3. sz. melléklet

Balaton-felvidéki Nemzeti Park Igazgatóság
8229 Csopak, Kossuth u. 16.

Iktatószám: 351/2020.

## INTÉZKEDÉSI TERV – KÜLSŐ ELLENŐRZÉSHEZ

„ A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Hatósági Főosztály által a Balaton-felvidéki Nemzeti Park Igazgatóságon a 420/A-90-2/2016 iktatószámú végzés alapján lefolytatott átfogó vizsgálat"
című vizsgálathoz

| Megállapítás | Javaslat | Intézkedés | Határidő | Felelős |
|---|---|---|---|---|
| Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 14. § (2) bekezdésének c) pontja, valamint az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. Korm. rendelet 6. § (1) bekezdése szerint biztonsági hiányosságok feltárására került sor, amely alapján elrendelték ezek elhárítását. | 1.a. Az állami és önkormányzati szervek elektronikus információ biztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: BM rendelet) szerint definiált biztonsági osztály és -szint kategóriák használata, és az azok szerinti besorolások elvégzése.<br>1.b. Az informatikai és információbiztonsági tevékenységekhez kapcsolódó szerepkörök, feladatok, jogosultságok, felelősségek meghatározása, továbbá a szereplők együttműködési rendszerének szabályozása.<br>1.c. Biztonsági helyzet-, és eseményértékelés eljárási rend kialakítása.<br>1.d. Az intézkedési tervek felülvizsgálata és karbantartása a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján.<br>1.e. A munkakörök biztonsági besorolása, az ehhez kapcsolódó ellenőrzésének szabályozása (lehetséges más belső szabályozóban is).<br>1.f. Az interneten követendő viselkedési szabályok meghatározása | 1. A javaslatként megfogalmazott feladatok végrehajtása. Ehhez külső szakértő(k) bevonása szükséges.<br>2. Szükséges tárgyi feltételek (pl. hardver, szoftver) beszerzése is szükségessé válhat.<br>3. Az elvégzettekről a 2020. évben tájékoztatni kell a hatóságot. | 2020.06.30 | Gál Róbert osztályvezető, Takács Bódis Attila informatikus, Barcsik Kálmán rendszergazda-informatikus |
| | 2. Az elektronikus információs rendszerek mentési eljárásrendjében (BfNPI Mentési Rend) rögzíteni az egyes rendszerekre vonatkozó RPO és RTO értékeket, amelyek szükségesek a mentések gyakoriságának megállapításához. | | | |
| | 3. Az üzletmenet-folytonosságra vonatkozó eljárásrend (BfNPI Katasztrófaelhárítási terve) aktualizálása a BM rendelet 3.1.4.2 pontban és alpontjaiban meghatározott követelményeknek megfelelően. | | | |
| | 4. Az elektronikus információs rendszerek biztonsági eseménykezelési eljárásrendje (BfNPI Incidenskezelési szabályzat) aktualizálása a BM rendelet 3.1.5.8 pontban és alpontjaiban meghatározott követelményeknek megfelelően. | | | |
| | 5. A távozó munkavállalók estében a jogosultságok visszavonásának dokumentálása és ellenőrzése. | | | |
| | 6. A rendszerelem leltár kiegészítése, továbbá a rendszerek és eszközök közötti logikai kapcsolatok feltüntetése. | | | |
| | 7.Az adathordozók újrafelhasználásának, selejtezésének, illetve ehhez kapcsolódóan a visszaállíthatatlan törlésüknek a szabályozása. | | | |
| | 8. Kizárási házirend alkalmazása a sikertelen bejelentkezési kísérletek meghatározott száma fölött a hálózati belépések (AD) esetében. | | | |
| | 9. Az azonosított elektronikus információs rendszerek tekintetében a BM rendelet szerinti biztonsági osztályba sorolás elvégzése, a kapcsolódó NEIH-OVI űrlapok kitöltése és megküldése. Amennyiben a felmérés alapján a rendszerek nem teljesítik a megállapított osztályhoz tartozó biztonsági követelményeket, úgy cselekvési terv készítése. | | | |
| | 10. A szervezet BM rendelet szerinti biztonsági szintbe sorolásának elvégzése, a kitöltött NEIH-SZVI űrlap/ok megküldése hivatali kapun keresztül. Amennyiben a szervezet nem teljesíti az előírt követelményeket, úgy cselekvési terv készítése. | 1. A javaslatként megfogalmazott feladatok végrehajtása. Ehhez külső szakértő(k) bevonása szükséges.<br>2. Szükséges tárgyi feltételek (pl. hardver, szoftver) beszerzése is szükségessé válhat.<br>3. Az elvégzettekről a | 2020.06.30 | Gál Róbert osztályvezető, Takács Bódis Attila informatikus, Barcsik Kálmán rendszergazda- |
| | 11. A rendszeres karbantartásokra vonatkozó dokumentáció bevezetése. | | | |
| | 12. Külső rendszerekkel történő kapcsolódás esetében a szolgáltatási szerződésekben minden esetben szerepeltetni az információbiztonsági előírásokat | | | |

| | | | | |
|---|---|---|---|---|
| | 13. Kockázatelemzés alapján meghatározni azon adathordozók körét, amelyek titkosítása szükséges, az eredmény függvényében a használt adathordozók titkosítása | 2020. évben tájékoztatni kell a hatóságot. | | informatikus |
| | 14. A rendszer hozzáférési jogosultságok felülvizsgálatának szabályozása és dokumentálása. | | | |
| | 15. A biztonsági értékelés módszerének kidolgozása és bevezetése. | | | |
| | 16. A szervezetről nyilvánosan elérhető tartalom (pl. honlap, közösségi média) publikálási szabályainak kidolgozása. | | | |
| | 17. A tesztelés eseteire, menetére, dokumentációjára szabályok kialakítása. | | | |
| | 18. Konfigurációkezelési eljárásrend kialakítása, az alapkonfigurációk és a változások dokumentálása. | | | |
| | 19. Az adminisztrátori jogosultságok szükségességének felülvizsgálata, a felhasználók általi szoftver telepítési lehetőség szabályozása és ellenőrzése. | | | |
| | 20. Meghatározott ideju inaktivitas utan a felhasználói fiók felfüggesztésének szabályozása, végrehajtása, dokumentálása. | 1. A javaslatként megfogalmazott feladatok végrehajtása. Ehhez külső szakértő(k) bevonása szükséges.<br>2. Szükséges tárgyi feltételek (pl. hardver, szoftver) beszerzése is szükségessé válhat.<br>3. Az elvégzettekről a 2020. évben tájékoztatni kell a hatóságot. | 2020.06.30 | Gál Róbert osztályvezető, Takács Bódis Attila informatikus, Barcsik Kálmán rendszergazda-informatikus |
| | 21. A privilegizált fiókhoz történő hálózati hozzáférés esetén kétfaktoros autentikáció bevezetése. | | | |
| | 22. A távoli hozzáférés szabályainak kidolgozása, beleértve az engedélyezést, a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket. | | | |
| | 23. A hivatali tevékenységhez használt mobil eszközök alkalmazási szabályainak, követelményeinek, korlátozásainak meghatározása. | | | |
| | 24. Naplózási eljárásrend kidolgozása, melyben ki kell térni legalább a naplózandó események meghatározására, a naplóellenőrzés folyamatára, a riasztások kezelésére. | | | |

Intézkedési terv elfogadása

Alulírott Puskás Zoltán, mint a Balaton-felvidéki Nemzeti Park Igazgatóság igazgatója tájékoztatom az intézkedési terv elkészítéséért felelős szakmai igazgatóhelyettest és az intézkedési tervben felsorolt felelősöket, hogy az intézkedési tervet elfogadom.

Csopak, 2020. január 20.

Puskás Zoltán
igazgató

Balaton-felvidéki Nemzeti Park Igazgatóság Csopak 1.

Az intézkedési tervet átvettem:

Csopak, 2020. január 20.

Gál Róbert

Takács Bódis Attila

Barcsik Kálmán