LOGNESS a magyar biztosítási szektor szereplőinek 80%-ánál végzi a naplógyűjtést- és elemzést.

PRAUDIT Continuity Planner (PCP)

PCP üzletmenet-folytonosságot támogató alkalmazás támogatja a szervezet folyamatainak felmérését és átfogó üzleti hatáselemzésen (BIA) alapuló értékelését, illetve lehetőséget biztosít továbbá a folyamatokhoz tartozó adatkörök azonosítására és osztályozására, valamint a teljes adatvagyon felmérésére. Az alkalmazás segítségével mód van a különböző fenyegető tényezők és sebezhetőségek azonosítására, a működési kockázatok több szempont figyelembevételével történő elemzésére és a kapcsolódó folytonossági tervek (BCP) elkészítésére. PCP támogatja továbbá a 2013. évi L. törvény (Ibtv.) által előírt osztályba sorolás és kockázatelemzés végrehajtását, a besoroláshoz szükséges felmérések gyors, hatékony és érdemi elvégzését és karbantartását.

JOGI NYILATKOZAT

Jelen dokumentumban foglaltak tájékoztató jellegű megállapítások, a szerzők és szerkesztők nézőpontjait, értelmezéseit tükrözik és nem vonatkoznak semmilyen konkrét szervezet, vagy egyén körülményeire. Jelen dokumentum törekszik a pontos és naprakész tájékoztatásra, azonban nem biztosítható, hogy az adott tájékoztatás a dokumentum megtekintésekor, vagy a jövőben is pontos információkat tartalmaz, a jövőben a dokumentum időnként módosításra kerülhet. A PR-AUDIT nem vállal felelősséget a közölt információk hatályosságáért, valamint az olyan tevékenységből eredő károkért, amelyek az itt közölt információk felhasználásából erednek az adott esetet érintő átfogó vizsgálatunk és szaktanácsadásunk hiányában. A PR-AUDIT nem felelős a jelen dokumentumban megjelölt külső források tartalmáért. A harmadik fél forrásai megfelelően kerültek idézésre.

ALKALMAZOTT MÓDSZERTAN

Az MNB határozatainak áttekintésére, elemzésére az MNB határozatok keresésére kialakított felület[2] útján került sor, mely felületen az MNB döntéseit többféle szempont – időszak, ágazatok (pénzpiac, biztosítási piac, tőkepiac, pénztár), típus (engedélyezési, jogérvényesítési, piacfelügyeleti, fogyasztóvédelmi) – szerint is lehet keresni. **A határozatok nyilvánosak, a jelen dokumentumban összefoglaló bemutatásuk anonim módon történik.**

A vizsgált időszakba eső felügyeleti határozatok közül az informatika és információbiztonság területét érintő megállapításokat tartalmazó határozatok elemzésére került sor. A vizsgálat során a határozatok informatika és információbiztonság területével összefüggő megállapításaiból származó információk csoportosításra kerültek. A csoportosítás során, a könnyebb áttekinthetőség érdekében, ahol lehetséges összevonásra kerültek az egyes eltérő MNB határozatok hasonló megállapításai figyelemmel az egyazon MNB határozatban foglalt megállapítások kohéziójára.

Ennek megfelelően a megállapítások téma szerinti csoportosításai címek és alcímek szerint a következők:

I. Adatvagyon
   I.1. Adatvédelem
   I.2. Adatok, rendszerek biztonsági osztályba sorolása
II. Kártékonykód elleni védelem
III. Határvédelem
IV. Naplózás
V. Jogosultság-menedzsment
   V.1. Szabályozás
   V.2. Felhasználói jogosultságok
   V.3. Kiemelt jogosultságok
   V.4. Összeférhetetlenségek kezelése
   V.5. Jogosultságnyilvántartás
   V.6. Egyéb
VI. Mentések kezelése
VII. Üzletmenet-folytonosság
VIII. Biztonsági kockázatelemzés
IX. Jelszókezelés
X. Tevékenység kiszervezése
XI. Nyilvántartások
XII. Szabályozás
XIII. Ellenőrzés
XIV. Fejlesztés, változáskezelés

[2] http://alk.mnb.hu/bal_menu/hatarozatok/hatarozatok_keresese

Szem előtt tartva a vizsgálati eredmények átláthatóságát és a vizsgálat célelvű megközelítését, kizárólag az önállóan értelmezhető és információt hordozó megállapítások kerültek külön megjelenítésre. Az MNB a részletes vizsgálati jelentéseket, a határozatok és javaslatok indoklásait nem hozza nyilvánosságra, így sok esetben a hiányosság önmagában nem értelmezhető, vagy túl általános jelen dokumentumba történő foglaláshoz.

Kiemeljük, hogy a téma szerinti csoportosítás során az összevonás alapját a megállapítások témaköre képezte, így elképzelhető, hogy egyes megállapítások a határozatban foglaltaknál tágabb körbe kerültek, azonban az összevonások, csoportosítások a határozatban foglalt minimum követelmények megtartásával történtek.

Megjegyzendő, hogy tekintettel a határozatokban foglalt bírságok fejezetekre osztottságára, ahol a kiszabott bírság több fejezetet is átölelhet, nincs lehetőség minden határozat tekintetében az informatikai és információbiztonsági területre vonatkozó megállapítások bírság mértékének pontos kiszámolására. Jelen dokumentum tekintetében a 2017. évi vizsgált határozatok a 2018. év megállapításainak részét képezik.

VEZETŐI ÖSSZEFOGLALÓ

1. VIZSGÁLT IDŐSZAK

Jelen dokumentum a 2017. november 21. – 2019. december 14. közötti időtartamban hozott határozatok elemzésére terjed ki.

Vizsgált időszakba eső határozatok száma: 2017 – 3 határozat; 2018 – 16 határozat; 2019 - 19 határozat. Jelen dokumentum tekintetében a 2017. évi vizsgált határozatok a 2018. év megállapításainak részét képezik.

2. VIZSGÁLAT HELYSZÍNE

A vizsgálat során az információk feldolgozása, értékelése, valamint a vizsgálati összefoglaló dokumentum elkészítése a PR-AUDIT Kft. székhelyén - 1145 Budapest Szenttamás utca 4. - történt.

3. A VIZSGÁLAT SORÁN ÁTTEKINTETT DOKUMENTUMOK

A vizsgálat során az MNB határozatainak áttekintésére, elemzésére az MNB határozatok keresésére kialakított felület[3] útján került sor, mely felületen az MNB döntéseit többféle szempont – időszak, ágazatok (pénzpiac, biztosítási piac, tőkepiac, pénztár), típus (engedélyezési, jogérvényesítési, piacfelügyeleti, fogyasztóvédelmi) – szerint is lehet keresni. A határozatok nyilvánosak, a jelen dokumentumban összefoglaló bemutatásuk anonim módon történik.

A vizsgált időszakba eső felügyeleti határozatok közül az informatika és információbiztonság területét érintő megállapításokat tartalmazó határozatok elemzésére került sor a jelen dokumentumban meghatározott módszertannak megfelelően. A vizsgálat során a határozatok informatika és információbiztonság területével összefüggő megállapításaiból származó információk csoportosításra kerültek. A csoportosítás során, a könnyebb áttekinthetőség érdekében, ahol lehetséges összevonásra kerültek az egyes eltérő MNB határozatok hasonló megállapításai figyelemmel az egyazon MNB határozatban foglalt megállapítások kohéziójára.

[3] http://alk.mnb.hu/bal_menu/hatarozatok/hatarozatok_keresese

4. JOGI KÖRNYEZET

Az MNB mindenkori honlapján közzéteszi azon magyar és európai jogszabályok listáját, amelyek érintik az általa felügyelt intézmények tevékenységét és szolgáltatások végzését, valamint a felügyeleti érdekkörébe tartozó jogszabályok esetében az alkalmazandó hatályos jogi normák szövegének elérhetőségét is biztosítja. Ilyen jogszabályok lehetnek MNB rendeletek, egyéb magyar jogszabályok (törvények, kormányrendeletek, pénzügyminiszteri / nemzetgazdasági miniszteri rendeletek, gazdasági miniszteri rendelet, kormányhatározatok), valamint Európai szintű jogszabályok.

Az MNB által felügyelt hitelintézeti, biztosítási, pénztári és tőkepiaci szektorok tevékenységét érintő jogszabályokon túl szükség van olyan felügyeleti eszközökre is, amelyek a felügyelt intézményeket segítik, orientálják a jogszabályok felügyeleti értelmezésével, betartásával kapcsolatban, leírják a jegybank konkrét elvárásait, illetve egyes kiemelt kérdéskörökben tájékoztatják az összes piaci szereplőt, érdeklődőt. A felügyeleti szabályozó eszközök nem jogi kötelmen alapulnak, azok betartása nem kényszeríthető ki, de alkalmazásukat az MNB vizsgálja és értékeli.

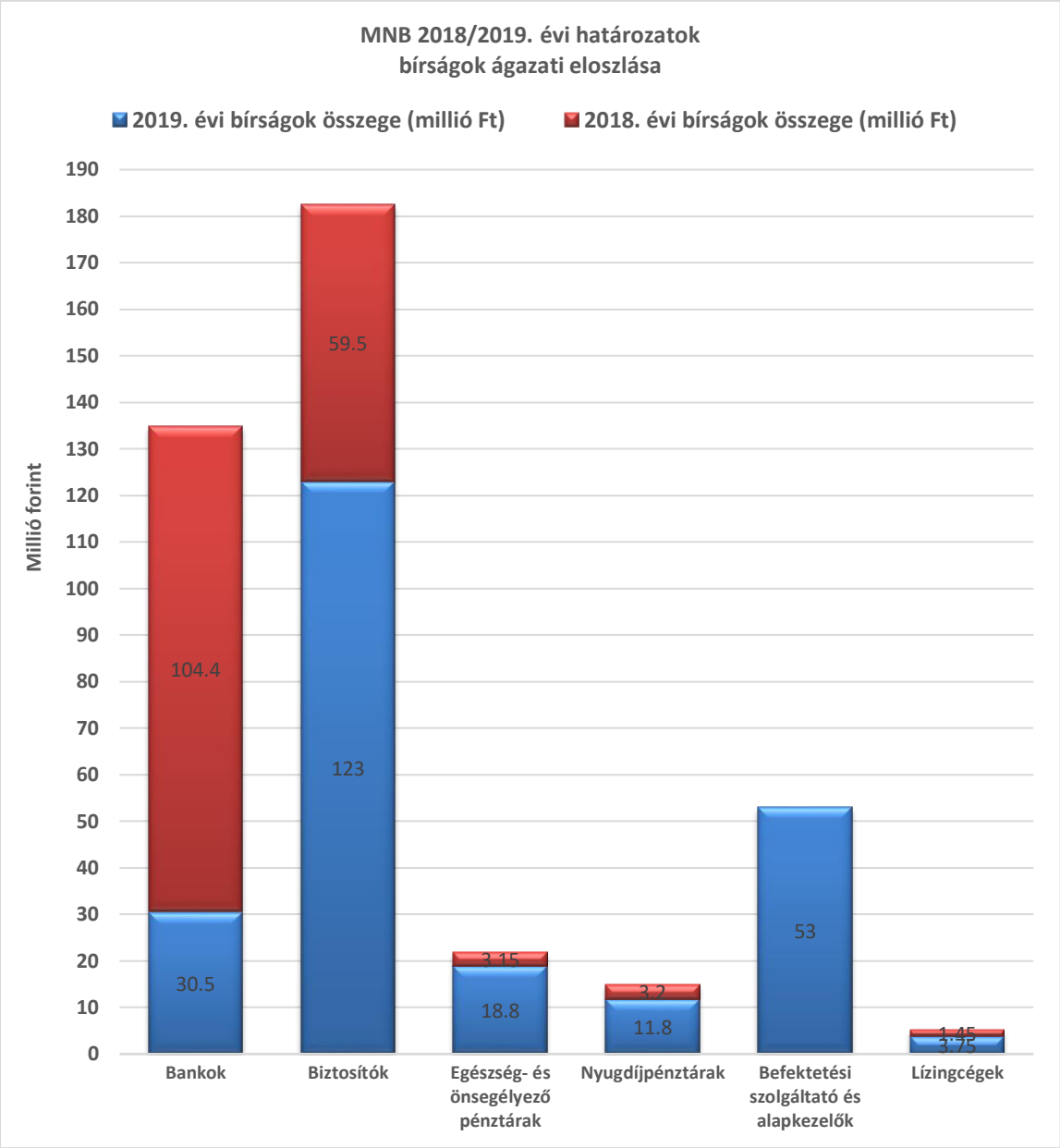
A vizsgálat témáját érintően két szabályozó kiemelendő:

- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről,
- 7/2017 (VII. 5.) MNB ajánlás az informatikai rendszer védelméről.

5. A HATÁROZATOK ÁTTEKINTÉSE

Jelen dokumentum elkészítése érdekében a vizsgált időszak alá tartozó 38 MNB határozat elemzésére került sor. A határozatokkal érintett szervezetek között megtalálhatók bankok (9), biztosítók (7), nyugdíjpénztárak (8), egészség és önsegélyező pénztárak (7), befektetési szolgáltató(k) (1) és alapkezelők (3), valamint lízingcégek (2). **A vizsgált időszakba eső határozatokban foglalt bírságok összege meghaladja a 410.000.000,- Ft-ot** (azaz négyszáztízmillió forintot), azonban az említett összeg mellett szükséges figyelembe venni a bírságok mértékével kapcsolatosan tett fenntartásokat.

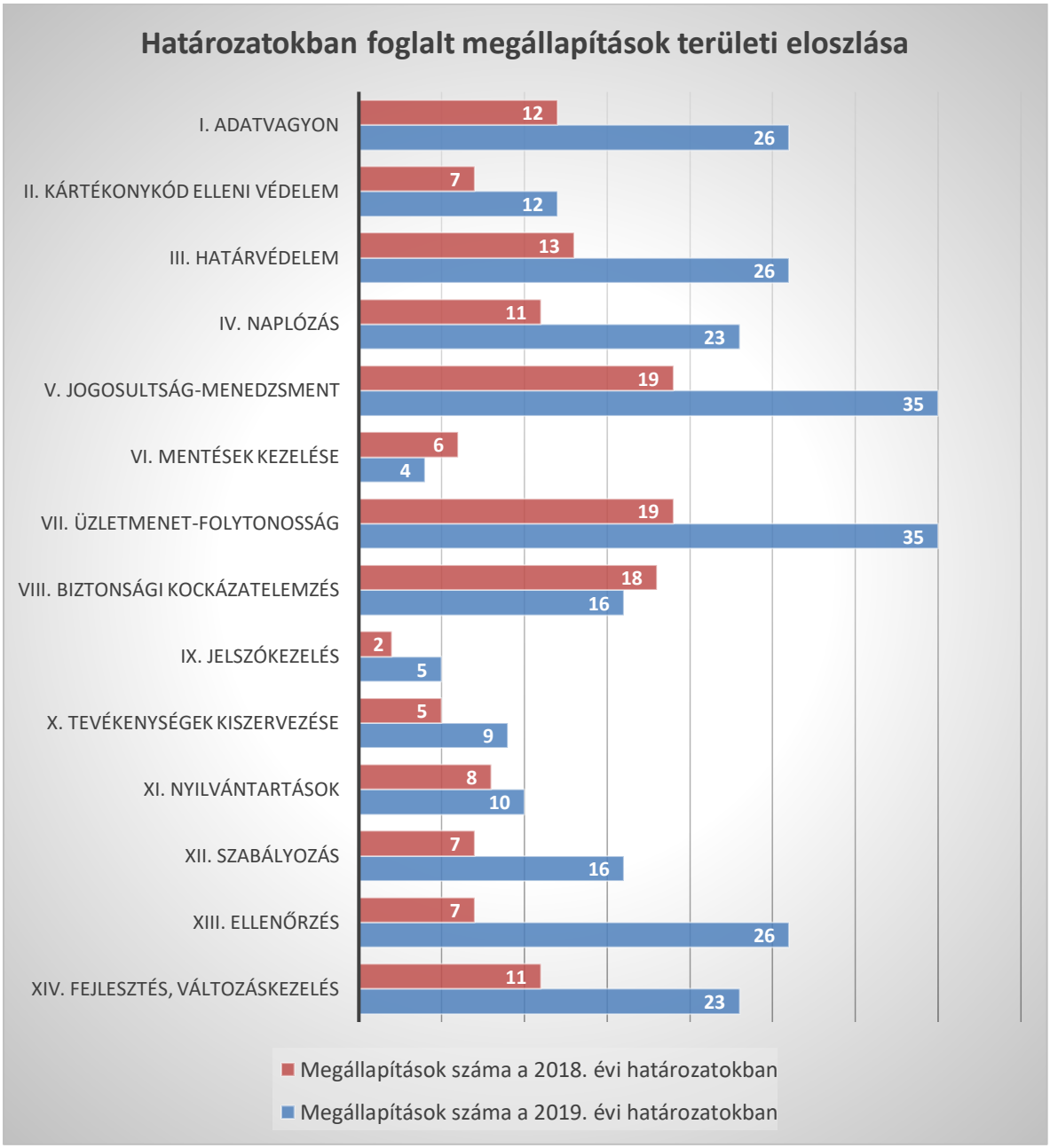
A bírságok tekintetében kiemeljük, hogy az MNB jogalkalmazói gyakorlatából kifolyólag nem állapítható meg, hogy a kiszabott bírság mértékének meghatározása során milyen súllyal kerültek az egyes szakterületek és megállapítások figyelembevételre.



Fontos megjegyezni, hogy ugyan a jelen dokumentumban foglalt megállapítások, a levont következtetések, azok összefoglalása az érintett ellenőrzési területek súlypontjait emelik ki és nyújtanak áttekintést, azonban minden esetben kizárólag az irányadó szabályozóknak való teljeskörű megfelelés várható el a szervezet részéről a felügyeleti ellenőrzésnek való megfelelés érdekében.

Az MNB vizsgált időszakra eső határozatainak egységes összefoglalásával és megfelelő következtetések levonásával, megérthető a szervezetek számára, hogy melyek azok az informatikával és információbiztonsággal kapcsolatos területek, amelyekre különös figyelmet érdemes fordítani, egyúttal látható, hogy milyen mértékű bírsággal fenyeget az egyes területek felkészületlensége.

A vizsgált időszak határozataiban foglalt valamennyi megállapítás jelen dokumentum módszertana szerinti területi eloszlásának alakulását az alábbi diagramm mutatja be. A felügyelet jelen dokumentum tárgyát képező 2018. évi, vizsgált határozatainak száma 16, míg a 2019. évi, vizsgált határozatok száma 18.



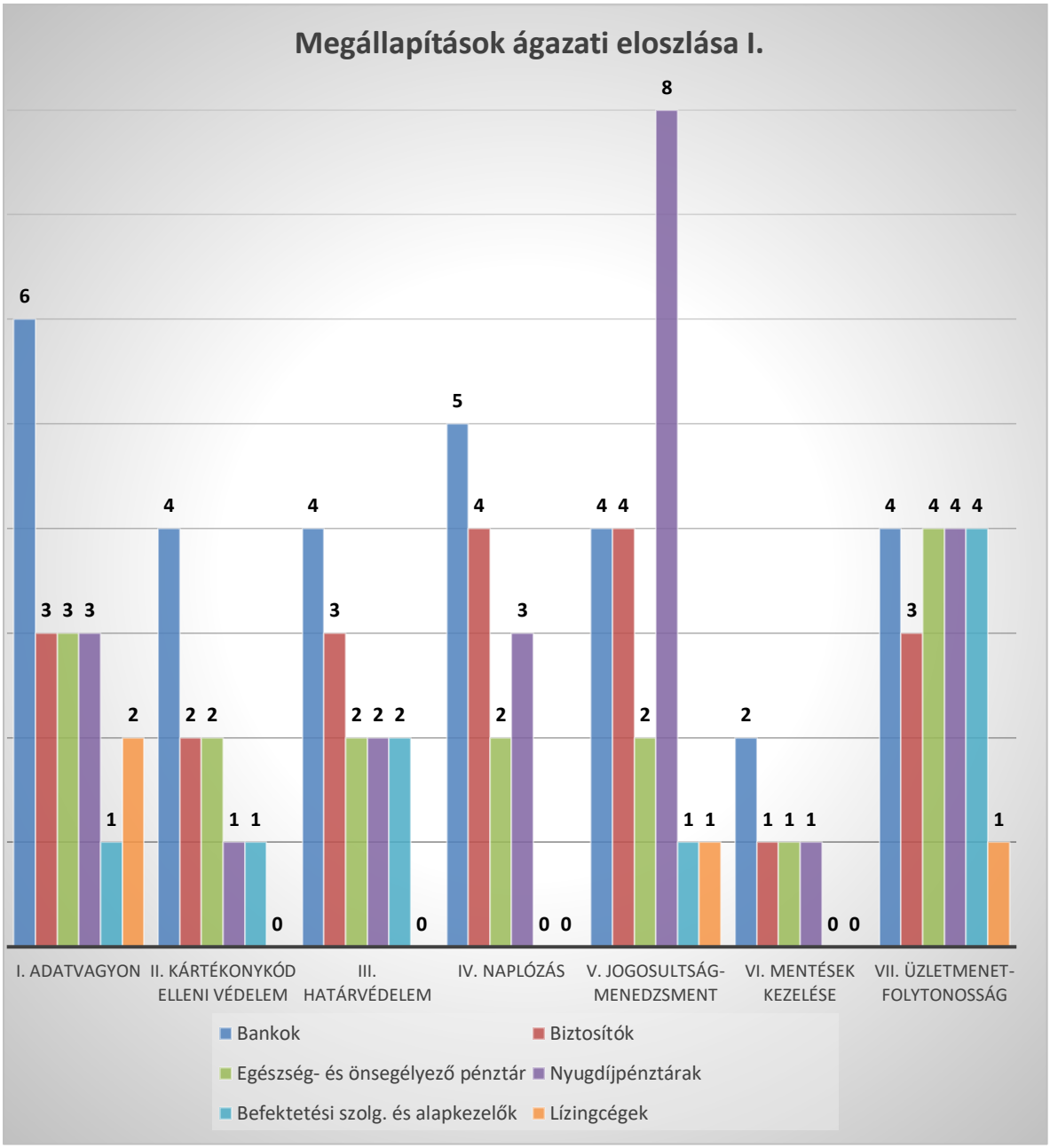
Figyelembe véve a fenti ábra adatait és annak tényét, hogy a felügyelet 2018. évben és a 2019. évben is közel azonos számú határozatot hozott, megállapítható, hogy változatlan felügyeleti aktivitás mellett a megállapítások száma jelentősen megnövekedett egyes területeken.

A felügyelet vizsgálati megállapításai 2018. évben leginkább a jogosultság-menedzsment, üzletmenet-folytonosság és biztonsági kockázatelemzés területeit érintették.

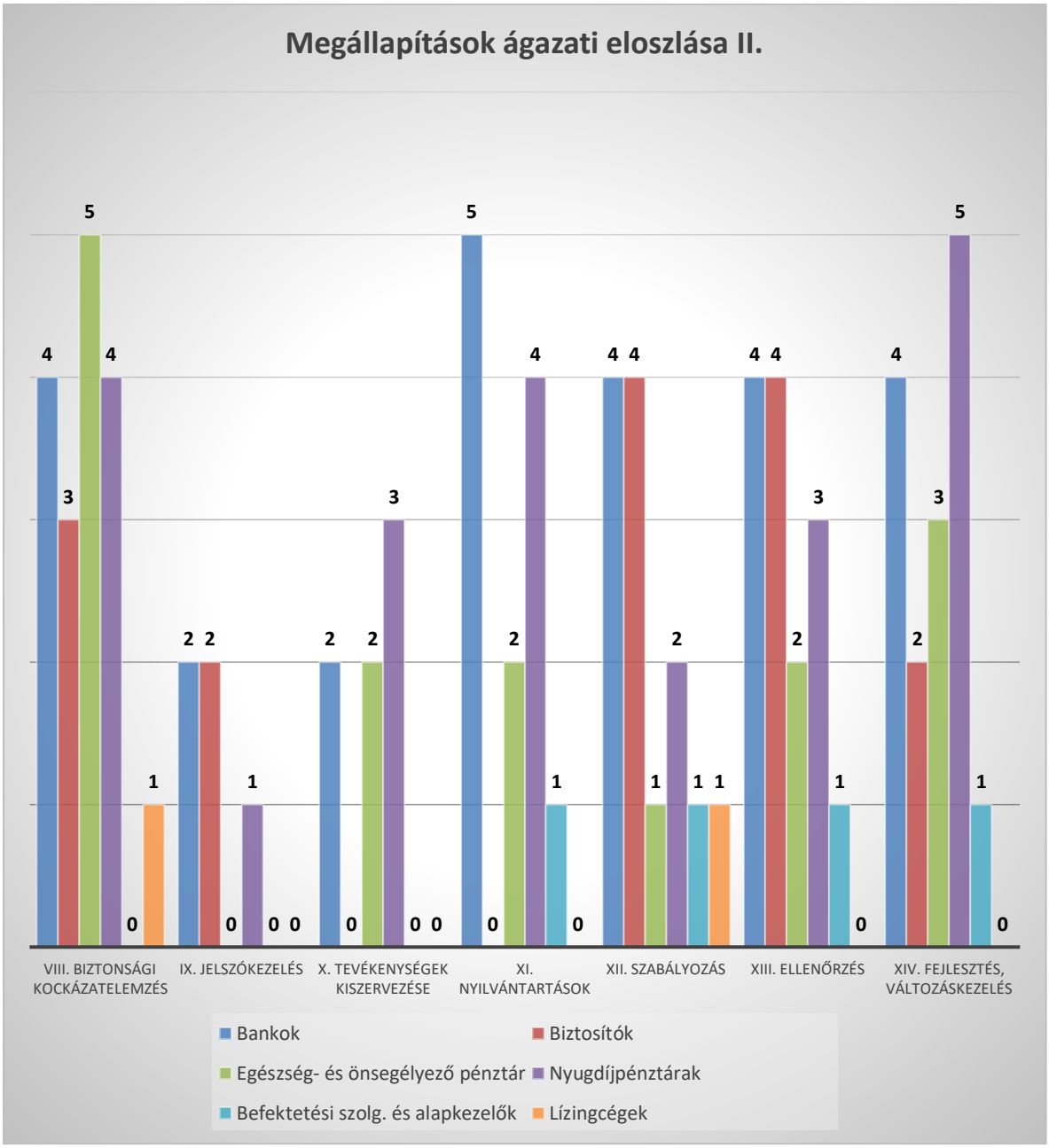
Látható, hogy a 2018. évben kiemelt területek mellett 2019. évben megnövekedett az adatvagyonnal, határvédelemmel, ellenőrzéssel, fejlesztés és változáskezeléssel kapcsolatos megállapítások száma, azzal, hogy továbbra is a jogosultság-menedzsment és az üzletmenet-folytonosság maradtak a vizsgálat során kiemelt figyelemben részesülő területek.

Átlátva a felügyelet 2018. és 2019. évi határozataiban foglalt megállapításainak számát és a módszertanban foglalt tárgykörök szerinti eloszlását, valamint a kiszabott bírság mértékét, érdemes összegezni, hogy a megállapítások milyen mértékben érintik az egyes ágazatokat. A megállapítások ágazati bontásának célja, hogy az egyes ágazatok számára látható legyen, hogy a felügyelet 2018. és 2019. évben informatikai és információbiztonsági területén tett megállapításai mely területeket érintették leginkább az adott szervezet esetében.

A területek sokféleségére tekintettel, két ábrán szemléltethető, hogy a határozatokban foglalt - módszertan szerinti I.- VII. területekre vonatkozó - megállapítások, mely szektorokat és milyen mértékben érintik.



Az alábbi ábra szemlélteti, hogy a határozatokban foglalt - módszertan szerinti VIII. - XIV. területekre vonatkozó - megállapítások, mely szektorokat és milyen mértékben érintik.



Célunk, hogy követve az MNB határozatait, évente hasonló tárgyú és tartalmú kiadvány elkészítésével támogassuk ügyfeleit, a pénzügyi piac szereplőit és az információbiztonság területén dolgozó szakembereket. **Céljainkkal összhangban kiemeljük, hogy az MNB 2020. évi prudenciális ellenőrzési terve szerint az MNB 2020-ban a teljes pénzügyi szektorra vonatkozó prioritása az elavult IT rendszerek kiemelt vizsgálata.4**

[4] https://www.mnb.hu/letoltes/2020-evi-prudencialis-ellenorzesi-terv-web.docx

RÉSZLETES MEGÁLLAPÍTÁSOK

Jelen fejezetben kerülnek összefoglalásra a módszertannak megfelelő téma szerinti csoportosításban az egyes megállapítások, valamint levonásra kerülnek a releváns következtetések a megállapításokból azok előfordulásának gyakoriságától és pénzügyi ágazati érintettségétől függően.

TOP MEGÁLLAPÍTÁSOK

Jelen fejezetben kiemeljük azon megállapításokat, melyek a vizsgált időszakban a legtöbbször szerepeltek a vizsgált MNB határozatokban. A lista gyors áttekintetést ad azon követelményekről melyeknek történő részleges megfelelés, minden kétséget kizáróan, megállapítást eredményez egy MNB vizsgálat során.

A teljes körű, így álláspontunk szerint az igazán érdekes, sokszor egyedi, a vizsgálatot végző auditor egyéni megközelítését is tükröző megállapítások listáját jelen fejezet „Megállapítások tételes felsorolása” pontja tartalmazza.

Megállapítás	Előfordulás a vizsgált időszakban
I. Adatvagyon	
I.1. Adatvédelem	
Végezze el a nem éles (vagy nem az élesnek megfelelően kontrollált) környezetekben a védendő információk anonimizálását, ezáltal biztosítva, hogy a felhasználók kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhessenek a védendő információkhoz.	4
I.2. Adatok, rendszerek biztonsági osztályba sorolása	
Dolgozza ki az adatosztályozás rendjét, határozza meg az adatosztályokhoz tartozó védelmi elveket és intézkedéseket	6
Mérje fel és osztályozza adatvagyonát. Alakítsa ki az adatvagyon elemek nyilvántartását, rendszeresen végezze el az adatok szabályzat szerinti, dokumentált biztonsági osztályba sorolását. Következetesen sorolja biztonsági osztályba a személyes adatokat is tartalmazó rendszereket.	9
III. Határvédelem	
Vizsgálja felül a tűzfalszabály kezelési-, felülvizsgálati-, és nyilvántartási eljárásait, gyakorlatát, a kockázatokkal arányosan gondoskodjon olyan szabályozásról és folyamatokról, melyek biztosítják a tűzfalszabályok megfelelő igénylési, jóváhagyási, kezelési és nyilvántartási	7

folyamatait, valamint a tűzfalszabályok rendszeres érdemi felülvizsgálatát, és az ellenőrzések teljeskörűségét	
Megfelelően és folyamatosan biztosítsa az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az internet irányából elérhető szolgáltatásai, mobilalkalmazásai esetében	4
A kockázatokkal arányosan különítse el a belső hálózaton a különböző kritikusságú és funkciójú hálózatokat	5
IV. Naplózás	
Biztonsági kockázattal arányos módon - jogszabályokban foglaltaknak megfelelően - gondoskodjon olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, továbbá alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is. A kockázatokkal arányosan alakítsa ki a központi automatikus biztonsági naplóelemzési- és riasztási képességeit.	13
Gondoskodjon a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenység naplózásáról, a naplófájlok sérthetetlenségének és rendelkezésre állásának biztosítottságáról és a naplóállományok továbbítása, tárolása során, valamint kritikus rendkívüli eseményekről történő automatikus figyelmeztetések generálásáról	5
Vizsgálja felül a naplóelemzési eljárásait, szabályozza a tevékenységet, ennek keretében készítsen tervet az infrastruktúra elemek, alkalmazások, adatbázisok bekötésére vonatkozóan, majd készítsen tervet és valósítsa meg az infrastruktúra elemek, szerverek, alkalmazások, adatbázisok biztonsági naplózását, a naplóállományok gyűjtését.	5
V. Jogosultság-menedzsment	
V.2. Felhasználói jogosultságok	
Biztonsági kockázattal arányos módon gondoskodjon (informatikai) rendszereinek szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról, ennek keretében erősítse a jogosultságok kezelésének, nyilvántartásának és ellenőrzésének folyamatait	9
V.5. Jogosultságnyilvántartás	
Gondoskodjon a teljes körű és naprakész jogosultságnyilvántartás folyamatos rendelkezésre állásáról.	6
VII. Üzletmenet-folytonosság	
Hajtsa végre az üzletmenet-folytonossági (BCP) és katasztrófa helyreállítási, katasztrófaelhárítási (DRP) tervek teljes körű, dokumentált és az üzleti szakterületek által hitelesített tesztelését, bizonyítva felkészültségét a rendkívüli helyzetek kezelésére, a mért végrehajtási időkkel igazolja a szolgáltatásainak az elvárt időn belül történő helyreállítási képességét.	9
VIII. Biztonsági-kockázatelemzés	
Végezze el, illetve vizsgálja felül az informatikai rendszer biztonsági kockázatelemzését, vagy a szolgáltató által készített kockázatelemzés alkalmazását fogadja el (adott esetben az MNB részére dokumentumokkal igazoltan) a jövőben pedig szükség szerint, de legalább a	10

jogszabály által előírt rendszerességgel gondoskodjon a kockázatelemzés kitöltésének teljességéről.	
XI. Nyilvántartások	
Vizsgálja felül a nyilvántartási rendszerét, hogy az mindenkor naprakészen, valamint egyértelmű és visszakereshető módon tartalmazza a használt és engedélyezett szoftver és hardvereszközöket, az adathordozókat, illetve – tárolási formától függetlenül – a technikai és magas szintű jogosultságokat, megfelelő dokumentummal igazolja a telepített és megvásárolt szoftverek jogtisztaságát.	5
XIII. Ellenőrzés	
Gondoskodjon a hálózati és hálózatbiztonsági eszközök konfigurációjának rendszeres felülvizsgálatáról és a kockázatokkal arányosan erősítse meg a biztonsági beállításokat, a hálózati szegmentációs beállításokat és hozzáféréseket, így a kockázatokkal arányosan különítse el a különböző kritikusságú és funkciójú hálózatokat	6
Vizsgálja felül és erősítse „hardening" beállításait és ellenőrzési folyamatait hálózati eszközei, operációs rendszerei, adatbázisai, alkalmazásai és virtuális környezetei esetében. Gondoskodjon az IT környezetére releváns „hardening" eljárások definiálásáról, azok naprakészen tartásáról és alkalmazásáról. A biztonsági kockázatokkal arányosan alakítson ki és folyamatosan tartson naprakészen adatbáziskezelő verziónként egységes „hardening" eljárásokat, és biztosítsa azok alkalmazását az adatbáziskezelő rendszerein.	5
XIV. Fejlesztés, változáskezelés	
Mindenkor gondoskodjon az éles-, a fejlesztői és a tesztkörnyezetek (adott esetben adatbázisok) megfelelő szétválasztásáról mind a bizalmasság, mind a sértetlenség és a rendelkezésre állás vonatkozásában. Biztosítsa az alkalmazási, produktív környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől.	7
Vizsgálja felül és erősítse egyes rendszereiben használt verzióváltozások és nyomon követések folyamatát, szabályozását, és gondoskodjon egyes rendszerei naprakészségéről, a biztonsági javítások telepítésének rendszerességéről, a használt termékverziók egyenszilárdságáról	7
Biztosítsa a már nem támogatott operációs rendszerek, alkalmazások, adatbázisok cseréjét, vagy – amennyiben ez valamilyen üzleti funkcionalitás fenntartása miatt csak hosszú távon lehetséges – azok kiegészítő kontrollokkal történő megerősítését, és vállalást a hosszú távú kivezetés határidejére	7

MEGÁLLAPÍTÁSOK ÉRTÉKELÉSE

ADATVAGYON

1. ADATVÉDELEM

Az MNB felügyeleti főosztálya többször, több fórumon kommunikálta, hogy a 2018-as év során a személyes adatok kezelésének ellenőrzésére – a GDPR alkalmazási határidejére tekintettel - kiemelt hangsúlyt fektetett. Ez a határozatokban is egyértelműen nyomon követhető, figyelembe véve, hogy klasszikus adatvédelmi kérdések az MNB auditjaiban 2018 előtt igencsak elvétve fordultak elő. Meglátásunk szerint a vizsgálatok csak az adatkezeléssel kapcsolatos követelmények felszínét súrolták, például hozva, hogy adattörléssel, adatmegőrzési idővel kapcsolatos hiányosság csak egy esetben fordult elő a vizsgált határozatokban, pedig a probléma általánosnak volt tekinthető még 2019-ben is a pénzügyi szektorban.

Itt fontos kiemelni, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) szerepköre a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése, az általános adatvédelmi rendeletben (GDPR) a NAIH részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében az általános adatvédelmi rendeletben és e törvényben meghatározottak szerint a NAIH gyakorolja. Mindezek mellett az MNB ajánlásaiban foglalt elvárásai között szerepel a személyes adatok anonimizálásának, valamint az adatokra irányadó megőrzési idő megtartásának, valamint a személyes adatokat is tartalmazó rendszerek következetes biztonsági osztályba sorolásának követelménye.

2. ADATOK, RENDSZEREK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

Több ágazatot is érintően, számos határozatban foglalt követelményként szerepelt, így láthatóan az MNB fókusza valamennyi ellenőrzése esetén az adatvagyon felmérés megfelelősége, az adatvagyon elemek nyilvántartásának kialakítása, az adatok szabályzat szerinti, dokumentált biztonsági osztályba sorolásának rendszeres elvégezése. A fent említetteken túl látható, hogy több esetben is elrendelésre került az adatgazdák kijelölése, az adatgazdák megfelelő kontroll-lehetőségeinek biztosítása.

Az adatgazdák kinevezésével, feladatköreivel, valamint az adatosztályozással kapcsolatos MNB elvárások már a legkorábbi felügyeleti ajánlásokban is megtalálhatóak voltak, valamint több, mint 10 éve nyomon követve a felügyeleti ellenőrzéseket ki lehet jelenteni, hogy az ellenőrzések minden esetben kiterjedtek ezen kontroll követelmények ellenőrzésére. Ennek ellenére az adatgazdai kinevezések, feladatkörök meghatározása és azok **érdemi** végrehajtása terén továbbra is jelentős hiányosságok tapasztalhatók a pénzügyi szektorban. Több szervezetnél találkozunk a problémával, hogy a rendszeres, éves elmélyítő oktatások ellenére a jogosultságok ellenőrzése, összeférhetetlen szerepkörök meghatározása, mentendő adatkörök meghatározása, RTO, RPO értékek definiálása – és még sorolhatnánk – tekintetében az adatgazdák nem tudnak érdemi döntéseket hozni,

csupán aláírják az informatika által meghatározott „változókat”. Ez láthatóan megjelenik a vizsgált MNB határozatokban.

A fentiek mellett érdemesnek tartjuk kiemelni, hogy több esetben találkoztunk azzal, hogy az eddig elterjed és az MNB által „elnézett” gyakorlattal ellentétben, mely az adatosztályozás tekintetében kizárólag a bizalmasságot vette tekintetbe – nyilvános, belső használatú, üzleti titok, személyes adat, stb. – az MNB megkövetelte az adatok integritási és a rendelkezésre állási követelményeinek, valamint megőrzési időtartamának meghatározását is a szervezettől.

KÁRTÉKONYKÓD ELLENI VÉDELEM

A szervezet hálózatához csatlakozó felhasználói munkaállomások a hálózati biztonság egyik leggyengébb pontjának tekinthetők és egyben teszik a végpontvédelem megfelelő kialakítását és folyamatos tesztelését, felülvizsgálatát a szervezetek egyik legfontosabb feladatává. Látható, hogy az MNB is kiemelt hangsúlyt fordít a vírusvédelem meglétére, így különösen elvárja, hogy a szervezet gondoskodjon *az informatikai biztonsági rendszer önvédelméről, kritikus elemei védelmének zártságáról és teljeskörűségét biztosító ellenőrzésekről, eljárásokról a kártékony kód elleni védelem megoldásának teljes körű telepítéséről, valamint a rendszer biztonsági kockázattal arányos vírus- és más rosszindulatú program elleni védelméről, továbbá a védelmi rendszerek ellenőrzéséről, jelentéséről megfelelő rendszerességgel.*

A fentekre tekintettel figyelmet érdemel, hogy 2010-es évek végén is még 11 pénzügyi szervezetnél tárt fel alapvető hiányosságot a felügyeleti ellenőrzés.

HATÁRVÉDELEM

A határozatok többnyire a már meglévő védelmi intézkedések eljárásainak, gyakorlatának, szabályozottságának finomítására, valamint a biztonsági környezet további erősítésének megkövetelésére terjednek ki. A szekcióba tartozó megállapítások esetében jól látható, hogy elsődlegesen nem egy védelmi intézkedés vagy rendszer – DLP, IPS, SSL inspection, DDoS elleni védelem - bevezetésére szólítják fel a szervezeteket, hanem a felügyelet elvárása a kockázatokkal arányos biztonsági környezet megfelelő kialakítása, a kialakított környezet védelmi képességeinek folyamatos felülvizsgálata, ellenőrzése. Ez összhangban van azzal, hogy ezen kontrollok és rendszerek bevezetése egyértelműen nem vezethető le a jogszabályokból, elsődlegesen a felügyeleti ajánlások tartalmaznak iránymutatásokat, melyek minden esetben a kockázatarányos megközelítést alkalmazzák.

Kiemelendő, hogy elterjedté vált a pénzügyi szektorban az informatikai erőforrások cégcsoportokon belüli központosítása, európai szolgáltatás központok létrehozása. Tapasztalatunk szerint, ezekben az esetekben a magyar leányvállalatok részére sok esetben nehézkes egyáltalán információt szerezni a kialakított határvédelmi rendszerről, nem beszélve annak érdemi kontrolljáról. **A vizsgált határozatokban látható, hogy a felügyelet nem fogadja el, ha a vizsgált szervezetnek nincs érdemi ráhatása a határvédelmi rendszer kialakítására, az őt érintő szabályok érdemi felülvizsgálatára.**

NAPLÓZÁS

A naplózással kapcsolatos megállapítások számából, valamint azok átfogó jellegéből adódóan ki lehet jelenteni, hogy a szervezeteknek 2020-ra sem sikerült teljesíteniük a központi naplógyűjtéssel és naplóelemzéssel, annak

teljes körűségével és a riasztási, riportolási képességgel kapcsolatos felügyeleti elvárásokat. A naplózás 2010-ben került a felügyeleti ellenőrzések fókuszába és ennek ellenére továbbra is kevés szervezet mondhatja el magáról, hogy teljesen nyugodtan várhatja a felügyeleti ellenőrzést.

Tapasztalatunk, hogy pusztán egy piacvezető termék megvásárlása, annak megfelelő integráció nélkül nem fogja a szervezet megfelelőségét biztosítani. A felügyeleti a kezdetekben nyíltan kommunikálta, hogy első lépésként megelégszik az alapinfrastruktúra naplóinak bevonásával, pusztán javasolni fogja az alkalmazói rendszerek bevonását. Ez a türelmi időszak véget ért, tapasztalatunk szerint a felügyelet elvárja minden szinten az érdemi naplóelemzést.

Az előző pontban említett központosított naplóelemző rendszerek is csak abban az esetben jelenthetnek megoldást, ha a magyar leányvállalat érdemben bevonásra kerül a kontroll környezet kialakításába, melynek végén érdemi riportokat, riasztásokat tud felmutatni.

JOGOSULTSÁG-MENEDZSMENT

A megfelelően működtetett jogosultság-menedzsment az adatok bizalmasságának és sértetlenségének megőrzése érdekében egyik legfontosabb és talán mondhatjuk legösszetetteb terület. Ez egyértelműen látszik abból is, hogy a vizsgált felügyeleti határozatokból több, mint 50, a jogosultság-menedzsment tárgyköréhez tartozó megállapítást gyűjtöttünk össze.

Természetesen ez fakad abból is, hogy a kontroll terület – például a naplóelemzéssel ellentétben – valamilyen érettségi szinten, de minden szervezetnél működő és alkalmazott folyamat, így a felügyeleti megállapítások is széles szórásban, annak finomhangolására vonatkoznak. A számosság indokolta, hogy a területhez tartozó megállapításokat az alábbi bontásban publikáltuk.

- V.1 Szabályozás
- V.2 Felhasználói jogosultságok
- V.3 Kiemelt jogosultságok
- V.4 Összeférhetetlenségek kezelése
- V.5 Jogosultságnyilvántartás
- V.6 Egyéb

MENTÉSEK KEZELÉSE

A várakozásoknak megfelelően, a mentések jogszabályoknak és felügyeleti elvárásoknak megfelelő végrehajtásáról a legtöbb szervezet – öt vállalat kivételével – sikeresen gondoskodott. A mentések hosszú évek óta legkevesebb vitát és kérdést kiváltó kontroll terület, annak fontosságát sem a szakma, sem az üzleti terület nem kérdőjelezi meg.

ÜZLETMENET-FOLYTONOSSÁG

Valamennyi vizsgált határozat tekintetében megállapítható, hogy az üzletmenet-folytonosság területén tett megállapítások fő témája az üzleti hatáselemzés, illetve üzletmenet-folytonossági tervek felülvizsgálata, az üzletmenet-folytonossági (BCP) és katasztrófa helyreállítási, katasztrófaelhárítási (DRP) tervek teljes körű,

dokumentált és az üzleti szakterületek által hitelesített tesztelése, melyből kitűnik, hogy a szervezetek túlnyomó többségénél a már meglévő üzletmenet-folytonossági és kapcsolódó dokumentumai szorulnak kiegészítése, vagyis azok megléte alapvetés a vizsgált szervezetek tekintetében.

BIZTONSÁGI KOCKÁZATELEMZÉS

A biztonsági kockázatelemzés és kezelés területén továbbra is az számít meglepetésnek, ha a felügyeleti ellenőrzés nem tár fel nem-megfelelőséget, nem fogalmaz meg javaslatokat. A határozatokból viszont már kiolvasható, hogy a legtöbb esetben nem a kockázatelemzés hiánya a probléma - ennek fontosságát vagy szükségszerűségét a szervezetek már felismerték - hanem annak teljes körűsége és a kockázatkezelés területén vannak lényegi hiányosságok. **Számos megállapítást találunk a kockázatcsökkentő intézkedési hiányára – 18 megállapítás közül 11 kapcsolódik a kockázatkezelési folyamat nem-megfelelőségéhez -, azok nem megfelelő dokumentáltságára, nyomon követésére vagy nem megfelelő szinten történő (pl. Igazgatótanács, felső vezetés, stb.) elfogadására.**

JELSZÓKEZELÉS

A jelszókezeléshez a többi területhez képest jelentősen kevesebb megállapítás társítható, míg az elvárások többsége szintén a meglévő szabályozás erősítését, felülvizsgálatát érinti, valamint több esetben a jelszavak komplexitásából fakadó hiányosságot tárt fel az audit.

TEVÉKENYSÉG KISZERVEZÉSE

Tapasztalatunk szerint, a felügyelet az elmúlt években kiemelt figyelmet fordít a kiszervezések ellenőrzésére, így annak vizsgálatára is, hogy a szervezetek tudnak-e érdemi kontrollt gyakorolni a szolgáltatók feladatvégzése során megvalósuló adatkezelésre, a szolgáltatók ellenőrzésére, valamint, hogy a szolgáltató megszűnésének vagy SLA sértő tevékenység végzésének eseteire rendelkezik-e a szervezet megfelelő folytonossági tervekkel.

Továbbra is több esetben találkoztunk a kiszervezési szerződések nem megfelelő azonosításával, pedig a felügyeleti ajánlások évek óta iránymutatásként tartalmazzák, hogy alkalmazni kell a kiszervezésre vonatkozó jogszabályi előírásokat azon cégek, informatikai szolgáltatók vonatkozásában, amelyek ügyfél adatokhoz vagy bank-, illetve értékpapírtitoknak, vagy pénzügyi ágazati törvény által titoknak minősülő adatokhoz férnek hozzá.

NYILVÁNTARTÁSOK

Az informatikai nyilvántartások vezetésének módszere és informatikai támogatottsága, automatizáltsága tekintetében rendkívül sokszínű a hazai gyakorlat, mellyel kapcsolatban az MNB-nek, tapasztalatunnk szerint, nincs kifejezett elvárása, amennyiben annak adattartalma megfelel a felügyeleti elvárásoknak. A felügyeleti határozatok összesítése alapján elmondható, hogy a legtöbb tartalmi hiányosság a licencek, szoftverek és a géptermi nyilvántartások tekintetében került megállapításra. Továbbra is kiemelt követelmény, hogy a szoftverek jogtisztasága, valamint használatuk szükségessége, jogossága mindenkor teljes körűen és naprakészen bizonyítható legyen. Tapasztalatunk szerint sok pénzügyi szervezetnél még hiányosságok vannak az

alapszoftverek, engedélyezett szoftverek, tiltott szoftverek elméleti azonosítása, valamint az engedélyezési folyamat napi alkalmazása tekintetében, mely felügyeleti megállapítást is eredményezhet.

SZABÁLYOZÁS

A szabályozás szekcióban főleg általános, vagy egyes kontroll területek egészére általában érvényes megállapítások kaptak helyet. Gyakorlati hasznuk kevesebb a többi szekcióhoz képest, de érdemben rámutat, hogy a szabályzati rendszer felügyeleti ajánlásokkal összhangban történő kialakítása, valamint annak aktuálisan tartása mindig jelen lévő és mindenki számára egyértelmű kötelezés.

ELLENŐRZÉS

A vizsgált időszakban a felügyeleti ellenőrzések a független ellenőrzés területén számos hiányosságot tártak fel. Tapasztalatunk szerint az MNB az informatikai szakterület független informatikai biztonsági felügyeletét és kontrollját biztosító szervezeti és működési rendek meglétét, azok szabályozásnak megfelelő megvalósulását és a feltárt hiányosságok kezelésének dokumentált intézkedési terv szerinti végrehajtását minden esetben a vizsgálat kiemelt fókuszába helyezik. Az ellenőrzések elvárások szerinti végrehajtása továbbra is a – szervezetileg és/vagy anyagi erőforrások tekintetében - kisebb szervezetek esetében jelentenek problémát, ahol nem áll dedikált humán erőforrás rendelkezésre a vizsgálatok lefolytatására, azok kiszervezés keretében történő végrehajtása pedig jelentős anyagi terhet jelenthet.

A vizsgált határozatok alapján is látható, hogy a felügyeleti ellenőrzés egyre nagyobb hangsúlyt fektet a technológiai ellenőrzések (internet felőli és belső hálózatain sérülékenységvizsgálatok lefolytatása, hálózati és hálózatbiztonsági eszközök konfigurációjának rendszeres felülvizsgálata, hardening vizsgálatok) megvalósulásának vizsgálatára.

FEJESZTÉS, VÁLTOZÁSKEZELÉS

A fejlesztés, változáskezelés szekcióban kevés számú és túlnyomórészt az éles-, a fejlesztői és a teszt környezetek elkülönítésével – a vizsgált időszakban 7 pénzügyi szervezetnél azonosított hiányosságot a felügyelet -, szabályozási kérdésekkel, és a fejlesztett termékek dokumentálásával és a forráskód kezeléssel kapcsolatos megállapítások kerültek.

Szeretnénk kiemelni, hogy szintén 7 szervezetnél merült fel hiányosságként **a biztonsági javítások telepítésének elmaradása, a használt termékverziók egyenszilárdságának hiánya, valamint a már nem támogatott operációs rendszerek, alkalmazások, adatbázisok használata**, mely vizsgálataink során szinte minden esetben magas kockázatként kerül azonosításra.

MEGÁLLAPÍTÁSOK TÉTELES FELSOROLÁSA

Jelen fejezetben felsorolásra kerülnek tételesen, területekre bontva a megállapítások, a fenti módszertannak megfelelő téma szerinti csoportosításban. Ismételten kiemeljük, hogy a téma szerinti csoportosítás során az összevonás alapját a megállapítások témaköre képezte, így elképzelhető, hogy egyes megállapítások a határozatban foglaltaknál tágabb körbe kerültek, azonban az összevonások, csoportosítások a határozatban foglalt minimum követelmények megtartásával történtek.

Megállapítás	Előfordulás a vizsgált időszakban
I. Adatvagyon	
I.1. Adatvédelem	
Mindenkor feleljen meg az ügyfeleivel, volt ügyfeleivel vagy a létre nem jött szerződésekkel kapcsolatos személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, e tekintetben végezzen adattisztítást a rendszereiben	2
Végezze el a nem éles (vagy nem az élesnek megfelelően kontrollált) környezetekben a védendő információk anonimizálását, ezáltal biztosítva, hogy a felhasználók kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhessenek a védendő információkhoz.	4
Az ügyfelek adatainak kezelésével összefüggésben a megszűnt biztosítási szerződések kapcsán személyes adatot a jövőben csak addig kezeljen, amíg a biztosítási jogviszonnyal kapcsolatban igény érvényesíthető, illetve amelynek kezeléséhez van törvényi jogalapja.	1
Az ügyfelek adatainak nyilvántartása terén vizsgálja felül és alakítsa át az ügyféladatokat nyilvántartó rendszereit az aktuális jogszabályi előírásban foglalt kötelezettségének betartása érdekében, hogy a papír alapon elérhető és elektronikusan tárolt adatok konzisztensek legyenek.	1
Végezze el az ügyféladatok anonimizálását azokban a tesztkörnyezetekben, amelyek csak tesztelési célokat szolgálnak. Ahol az anonimizálás nem lehetséges, ott intézkedjen az éles rendszerrel egyenértékű védelemről (jogosultságkezelés, naplózás stb.).	1
Tegye alkalmassá a rendszereit a tárolt adatok ellenőrzéséhez való felhasználásra	1
Szabályozza a szerződésekben az adatvédelemre vonatkozó előírások érvényesítését.	1
Dokumentáltan vizsgálja felül az egyes rendszereihez hozzáférő harmadik személyek körét annak megállapításához, hogy megvalósul-e pénzügyi szolgáltatási tevékenységhez kapcsolódó rendszeres adatkezelés	1
I.2. Adatok, rendszerek biztonsági osztályba sorolása	

Személyhez kötötten és a teljes adatvagyonra (adatkörök szerint) kiterjedően jelölje ki az adatgazdákat	3
Adatbesorolási szabályozásában és gyakorlatában valósítsa meg az adatok integritási és a rendelkezésre állási követelményeinek, valamint megőrzési időtartamának meghatározását, mindehhez biztosítsa az adatgazdák megfelelő kontroll-lehetőségeit	3
A jövőben az adatgazdák gyakoroljanak megfelelő kontrollt az adatok biztonsági osztályba sorolása, az adatok alapvető biztonsági, hozzáférési, továbbítási, tárolási, archiválási, törlési, megsemmisítési, fizikai hozzáférés-védelmi, címkézési, kódolási és szállítási szabályai, folyamatai felett, ezekről megfelelő ismeretekkel rendelkezzen	2
Gondoskodjon az általa kezelt adatok és az adatokat kezelő vagy feldolgozó informatikai rendszerek és rendszerelemek megfelelő biztonsági osztályozásának kialakításáról.	2
Dolgozza ki az adatosztályozás rendjét, határozza meg az adatosztályokhoz tartozó védelmi elveket és intézkedéseket	6
Biztosítsa, hogy rendelkezésre álljon az informatikai rendszer elemeinek biztonsági osztályokba történő besorolási rendszere	1
Mérje fel és osztályozza adatvagyonát. Alakítsa ki az adatvagyon elemek nyilvántartását, rendszeresen végezze el az adatok szabályzat szerinti, dokumentált biztonsági osztályba sorolását. Következetesen sorolja biztonsági osztályba a személyes adatokat is tartalmazó rendszereket.	9
II. Kártékonykód elleni védelem	
Hajtsa végre az eszközein a rendszeres, heti gyakoriságú, teljes rendszert lefedő kártékonykód ellenőrzések futtatását	1
Formalizálja a vírusriadók esetén szükséges intézkedések folyamatát, rendszeres, dokumentált teszteléssel ellenőrizze az eljárásrendjében leírtak alkalmazhatóságát	3
A biztonsági kockázattal arányos módon gondoskodjon az informatikai biztonsági rendszer önvédelméről, kritikus elemei védelmének zártságáról és teljeskörűségét biztosító ellenőrzésekről, eljárásokról. Gondoskodjon a rendszerbiztonsági kockázattal arányos vírus és más rosszindulatú program elleni védelemről, ennek megteremtése érdekében végezze el a kártékony kód elleni védelem megoldásának teljes körű telepítését.	10
A biztonsági kockázatokkal arányosan alakítson ki és működtessen olyan folyamatot, mely biztosítja a hálózatán üzemelő eszközökön a kártékony kód elleni védelmi rendszer telepítettségének rendszeres ellenőrzését, jelentését;	3
A Pénztár biztosítsa az eszközeinek heti teljes (Full Scan) vírusellenőrzését, valamint a kockázatokkal arányosan alkalmazza a rendszer riasztási és riportolási funkcióit.	1
A Pénztár erősítse továbbá az internetes elérések során a többszintű, mélységi kártékonykód elleni védelmet nyújtó biztonsági környezetet.	1
III. Határvédelem	
Vizsgálja felül a tűzfalszabály kezelési-, felülvizsgálati-, és nyilvántartási eljárásait, gyakorlatát, a kockázatokkal arányosan gondoskodjon olyan szabályozásról és folyamatokról, melyek biztosítják a tűzfalszabályok megfelelő igénylési, jóváhagyási, kezelési és nyilvántartási	7

folyamatait, valamint a tűzfalszabályok rendszeres érdemi felülvizsgálatát, és az ellenőrzések teljeskörűségét	
Szerezze be az információkat a hálózati topológia kialakításáról, a beállított tűzfal szabályok megismeréséről, a tűzfal rendszer sérülékenységi ellenőrzéséről	1
A pénztári eszközök és munkatársak internetelérésének védelme érdekében a jövőben a biztonsági kockázatokkal arányosan végezzen proxy alapú szűréseket.	2
Vizsgálja meg és a kockázatokkal arányosan biztosítsa a titkosított adatkapcsolatok biztonsági alapú szűrését (SSL Inspection) a határvédelmi eszközei esetében.	1
Biztosítsa a hálózati és hálózatbiztonsági eszközök működtetésével az információk biztonságának, integritásának és bizalmas jellegének megőrzését	1
MDM megoldás bevezetéséig, vagy bevezetését követően vizsgálja felül az MDM megoldásának és az Exchange rendszerének biztonsági paramétereit és gondoskodjon az elérhető biztonsági funkcióik megerősítéséről.	3
Biztosítsa az adathordozók szállítása, azonosítása, létesítménybe való ki- és beszállítása, és megsemmisítése során a Pénztár kockázatarányos biztonsági elvárásainak teljesülését.	1
Vizsgálja felül az adatszivárgási kockázatok kezelésére szolgáló megoldásait és folyamatait, majd ennek eredményeképpen a kockázatokkal arányosan alakítson ki olyan integrált védelmi megoldást, eljárásokat, melyek lehetővé teszik az adatszivárgási kockázatok érdemi kezelését, csökkentését,	2
Megfelelően és folyamatosan biztosítsa az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az internet irányából elérhető szolgáltatásai, mobilalkalmazásai esetében	4
Vizsgálja meg a DDoS támadás elleni védelem bevezetését, és amennyiben a felmerülő kockázatok indokolják, alkalmazza e biztonsági megoldást is	3
Vizsgálja felül az elektronikuslevél-védelmi megoldásainak biztonsági paramétereit és ennek eredményeképpen erősítse ki az elérhető biztonsági funkciókat az elektronikus levelezésének védelme érdekében, biztosítva ezzel az üzenettovábbítás (távadatvitel) bizalmasságát, sértetlenségét és hitelességét.	2
Informatikai rendszerei esetében mindenkor biztosítsa a biztonsági kockázatelemzés eredményének értékelése alapján, a biztonsági kockázattal arányos módon a távadatátvitel bizalmasságát, sértetlenségét és hitelességét.	2
Vizsgálja felül behatolás elleni védelmi képességeit és a kockázatokkal arányosan biztosítsa az IPS funkcionalitás használatát, a titkosított adatkapcsolatok ellenőrzését és alkalmazza védelmi rendszereinek biztonsági monitorozási, riasztási funkcióit.	3
Szüntesse meg az üzletileg nem indokolt, illetve biztonságilag kockázatos tűzfalszabályokat.	2
A kockázatokkal arányosan különítse el a belső hálózaton a különböző kritikusságú és funkciójú hálózatokat	5
IV. Naplózás	
Biztonsági kockázattal arányos módon - jogszabályokban foglaltaknak megfelelően - gondoskodjon olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, továbbá alkalmas a naplózás	13

rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is. A kockázatokkal arányosan alakítsa ki a központi automatikus biztonsági naplóelemzési- és riasztási képességeit.	
Naplózáshoz kapcsolódóan alakítson ki és folyamatosan tartson naprakészen adatbáziskezelő verziónként egységes „hardening" eljárásokat, és biztosítsa azok alkalmazását az adatbáziskezelő rendszerein.	1
A naplóállományok védelme érdekében hozzon létre olyan tárolási és hozzáférési rendszert, mely biztosítja a védendő állományok módosításának vagy törlésének nyomon követhetőségét.	1
Gondoskodjon a végfelhasználók és a kiemelt jogosultságokkal elvégzett tevékenység naplózásáról, a naplófájlok sérthetetlenségének és rendelkezésre állásának biztosítottságáról és a naplóállományok továbbítása, tárolása során, valamint kritikus rendkívüli eseményekről történő automatikus figyelmeztetések generálásáról	5
Vizsgálja felül a naplóelemzési eljárásait, szabályozza a tevékenységet, ennek keretében készítsen tervet az infrastruktúra elemek, alkalmazások, adatbázisok bekötésére vonatkozóan, majd készítsen tervet és valósítsa meg az infrastruktúra elemek, szerverek, alkalmazások, adatbázisok biztonsági naplózását, a naplóállományok gyűjtését.	5
Kockázatokkal arányosan erősítse a központi naplóelemző megoldás automatikus elemzési- és riasztási képességeit, valamint üzemeltetési szempontú biztonsági monitorozását.	3
Vizsgálja felül a CD/DVD írási jogosultsággal rendelkező felhasználók körét, szűkítse az engedélyezett USB portok számát csak azokra a felhasználókra, akiknek a munkájukhoz feltétlenül szükséges, ezekben az esetekben naplózza az adatírást	1
Biztosítsa az üzemeltetési folyamatokat tartalmazó operátori naplók vezetését, továbbá gondoskodjon azok visszakereshetőségéről, valamint elektronikus formában való hosszú távú megőrzéséről	1
Szabályzataiban rögzítse az általa alkalmazni kívánt naplózási gyakorlatot, a részletes információbiztonsági naplózási és naplóelemzési követelményeket	3
Erősítse a rendszerek változásainak felügyeletét, információbiztonsági naplóellenőrzéseit kiemelt figyelemmel végezze a fejlesztő és támogató munkatársak tevékenységeire vonatkozóan.	1
V. Jogosultság-menedzsment	
V.1. Szabályozás	
A teljes infrastruktúrájára kiterjedően határozza meg a jogosultságkezelés, nyilvántartás és ellenőrzés szabályait, és azokat folyamatosan működtesse	1
Gondoskodjon a jogosultságnyilvántartás és az összeférhetetlenségi politika felülvizsgálatáról és kiegészítéséről	1
Dolgozza ki a felhasználói, kiemelt és technikai jogosultságok felülvizsgálatának folyamatát, és annak alapján végezze el a felülvizsgálatot.	1
Alakítsa ki az adatokhoz való hozzáférés rendjét és határozza meg a felhasználók azonosításának követelményeit	1

A jogosultságkezelés területén olyan részletes jogosultságkezelési szabályozását alakítson ki, amely meghatározza a jogosultság igénylések adatgazdai jóváhagyását és a jogosultságok rendszeres felülvizsgálatát és alkalmazza azt.	1
V.2. Felhasználói jogosultságok	
Biztonsági kockázattal arányos módon gondoskodjon (informatikai) rendszereinek szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról, ennek keretében erősítse a jogosultságok kezelésének, nyilvántartásának és ellenőrzésének folyamatait	9
Vizsgálja felül a CD/DVD írási jogosultsággal rendelkező felhasználók körét, szűkítse az engedélyezett USB portok számát csak azokra a felhasználókra, akiknek a munkájukhoz feltétlenül szükséges, ezekben az esetekben naplózza az adatírást	1
Határozza meg a belépő munkatársak részére megadandó alapjogosultságok körét	1
V.3. Kiemelt jogosultságok	
Vizsgálja felül a jogosultságkezelési gyakorlatát és szabályozását annak érdekében, hogy az kockázatarányosan és dokumentáltan biztosítsa a rendszeradminisztrátori jogosultságok megfelelő kezelését	1
Igazolja, hogy a kiemelt (adminisztrátori) jogosultságok felhasználókhoz való rendelése a Pénztárnál biztosított	1
Igazolja a kiemelt felhasználói jogosultsággal rendelkező személyek esetében az erre vonatkozó nyilatkozatokat	1
Gondoskodjon a rendszergazdai feladatok egyértelmű meghatározásáról és a rendszergazdák kijelöléséről	1
Gondoskodjon a rendszergazda és az adatgazda feladatainak pontos kijelöléséről és a felelősségeik egyértelmű meghatározásáról.	1
A technikai felhasználókat rendelje természetes személyhez	1
Gondoskodjon arról, hogy a fejlesztő, ha az éles rendszerhez való hozzáférése a működés elégséges szintjének biztosításához nélkülözhetetlen, kizárólag erős kontrollok mellett és csak ideiglenesen kapjon hozzáférést.	1
V.4. Összeférhetetlenségek kezelése	
Az összeférhetetlenségi szabályok figyelembe vételével gondoskodjon a jogosultság ellenőrzések rendszeresen ismétlődő végrehajtásáról	1
Biztosítsa az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az összeférhetetlen informatikai és IT biztonsági feladatkörök szétválasztását a szervezeti és működési rend, a felelősségi, a nyilvántartási és a tájékoztatási szabályok meghatározásával, valamint a folyamatba épített ellenőrzési követelmények szabályok alkalmazásával.	1
Erősítse az összeférhetetlenségek meghatározásának és kezelésének, visszavonásának és ellenőrzésének folyamatait	1
Igazolja, hogy az összeférhetetlenséggel érintett személyek esetében az összeférhetetlenség megszüntetésre került	1

Vizsgálja felül az összeférhetetlen szerepköreinek kialakítását, beleértve az IT jellegű kiemelt jogosultságok kapcsán is és biztosítsa a meghatározott összeférhetetlenségek megfelelő kezelését	1
Kritikus rendszerei vonatkozásában határozza meg az összeférhetetlen üzleti és informatikai szerepköröket	1
Határozza meg az összeférhetetlen szerepköröket, dokumentálja azt, és alkosson részletes szabályozást a hozzáféréskezelés vonatkozásában.	1
Végezze el az összeférhetetlen szerepkörök meghatározását, és dokumentálja azt	1
V.5. Jogosultságnyilvántartás	
Gondoskodjon a teljes körű és naprakész jogosultságnyilvántartás folyamatos rendelkezésre állásáról.	6
Mindenkor biztosítsa egyes rendszereiben az azonosítók egyértelmű személyhez rendelését.	4
Szüntesse meg a nem indokolt, szükségtelen (pl. kilépett munkavállaló) jogosultságokat.	3
Tegye teljes körűvé az adminisztrátori felhasználók nyilvántartását	1
Igazolja, hogy a Pénztár rendelkezik a jogosultságok nyilvántartására vonatkozó informatikai programmal	1
V.6. Egyéb	
Biztosítsa, hogy azokat a személyhez nem rendelhető felhasználókat, amelyek fenntartása üzleti vagy technológiai szempontból nem indokolt, zárja le, megfelelő kontrollokkal (zárt boríték, felnyitás és megváltoztatás szabályozása) gondoskodjon a fennmaradó felhasználók esetében a jelszó kezeléséről.	1
Gondoskodjon arról, hogy az informatikai jogosultságok kiadásának és visszavonásának igénylése dokumentált formában történjen.	1
Végezzen rendszeres jogosultság felülvizsgálatot az ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztráció érdekében.	2
Valósítsa meg a távelérések során az Active Directory azonosítók egyértelmű személyhez rendelését a támogató cégek esetében is	1
Erősítse a jogosultságok kezelésének, nyilvántartásának, beállításának, és ellenőrzésének IT rendszerrel történő támogatását	2
Gondoskodjon a jogosultságok számának a működéshez szükséges és elégséges szintre történő csökkentéséről, továbbá valamennyi, személyhez nem rendelhető aktív felhasználó felülvizsgálatáról.	1
VI. Mentések kezelése	
Gondoskodjon a mentési rendre épülő mentés teljeskörűségének dokumentáltságáról	1
Határozza meg az adatmentések elvárt gyakoriságát az egyes alkalmazások esetén	1
Gondoskodjon az elvárásoknak megfelelő mentési beállításokról	1
Biztosítsa a szalagnyilvántartásának rendelkezésre állását, alternatív helyszínen és elektronikus formában történő tárolását	1

A mentési kazetták mozgatására alakítson ki folyamatot és olyan nyilvántartást mely biztosítja a mentési adattárolók védelmét és nyomon követhetőségét	1
Rendelkezzen olyan biztonsági mentésekkel és mentési renddel, amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik	2
Vizsgálja felül a mentési eljárásait, és gondoskodjon az adatgazdák bevonásáról a mentési rend meghatározásába, valamint biztosítsa a mentési rendbe és rendszerbe bevonni szükséges eszközök naprakészen tartását	1
A jövőben biztosítsa a mentések kockázati szempontból elkülönített és tűzbiztos tárolását, a mentések forrásrendszerrel azonos szintű hozzáférés védelmét, a mentések bizalmasságát, a mentések jogszabályi elvárások szerinti megőrzési időig történő tárolását, valamint adott esetben hogy a nyilvántartási adatállomány teljes körű mentésének egy aktuális példánya - negyedévente - mindenkor rendelkezésre álljon	2
VII. Üzletmenet-folytonosság	
Gondoskodjon az üzleti hatáselemzéseinek, illetve üzletmenet-folytonossági terveinek éves gyakoriságú felülvizsgálatáról.	3
Gondoskodjon kritikus alkalmazásai/rendszerei/folyamatai teljes körű, a vonatkozó MNB ajánlásban elvárt időközönkénti teszteléséről.	1
Biztosítsa a Magyarországon üzemeltetett rendszereit kiszolgáló géptermek DR tesztelését.	1
Gondoskodjon arról, hogy az informatikai szolgáltató az informatikai rendszerek helyreállítását rendszeresen tesztelje, és azok helyreállítását az üzleti területek által elvárt helyreállítási időn belül biztosítsa.	1
Készítsen olyan helyreállítási terveket amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik.	1
Egyértelmű és dokumentált döntéssel oldja fel az üzleti hatáselemzésben elvárt és a teljesített legnagyobb kiesési idők közötti ellentmondást	1
Gondoskodjon az üzleti hatáselemzésben elfogadott legnagyobb kiesési időknek megfelelő helyreállítási időkről	2
Határozza meg az adatok és a rendszerek elvárt helyreállítási értékeit (RTO, PRO) és a jövőben biztosítsa a rendszerek működésének az elvárt időablakon belüli, elvárt pontra történő helyreállíthatóságát, ennek hiányában léptessen életbe helyettesítő folyamatot	2
Tervezze meg üzletmenet-folytonossági és katasztrófaelhárítási folyamatait	1
Intézkedjen a katasztrófaelhárítási tervek helyreállítási lépéseinek részletes meghatározásáról, a tesztelési folyamatába vonja be az érintett üzleti területeket, a tesztelési jegyzőkönyveiben rögzítse a tesztelt scenáriókat, a tesztek alapján mért helyreállítási időket és azok viszonyát az üzletileg elvárt helyreállítási időkhöz, a tesztben résztvevő üzleti szakemberek és adatgazdák aláírását	2
Teszteléssel bizonyítsa minden egyes kritikus alkalmazás esetén, hogy képes a katasztrófa-helyreállítási tervekben szereplő folyamat alapján az elvárt helyreállítási időn belül helyreállítani az alkalmazásokat	2

Rögzítse és tartsa naprakészen az üzletmenet-folytonossági folyamatainál értesítendő személyek elérhetőségeit.	1
Mérje fel az üzletmenet fennakadásának kockázatát és lehetséges forgatókönyveit	1
Dolgozza ki az üzletmenet folytonossági terveit az olyan esetekre is, amelyek során az informatikai szolgáltatás elérhető.	1
Az üzletmenet-folytonosság területén intézkedjen az üzletmenet-folytonossági terve és forgatókönyvei teljes körűvé tételéről	1
Alakítsa ki üzletmenet-folytonossági tervét székháza informatikai rendszerének elérhetetlenné válása esetére és rendszeresen végezze el az üzletmenet-folytonossági terve és forgatókönyvei tesztelését	1
Intézkedjen informatikai katasztrófaelhárítási terve teljes körűvé tételéről	1
Készítse el az adatbázisok katasztrófaelhárítási eljárásait és vegye figyelembe az üzleti területek által elvárt helyreállítási időtartamokat és időpontokat;	1
Végezze el kritikus informatikai erőforrásai helyreállítási terveinek teljes körű tesztelését, továbbá az elsődleges és a másodlagos adatközpontok közötti átkapcsolás tesztjét	1
Dolgozzon ki helyreállítási tervet a tagok, tagszervezők és a Pénztár közötti kommunikációt lehetővé tevő elektronikus rendszerére	1
Végezze el az üzletmenet-folytonossági terve és forgatókönyvei, valamint az informatikai erőforrásai helyreállítási terveinek teljes körű tesztelését.	1
Gondoskodjon a rendkívüli helyzetek kezelésére vonatkozó tervek és eljárások rendszeres oktatásáról.	1
A jogszabályi előírásoknak megfelelő gyakorisággal végezze el az üzletmenet- folytonossági terv felülvizsgálatát és a kulcsfontosságú üzleti folyamatokat érintő események bekövetkezése esetén alkalmazandó helyreállítási akciótervek dokumentált tesztelését.	1
Határozza meg az egyes üzleti folyamatokhoz és informatikai alkalmazásokhoz tartozó elvárt helyreállítási időt, továbbá a mentendő állományok körét és a mentési gyakoriságot az elvárt helyreállítási idővel összhangban	1
Alakítson ki olyan DRP terveket, amelyek valamennyi, a Pénztár működése szempontjából kritikus rendszerre, a kockázatelemzésben azonosított forgatókönyvre és hirtelen bekövetkező szcenáriókra kiterjednek.	2
Vizsgálja felül a feladat- és felelősségi köröket, jelölje ki a tartalék adattárolási és feldolgozási helyszínt.	1
Egészítse ki az üzletmenet-folytonossági és katasztrófa-helyreállítási terveit oly módon, hogy azok külső szakértő számára is végrehajtható módon tartalmazzák a szükséges lépéseket, valamint almazhatóak legyenek katasztrófa helyzetben	2
A tevékenységek, illetve szolgáltatások folytonosságát biztosító megoldások keretében intézkedjen a katasztrófaelhárítási tervek helyreállítási lépéseinek részletes meghatározásáról	2
Intézkedjen üzletmenetfolytonossági esemény bekövetkezése esetén is a telefonhívások utólagos ellenőrizhetőségéről, a vagyonkezelési tevékenység üzletmenet-folytonossági tervében az üzleti adatok bizalmasságának biztosításáról.	2

Hajtsa végre az üzletmenet-folytonossági (BCP) és katasztrófa helyreállítási, katasztrófaelhárítási (DRP) tervek teljes körű, dokumentált és az üzleti szakterületek által hitelesített tesztelését, bizonyítva felkészültségét a rendkívüli helyzetek kezelésére, a mért végrehajtási időkkel igazolja a szolgáltatásainak az elvárt időn belül történő helyreállítási képességét.	9
Gondoskodjon a kockázati szempontból elkülönült tartalék informatikai üzemeltetési helyszín kialakításáról	1
Rendelkezzen, illetve a biztonsági kockázatokkal arányosan gondoskodjon a szolgáltatások ellátásához szükséges informatikai rendszerek, valamint a szolgáltatások folytonosságát biztosító tartalékberendezések, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldások biztosításáról.	1
Vizsgálja felül a BCP és DRP eljárások kezelési, tervezési, és tesztelési gyakorlatát, gondoskodjon azok teljes körű, összefüggő és a jogszabályokban foglalt előírásoknak megfelelő biztosításáról.	1
Mérje fel és kockázatarányos módon alakítsa ki a székhelyén üzemeltetett géptermének redundáns elektromos- és kommunikációs csatlakozását.	1
Mindenkor gondoskodjon a nyilvántartásainak elhelyezését biztosító elsődleges szerverszoba esetében a megfelelő és kockázatokkal arányos üzembiztonságot garantáló fizikai környezet kialakításáról.	2
VIII. Biztonsági-kockázatelemzés	
Mindenkor gondoskodjon a jogszabályban előírtak teljesüléséről, készítse el a rendszer biztonsági kockázatelemzését, ennek keretében biztosítsa, hogy az információbiztonsági kockázatelemzés hatóköre kiterjedjen a Bank releváns eszközeire, folyamataira és adatköreire egyaránt.	2
Biztosítsa, hogy a kockázatkelés folyamata egyértelműen meghatározott legyen, végrehajtásának elemei dokumentáltak és visszakereshetőek legyenek.	1
Gondoskodjon jóváhagyott, felelősöket és határidőket is tartalmazó kockázatcsökkentő feladatterv készítéséről és annak a felső vezetés és az informatikai biztonsági vezető (CISO) által rendszeresen ellenőrzött, nyomon követett végrehajtásáról	3
Jogszabályban meghatározott gyakoriságon felül a lényeges változások esetén is dokumentáltan végezze el az informatikai biztonsági kockázatainak felmérését, és tegyen intézkedéseket a feltárt kockázatok megszüntetésére.	1
Végezze el, illetve vizsgálja felül az informatikai rendszer biztonsági kockázatelemzését, vagy a szolgáltató által készített kockázatelemzés alkalmazását fogadja el (adott esetben az MNB részére dokumentumokkal igazoltan) a jövőben pedig szükség szerint, de legalább a jogszabály által előírt rendszerességgel gondoskodjon a kockázatelemzés kitöltésének teljességéről.	10
Az informatikai biztonsági kockázatelemzéshez kapcsolódóan az informatikai biztonsági kockázatelemzése eredményeként azonosított, javítandó hiányosságok és kockázatok mértékét határozza meg, lehetővé téve azok kockázatokkal arányos kezelését és alkalmazza azt.	1
A kockázatelemzés eredményéről formális vezetői döntés keretében határozzon	3

A kockázatelemzés eredményeként azonosított, (informatikai rendszereiben) kezelendő kockázatokhoz teljes körűen és egyértelműen rendeljen hozzá releváns kockázatcsökkentő intézkedéseket és alkalmazza azokat	3
Mérje fel az informatikai folyamatok, fenyegetések és kockázatok teljes körét, különös tekintettel a nem támogatott operációs rendszerek használatából eredő kockázatokra, és gondoskodjon a megfelelő kockázatcsökkentő intézkedésekről is	1
Vizsgálja felül a kockázatelemzési és kockázatkezelési módszertanát annak érdekében, hogy az elfogadható kockázati szintet meghaladó kockázatok érdemi kezelésére minden esetben sor kerüljön.	1
Dolgozzon ki olyan kockázatelemzési és -kezelési eljárásrendet, ami biztosítja, hogy a kockázatelemzés kiterjedjen a vállalatirányítás, a tervezés, fejlesztés és beszerzés, az üzemeltetés, a monitorozás és a független ellenőrzés területeire, a belső munkavállalók és külső támadók által elkövetett bűncselekményekből fakadó kockázatokra, tartalmazza a feltárt kockázatok elfogadható szintjének meghatározását, valamint a kockázat elfogadható szintre való csökkentését, vagy egyéb módon történő kezelését.	1
Rögzítse a kockázatok felmérésének felelősét, határozza meg a felmérés elvégzésének és az azt követő tevékenységek elvégzésének szabályait	1
Amennyiben egy kockázat elfogadására vonatkozó döntést hoz meg a Bank, úgy gondoskodjon a döntés megalapozásáról, annak dokumentálásáról, és arról, hogy a kockázatok felvállalása a dedikált döntési szinteken valósuljon meg.	1
Alakítson ki olyan eljárásrendet, amely biztosítja, hogy a jogszabályi követelményekből eredő kockázatok kezelése kockázat elfogadással ne történhessen meg, minden ilyen esetben hajtson végre érdemi kockázatcsökkentő intézkedést.	1
Gondoskodjon a felvállalt kockázatok megfelelő dokumentálásáról, a kockázatcsökkentő intézkedések megvalósításának nyomon követéséről és ellenőrzéséről	1
Vizsgálja felül és aktualizálja az informatikai rendszerének biztonsági kockázatelemzésével kapcsolatos szabályzatait, módszertanát. A feltárt kockázatok csökkentésére vonatkozó akciótervet a Pénztár igazgatótanácsa fogadja el, határozza meg a felelősöket és határidőket, valamint a terv teljesülését kérje számon.	1
A tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez valósítsa meg a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket	1
Szabályzatban rögzítse az informatikai biztonsági kockázatelemzés módszertanát, folyamatának lépéseit és felelőseit, az akcióterv pontokhoz rendeljen felelőst és határidőt és gondoskodjon az akcióterv pontok formalizált, rendszeres nyomon követéséről.	1
IX. Jelszókezelés	
Erősítse meg adatbázis szinten a jelszó komplexitási és lejárati szabályokat	2
Vizsgálja felül az egyes rendszereiben alkalmazott jelszókövetelményeket és biztosítsa jelszóbeállításaik szabályozása szerinti elvárásoknak való megfeleltetését	2
Gondoskodjon arról, hogy a pénztártag web-service-es ügyfélhozzáférést biztosító jelszavát az arra nem jogosultak – így a Pénztár munkavállalói, szolgáltatói – ne ismerhessék meg.	1

Vizsgálja felül és erősítse az internetbanki szolgáltatása esetében a tranzakció jóváhagyási folyamatait, ezen belül a gondoskodjon második faktor megkövetéléséről és a kapcsolódó telefonszámok naprakészségéről, teljeskörűségéről.	1
A kockázatokkal arányosan mindenkor biztosítsa a megfelelő hitelesítési eljárások és jelszókövetelmények alkalmazását a kritikus rendszerei esetében, beleértve az internetbanki alkalmazását	1
X. Tevékenység kiszervezése	
Alkalmazza a kiszervezésre vonatkozó jogszabályi előírásokat azon cégek, informatikai szolgáltatók vonatkozásában, amelyek - akár éles - ügyfél adatokhoz vagy bank-, illetve értékpapírtitoknak, vagy pénzügyi ágazati törvény által titoknak minősülő adatokhoz férnek hozzá	2
Kiszervezett tevékenységet végző informatikai szolgáltatók vonatkozásában alakítson ki olyan folyamatokat, amelyek biztosítják a kiszervezett tevékenységek nyomon követését	1
A kiszervezésnek minősülő tevékenység végzésére harmadik féllel már megkötött szerződést haladéktalanul jelentse be az MNB részére	1
Vizsgálja felül valamennyi, informatikai tárgyban megkötött szerződését, azonosítsa azokat, amelyek kiszervezésnek minősülnek, és a kockázatelemzés elvégzését követően szerződéseiben rögzítse, gyakorlatában pedig érvényesítse a jogszabályi előírásokat	2
Gondoskodjon a közreműködők bevonása során a személyi, tárgyi feltételeknek való megfelelés vizsgálatáról, egyetértése esetén hagyja jóvá a közreműködői szerződéseket és gondoskodjon arról, hogy azok biztosítsák a kiszervezett tevékenységnek az MNB, a pénztár ellenőrző bizottsága, valamint könyvvizsgálója által történő ellenőrzését.	1
Készítsen a kiszervezésre vonatkozó szerződésben foglaltaktól eltérő tevékenységvégzésből eredő, rendkívüli helyzetek kezelésére kidolgozott intézkedési tervet	3
Határozza meg a kiszervezett tevékenységet végzőtől elvárt, a tevékenység végzésének minőségére vonatkozó részletes követelményeket. Gondoskodjon továbbá a szerződéses teljesítés folyamatba épített méréséről és értékeléséről.	2
Határozattal összhangban egészítse ki a Pénztár „Kiszervezési szabályok” elnevezésű szabályzatának 4. számú mellékletét a kiszervezett tevékenységek vizsgálatának szempontjaival.	1
A Pénztár dokumentáltan bizonyosodjon meg továbbá arról, hogy a Szervernet Kft. milyen kontrollok segítségével kényszeríti ki a szerverhez történő fizikai és konzolos hozzáférés szabályait.	1
XI. Nyilvántartások	
Vizsgálja felül a nyilvántartási rendszerét, hogy az mindenkor naprakészen, valamint egyértelmű és visszakereshető módon tartalmazza a használt és engedélyezett szoftver és hardvereszközöket, az adathordozókat, illetve – tárolási formától függetlenül – a technikai és magas szintű jogosultságokat, megfelelő dokumentummal igazolja a telepített és megvásárolt szoftverek jogtisztaságát.	5
Biztosítsa a hardver eszközök nyilvántartásának naprakészségét és a róluk tárolt adatok körének kiegészítését	1

Készítse el és tartsa napra készen a géptermi eszközeinek nyilvántartását, végezzen ellenőrzést arra vonatkozóan, hogy a géptermeiben olyan informatikai nyilvántartások álljanak rendelkezésre, melyek naprakészek, tartalmilag, alkalmazhatósági szempontból is megfelelnek a jogszabályi előírásoknak, e körben gondoskodjon arról, hogy a gépteremben lévő eszközök egyértelmű azonosítása megtörténjen és a nyilvántartások, valamint a géptermi leírások a valóságnak megfelelően tartalmazzák az ott tárolt és fellelhető eszközöket, azok legyenek ellenőrizhetők és számonkérhetők.	3
Készítse el az informatikai eszközök műszaki célú nyilvántartását	1
Az informatikai eszköz/szoftver és munkaállomás szoftverkonfiguráció nyilvántartását folyamatosan naprakészen vezesse	1
Nyújtsa be az általa használt licencek nyilvántartását, és igazolja, hogy a telepített szoftvereket teljeskörűen nyilvántartja	1
Alakítsa ki az informatikai eszközök nyilvántartására, valamint a virtuális rendszereire vonatkozó szabályozását és alkalmazza azt	1
Gondoskodjon engedélyezett és tiltott szoftverek körének meghatározására vonatkozó gyakorlat kialakításáról	1
Biztosítsa az informatikai rendszerét alkotó szoftverek és licencek naprakész nyilvántartását, valamint erősítse a szoftver és licenc ellenőrzési folyamatát annak érdekében, hogy a szoftverek jogtisztasága, valamint használatuk szükségessége, jogossága mindenkor teljes körűen és naprakészen bizonyítható legyen.	4
XII. Szabályozás	
Mindenkor fordítson kiemelt figyelmet arra, hogy belső szabályozási eszközeiben rögzítésre kerüljenek a jogszabály szerint elvárt tartalmi elemek.	1
Alakítsa ki a megfelelő és adminisztrált változáskövetési és változáskezelési eljárásrendjét	1
A kockázatokkal arányosan oly módon szabályozza az informatikai tevékenységét a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területein, ami biztosítja a feladatok, felelősségek egyértelmű meghatározását, számon kérhetőségét és dokumentált végrehajtását	1
A jogszabályi elvárásokkal és a kockázatelemzése eredményével összhangban vizsgálja felül szabályozási rendszerét. Biztosítsa szabályzatainak naprakészségét, a szükséges felülvizsgálatokat dokumentált módon hajtsa végre, valamint határozza meg a szabályzatok jóváhagyását megelőzően a véleményezésbe bevonandó üzleti területek körét.	1
A Pénztár a kockázatokra tekintettel határozza meg a szabályzatok személyi hatályát, és gondoskodjon a szabályzatok dokumentált megismertetéséről.	1
A Pénztár gondoskodjon az informatikai tárgyú szabályzatok és eljárásrendek olyan módon történő elkülönítéséről, hogy azokhoz csak azok a személyek férhessenek hozzá, akik számára ez feladatkörük alapján indokolt.	1
Biztosítsa az informatikai rendszerének működtetésére vonatkozó utasítások és előírások meghatározását, azok megfelelő dokumentálását.	1
Alakítson ki és alkalmazzon a megbízható és körültekintő működésnek megfelelő belső szabályzatokat	1

Belső szabályzatában határozza meg az egyes munkakörök betöltéséhez szükséges informatikai ismereteket	3
Az informatikai tevékenységének naprakész szabályozásához kapcsolódóan rendelkezzen az informatikai szabályzatainak felülvizsgálatáról és a felülvizsgálat gyakoriságáról	1
A szabályozási környezet és a gyakorlat összhangjának megteremtése érdekében vizsgálja felül a fejlesztési és rendszerbevezetési módszertanát	1
A teljes infrastruktúrájára kiterjedően határozza meg a jogosultságkezelés, nyilvántartás és ellenőrzés szabályait, és azokat folyamatosan működtesse	1
Alakítsa ki a virtuális rendszerei adminisztrációját biztosító folyamatokat.	1
Hozzon létre olyan kontroll folyamatokat, melyekkel biztosítani képes, hogy a tiltott kézi programozással indított eljárások felderítésre kerüljenek.	1
Belső szabályzatában határozza meg az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.	1
Vizsgálja felül jogosultságkezelési gyakorlatát, (adott esetben az egyes rendszereiben kialakított szerepköröket) és gondoskodjon a szabályozásában elvártak betartásáról	5
Vizsgálja felül a felhasználók azonosításának követelményeit, ideértve belső szabályozását, továbbá jogosultsági rendszerét, a szerverhozzáférésekre is kiterjedően, továbbá megfelelő kontrollokkal (zárt boríték, felnyitás és megváltoztatás szabályozása) gondoskodjon a fennmaradó felhasználók esetében a jelszó kezeléséről.	1
XIII. Ellenőrzés	
Határozza meg az informatikai területnek a tőle független informatikai biztonsági felügyeletét, kontrollját biztosító szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat,	1
Végezzen az informatikai tevékenységek tervezésére, működésére, illetve a biztonságra vonatkozó független ellenőrzéseket, alakítson ki kontroll intézkedéseket, majd az eredmények és a kockázatok függvényében gondoskodjon a folyamatok javításáról, irányításáról	1
Gondoskodjon a biztonsági kockázattal arányos módon az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, így különösen a belső és külső sérülékenységvizsgálatokról és penetrációs tesztekről és azok megfelelő szabályozottságáról.	3
A kockázatokkal arányosan javítsa a sérülékenységi vizsgálatok, illetve az auditok során feltárt, a határozat indokolási részében részletezett hiányosságokat	1
Számoljon be az ellenőrző bizottság által elvégzett informatikai vizsgálat eredményéről, illetve nyújtsa be az azonosított feladatok megoldási tervét határidő és felelősök kijelölésével	1
Az ellenőrző bizottság a jövőben az előirányozott időben folytassa le az informatikai tárgyú ellenőrzéseket.	1
Végezzen rendszeresen vizsgálatokat annak érdekében, hogy a (...) Kft. által feltárt hiányosságok kiküszöbölésére vonatkozó intézkedések nyomon követése megtörténjen és az intézkedések végrehajtása folyamatos kontroll alatt legyen.	1

Folyamatosan biztosítja az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az internetes - beleértve az internetbanki - rendszerei esetében	1
Rendszeresen hajtsa végre a szabályzataiban előírt vizsgálatokat	1
Gondoskodjon a hálózati és hálózatbiztonsági eszközök konfigurációjának rendszeres felülvizsgálatáról és a kockázatokkal arányosan erősítse meg a biztonsági beállításokat, a hálózati szegmentációs beállításokat és hozzáféréseket, így a kockázatokkal arányosan különítse el a különböző kritikusságú és funkciójú hálózatokat	6
Vizsgálja felül és erősítse „hardening" beállításait és ellenőrzési folyamatait hálózati eszközei, operációs rendszerei, adatbázisai, alkalmazásai és virtuális környezetei esetében. Gondoskodjon az IT környezetére releváns „hardening" eljárások definiálásáról, azok naprakészen tartásáról és alkalmazásáról. A biztonsági kockázatokkal arányosan alakítson ki és folyamatosan tartson naprakészen adatbáziskezelő verziónként egységes „hardening" eljárásokat, és biztosítsa azok alkalmazását az adatbáziskezelő rendszerein.	5
Határozza meg a szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.	1
A biztonsági vizsgálatok esetén az adathálózati sérülékenységek vizsgálatára évente, míg az Internet felől érkező alkalmazások sérülékenységének vizsgálatára az üzembe állítást megelőzően, majd legalább évente kerüljön sor, és a vizsgálatok során kockázatként meghatározott hibák javítása is történjen meg	1
Gondoskodjon megfelelő belső ellenőrzési rendszerről, melyben biztosítani tudja a teljes körű, az informatikai és biztonsági infrastruktúrát, folyamatokat, kockázatokat és a kiszervezett tevékenységek témaköreit lefedő auditok végrehajtásához szükséges erőforrást	1
Az ellenőrző bizottság, illetve az ellenőrző bizottság számára ellenőrzéseket lefolytató belső ellenőr a jövőben a kiszervezett tevékenységeket teljeskörűen – az informatikai és informatikai biztonsági szempontokra és a több pénztár számára kiszervezett tevékenységet végző szolgáltatók elkülönült adatkezelésére kiterjedően – vizsgálja	1
Részletesen szabályozza és erősítse a biztonsági vizsgálatok folyamatát, beleértve a felelősségeket, a kockázatok kezelését és felvállalását	4
A biztonsági kockázatokkal arányosan vizsgálja felül és biztosítsa belső hálózatain a sérülékenységvizsgálatok alkalmazását	3
XIV. Fejlesztés, változáskezelés	
Mindenkor gondoskodjon az éles-, a fejlesztői és a tesztkörnyezetek (adott esetben adatbázisok) megfelelő szétválasztásáról mind a bizalmasság, mind a sértetlenség és a rendelkezésre állás vonatkozásában. Biztosítsa az alkalmazási, produktív környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől.	7
Alakítson ki és működtessen olyan informatikai rendszert, amely lehetővé teszi a megfelelő változáskövetés és változáskezelés fenntartását	1
Módosítsa eljárásait a jogszabályoknak megfelelő fejlesztési és változáskezelési folyamatok kialakítása és azok következetes alkalmazása érdekében.	1

A fejlesztések vonatkozásában már a tervezéstől kezdődően „by design” folyamatosan biztosítsa az általános információbiztonsági zártság követelményeinek való megfelelést, a biztonsági kontrollok megfelelő beépítését.	1
Gondoskodjon az általa fejlesztett rendszer biztonsági kockázattal arányos vírusvédelméről és a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről	1
Gondoskodjon olyan applikációk bevezetéséről, amelyek szállító által támogatott operációs rendszer környezetben működnek, továbbá a szállítók által kiadott patchjavítások telepítéséről,	1
Vizsgálja felül és erősítse egyes rendszereiben használt verzióváltozások és nyomon követések folyamatát, szabályozását, és gondoskodjon egyes rendszerei naprakészségéről, a biztonsági javítások telepítésének rendszerességéről, a használt termékverziók egyenszilárdságáról	7
Biztosítsa a már nem támogatott operációs rendszerek, alkalmazások, adatbázisok cseréjét, vagy – amennyiben ez valamilyen üzleti funkcionalitás fenntartása miatt csak hosszú távon lehetséges – azok kiegészítő kontrollokkal történő megerősítését, és vállalást a hosszú távú kivezetés határidejére	7
Dolgozza ki az általa használt, egyedi fejlesztésű rendszerek esetében a fejlesztő megszűnésekor alkalmazandó eljárásokat, biztosítsa az ezekhez szükséges feltételeket	1
Intézkedjen annak érdekében, hogy a fejlesztők az éles nyilvántartáshoz ne férjenek hozzá, továbbá, hogy a fejlesztések élesbe állításának dokumentálása megfelelően megtörténjen	1
Az informatikai fejlesztések során minden esetben készítse el a fejlesztési naplókat és tesztelési jegyzőkönyveket a megfelelő változáskövetés és változáskezelés érdekében, illetve gondoskodjon a megfelelő változáskövetés és változáskezelés fenntartásáról	1
Rögzítse szabályzatban az informatikai igénykezelés, fejlesztés, tesztelés és élesbe állítás folyamatait és kontrolljait, különös tekintettel a dokumentációra vonatkozóan.	2
Gondoskodjon arról, hogy az általa használt, egyedi fejlesztésű rendszerek leírásai, szintaktikai szabályai folyamatosan elérhetőek legyenek.	1
Gondoskodjon arról, hogy az adott rendszer aktuális forráskódja és fejlesztői dokumentációja letétben mindenkor rendelkezésére álljon.	1
Gondoskodjon az általa fejlesztett informatikai rendszer (weboldala) felépítésének és működtetésének ellenőrzéséhez szükséges rendszerleírások és modellek rendelkezésre állásáról	1

KAPCSOLAT

Szeretnénk kiemelni, hogy a vizsgálat részletes eredményeit, így az egyes megállapítások szervezeti érintettségét, valamint az egyes szervezeteket érintő határozatok elérhetőségét is tartalmazó xls munkafüzet nem kerül jelen dokumentummal együtt publikálásra. A tanulmánnyal kapcsolatos kérdéseket kérjük a praudit@praudit.hu e-mail címre küldje meg részünkre.

A SZERZŐKRŐL

dr. Kőmíves Balázs

dr. Kőmíves Balázs a PR-AUDIT Kft. vezető tanácsadója. Az adatvédelem és információbiztonsági terén több, mint 10 éves szakmai tapasztalattal rendelkezik, számos KKV és nagyvállalat informatikai és információbiztonsági felkészítését irányította, valamint kiszervezés keretében látja el az adatvédelmi tisztviselő és informatikai biztonsági felelős napi feladatait.

Jogász végzettsége mellett, az adatvédelem területén CIPP/E (Certified Information Privacy Professional/Europe) és belső adatvédelmi felelősi, míg az információbiztonság területen ISO27001 Lead Auditor-i, valamint CISM (Certified Information Security Manager) nemzetközi minősítéssel rendelkezik.

Tóth Miklós

Tóth Miklós a PR-AUDIT Kft. adatvédelmi és információbiztonsági tanácsadója, munkája során több hazai közép és nagyvállalat adatvédelmi átvilágításában és felkészítésében vett részt. Az információbiztonság terén kiemelt szakterülete az üzletmenetfolytonossági (BCM) keretrendszerek kialakítása, valamint ISO27001 Lead Auditor-i nemzetközi minősítéssel rendelkezik.

Dátum: 2020. 06. 29.