MINISZTERELNÖKI KABINETIRODÁT VEZETŐ MINISZTER

Közli: Magyar Közlöny

A Miniszterelnöki Kabinetirodát vezető miniszter

MK rendelete

…/2023. (…. ….) MK rendelet

a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet módosításáról

A Magyarország kiberbiztonságáról szóló 2024. évi … törvény 81. § (3) bekezdés *a)* pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 9. § (1) bekezdés 7. pontjában meghatározott feladatkörömben eljárva – a Magyarország kiberbiztonságáról szóló 2024. évi … törvény 81. § (4) bekezdésében biztosított véleményezési jogkörében eljáró Szabályozott Tevékenységek Felügyeleti Hatósága elnöke véleményének kikérésével – a következőket rendelem el:

1. §

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) A Magyarország kiberbiztonságáról szóló 2024. évi … törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdése szerinti szervezet (a továbbiakban: szervezet) a rendelkezésében lévő elektronikus információs rendszert az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.”

2. §

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 2. §-a a következő szöveggel lép hatályba:

„2. § (1) Az 1. § (2) bekezdése szerint elvégzett besorolás alapján a szervezet a 2. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket az abban meghatározott módon teljesíti.

(2) A szervezetre és elektronikus információs rendszereire az e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív, logikai és fizikai védelmi intézkedések irányadók. Ha ezen intézkedésektől egy elektronikus információs rendszer

esetében a szervezet által elvégzett kockázatelemzés alapján indokolt eltérni, akkor az 1. mellékletben meghatározottak szerint kell eljárni.

(3) Ha a szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(4) A szervezet a kockázatelemzés és a kockázatok kezelése körében azonosítja és dokumentálja az elektronikus információs rendszer bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket a 3. melléklet szerinti fenyegetéskatalógus elemeinek vizsgálatával.”

3. §

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 3. §-a helyébe a következő rendelkezés lép:

3. § (1) A Kiberbiztonsági tv. 1. § (1) bekezdés *a)-c)* pontja szerinti szervezet
a) az elektronikus információs rendszer minden felhasználó szervezete tekintetében érvényesíti az elektronikus információbiztonsági követelményeket, ha az elektronikus információs rendszernek több felhasználó szervezete van, valamint
b) az elektronikus információbiztonsági követelményeket úgy érvényesíti a felhasználó szervezet tekintetében, hogy a követelményeknek való megfelelés a felhasználó szervezet elektronikus információbiztonsággal kapcsolatos eljárási rendjébe beépüljön.

(2) A Kiberbiztonsági tv. 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet, valamint a Kiberbiztonsági tv. 1. § (1) bekezdés *b)* pontja szerinti és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezetnek minősülő szervezet tekintetében az 1. melléklet 3.2.6. pontjában foglalt rendelkezések nem alkalmazhatók.”

4. §

(1) A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. melléklete az 1. melléklet szerint módosul.

(2) A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 2. melléklete a 2. melléklet szerint módosul.

5. §

Ez a rendelet 2025. január 1-jén lép hatályba.

6. §

Nem lép hatályba a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. § (1) bekezdése.

7. §

Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

Rogán Antal
Miniszterelnöki Kabinetirodát vezető miniszter

1. melléklet a .../2024. (...) MK rendelethez

1. A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 1. melléklet 1. pontja helyébe a következő pont lép:

„1. **A KOCKÁZATMENEDZSMENT KERETRENDSZER**

1.1. A szervezet a biztonsági osztályba sorolás és a védelmi intézkedések bevezetésének támogatására kockázatmenedzsment keretrendszert működtet, amelynek keretében

1.1.1. a keretrendszer alkalmazására való felkészülésként

1.1.1.1. a szervezetre vonatkozóan meghatározza és dokumentumban rögzíti:

1.1.1.1.1. az elektronikus információs rendszerei védelmével kapcsolatos szerepköröket, felelősségeiket, feladataikat és az ehhez szükséges hatásköröket,

1.1.1.1.2. a kockázatmenedzsment stratégiáját, amely leírja, hogy a szervezet hogyan azonosítja, értékeli, kezeli és felügyeli a biztonsági kockázatokat,

1.1.1.1.3. a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit,

1.1.1.2. az elektronikus információs rendszerekre vonatkozóan meghatározza és dokumentumban rögzíti:

1.1.1.2.1. a rendszer által támogatandó üzleti célokat, funkciókat és folyamatokat,

1.1.1.2.2. a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy szervezeteket,

1.1.1.2.3. az érintett vagyonelemeket,

1.1.1.2.4. a rendszer szervezeti és technológiai határát,

1.1.1.2.5. a rendszer által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát,

1.1.1.2.6. a rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését az 5. pontban meghatározott elvek szerint,

1.1.1.2.7. a rendszer helyét a szervezeti architektúrában, amennyiben a szervezet rendelkezik vele;

1.1.2. a 2. pontban meghatározott irányelvek szerint biztonsági osztályba sorolja az elektronikus információs rendszereit;

1.1.3. a 2. melléklet szerint beazonosítja a biztonsági osztályhoz tartozó védelmi intézkedéseket. A beazonosított intézkedéseket kockázatelemzés alapján testre szabja. Amennyiben a kockázatelemzés indokolja, a szervezet a 3. pontban meghatározott módon eltérhet a rendszerre vonatkozó biztonsági követelményektől, illetve a 4. pont szerint

alkalmazhat helyettesítő védelmi intézkedéseket. Fentiek végrehajtásával megállapítja az elektronikus információs rendszerre értelmezendő és alkalmazandó biztonsági követelményeket. A szervezet a biztonsági követelményeket a rendszerbiztonsági tervben dokumentálja, amelyet szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős szerepkört betöltő személy hagy jóvá. A szervezet a folyamatos felügyeleti stratégiával összhangban kidolgozza a rendszerre vonatkozó védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrendet;

1.1.4. rangsorolja, majd végrehajtja a kiválasztott és a rendszerbiztonsági tervben dokumentált intézkedéseket. Az intézkedések végrehajtása során a szervezet a rendszerbiztonsági tervet a védelmi intézkedések tényleges megvalósítása, valamint a tervtől való esetleges eltérések alapján frissíti;

1.1.5. értékeli a megvalósított védelmi intézkedéseket, amelynek érdekében

1.1.5.1. meghatározza a védelmi intézkedések értékeléséért felelős szerepkört betöltő személyeket,

1.1.5.2. kialakítja, felülvizsgálja és jóváhagyja a megvalósított védelmi intézkedések értékelésének tervét,

1.1.5.3. az értékelési tervben meghatározott értékelési eljárásrend alapján értékeli a védelmi intézkedéseket,

1.1.5.4. a védelmi intézkedések értékelésének dokumentálásaként elkészíti az észrevételeket és javaslatokat tartalmazó értékelési jelentését,

1.1.5.5. az értékelési jelentésben foglalt észrevételek és javaslatok alapján a szervezet további intézkedéseket vezet be a követelmények teljesítése érdekében, majd újraértékeli a védelmi intézkedéseket, valamint intézkedési tervet készít a fennmaradó kockázatok kezelésére;

1.1.6. a szervezet a rendszer biztonsági állapotára vonatkozó dokumentumok (rendszerbiztonsági terv, értékelési jelentés, rendszer kockázatelemzés, intézkedési terv) alapján az üzembe helyezésére vagy üzemben tartására vonatkozó kockázatokat megvizsgálja, és a szervezet vezetője más személyre át nem ruházható feladatkörében eljárva – jegyzőkönyvben dokumentált módon – dönt a rendszer használatbavételéről vagy használatának folytatásáról;

1.1.7. a védelmi intézkedések folyamatos felügyeletével az elektronikus információs rendszer teljes életciklusa alatt gondoskodik arról, hogy a bekövetkezett szervezeti, technológiai és biztonsági környezetének változása esetén a védelmi intézkedések a kockázatokkal arányosak maradjanak. Ennek keretében:

1.1.7.1. figyelemmel kíséri az elektronikus információs rendszerben vagy a működési környezetében bekövetkezett, a rendszer biztonsági helyzetét befolyásoló változásokat, és ennek alapján frissíti a vonatkozó dokumentumokat,

1.1.7.2. a folyamatos felügyeleti stratégia alapján értékeli a rendszerben megvalósított védelmi intézkedéseket, azok állapotát rendszeresen jelenti a jogosult személyek felé,

1.1.7.3. rendszeresen felülvizsgálja az elektronikus információs rendszer biztonsági állapotát, hogy megbizonyosodjon arról, hogy az azonosított kockázatok elfogadhatók-e a szervezet számára,

1.1.7.4. biztosítja, hogy a rendszer élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket.”

2. melléklet a .../2024. (...) MK rendelethez

1. A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet 2. melléklet 5. pontjában foglalt táblázat 4. és 5. sora helyébe a következő rendelkezések lépnek:

	(A	***B***	***C***	***D***	***E)***
”					
4.	5.3. Biztonsági értékelések – Független értékelők	5.3. A Kiberbiztonsági tv. 16. § (1) bekezdése szerint kiberbiztonsági auditra nem kötelezett szervezet - a honvédelmi célú rendszerek kivételével - független értékelőket vagy értékelőcsoportokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.	-	X	X
5.	5.4. Biztonsági értékelések – Kiberbiztonsági audit	5.4. A Kiberbiztonsági tv. 16. § (1) bekezdése szerint kiberbiztonsági auditra kötelezett szervezet független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.	X	X	X

”