5N | IT & SERVICE

7/2024. (VI. 24.) MK rendelet

a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

hatályos: 2025. január 1-én lép hatályba.
állapot:2025. 02. 06.

7/2024. (VI. 24.) MK rendelet

a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

hatályos: 2025. január 1-én lép hatályba.
állapot:2025. 02. 06.

1. §

(2) A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdése szerinti szervezet (a továbbiakban: szervezet) **a rendelkezésében lévő, a Kiberbiztonsági tv. hatálya alá tartozó elektronikus információs rendszerét az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.**

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**.

1. melléklet a 7/2024. (VI. 24.) MK rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolása és a védelmi intézkedések bevezetésének támogatására szolgáló kockázatmenedzsment keretrendszer

1. A KOCKÁZATMENEDZSMENT KERETRENDSZER

A biztonsági követelményeket **a rendszerbiztonsági tervben** dokumentálja, rangsorolja és végrehajtja. Ezt a tervet a szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős személy hagyja jóvá.

A szervezet a folyamatos felügyeleti stratégiával összhangban kidolgozza a rendszerre vonatkozó védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrendet; ez alapján értékeli azokat.

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.**

Az elektronikus információs rendszer biztonságáért felelős személy 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:

- figyelemmel kíséri az elektronikus információs rendszerben vagy a működési környezetében bekövetkezett, a rendszer biztonsági helyzetét befolyásoló változásokat, és ennek alapján frissíti a vonatkozó dokumentumokat
- értékeli a rendszerben megvalósított védelmi intézkedéseket, azok állapotát rendszeresen jelenti a jogosult személyek felé
- rendszeresen felülvizsgálja az elektronikus információs rendszer biztonsági állapotát, hogy megbizonyosodjon arról, hogy az azonosított kockázatok elfogadhatók-e a szervezet számára
- biztosítja, hogy a rendszer élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket.
- biztonsági osztályba sorolja a szervezetet, azonosítja az ehhez tartozó védelmi intézkedéseket, melyeket a kockázatelemzés alapján testre szab. *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.*

A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a szervezet felelőssége!

Az „ALAP" biztonsági osztály esetében:

- **legfeljebb csekély káresemény következhet be**, mivel az elektronikus információs rendszerben **jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet**
- a szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet
- lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy a közvetlen és közvetett **anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.**

A „JELENTŐS" biztonsági osztály esetében

- **közepes káresemény** következhet be, mivel nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet
- **személyi sérülések esélye megnőhet** (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányíthatatlansága miatti veszélyeket)
- a szervezet üzleti vagy ügymenete szempontjából **érzékeny folyamatokat kezelő rendszer**, információt képező adat vagy egyéb, **jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet**
- a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy a közvetlen és közvetett **anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.**

A „MAGAS" biztonsági osztály esetében

- **nagy káresemény** következhet be, mivel különleges személyes adat nagy mennyiségben sérülhet
- **emberi életek kerülnek közvetlen veszélybe**, személyi sérülések nagy számban következhetnek be
- nemzeti adatvagyon helyreállíthatatlanul megsérülhet
- **az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított**
- a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet
- súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy a közvetlen és közvetett **anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.**

3. ELTÉRÉSEK

A szervezet az alábbi lehetséges eltérésekkel teljesítheti a 2. mellékletben **meghatározott minimális követelményeket a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával**

A szervezet **a vonatkozó szabályozásában dokumentálja és indokolja,** hogy a jelen rendeletben foglalt védelmi intézkedésektől eltérő, általa meghatározott intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, kockázatokkal arányos biztonsági követelményszintjét, és azt, hogy miért nem használhatók a jelen rendeletben megjelölt védelmi intézkedések.

- A működtetési környezet jellegétől függő védelmi intézkedések
- A fizikai infrastruktúrával kapcsolatos eltérések
- A nyilvános hozzáféréssel kapcsolatos eltérések
- Technológiai eltérések
- A védelmi intézkedések bevezetésének fokozatosságával kapcsolatos eltérések
- Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei tekintetében egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak.

4. HELYETTESÍTŐ VÉDELMI INTÉZKEDÉSEK

A helyettesítő védelmi intézkedés során a szervezet az **adott biztonsági osztályhoz tartozó védelmi intézkedéssel egyenértékű vagy összemérhető védelmet nyújtó módon biztosít** minden külső vagy belső követelménynek (jogszabályoknak vagy szervezeti szintű szabályozóknak) való **megfelelést**

5. KOCKÁZATELEMZÉS ÉS A KOCKÁZATOK KEZELÉSE

- A szervezet értékeli az elektronikus információs rendszerrel, az általa kezelt adatokkal kapcsolatosan felmerülő kockázatokat
- Azonosítja és dokumentálja az EIR és az általa feldolgozott adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket.
- Azonosítja a sérülékenységeket és a hajlamosító körülményeket, amelyek befolyásolják annak valószínűségét, hogy a fenyegetések káros hatásokhoz vezetnek, továbbá meghatározza a káros hatások valószínűségét és mértékét.
- Meghatározza a fenyegetések káros hatásainak és azok bekövetkezésének valószínűsége alapján az eredő kockázatokat, valamint legalább négy fokozatú skálán („alacsony”, „közepes”, „magas”, „kritikus”) azok mértékét (kockázati kategória)
- Eldönti és dokumentumban rögzíti, hogy az egyes kockázatok kezelése érdekében milyen intézkedést alkalmaz (elkerülés, csökkentés, áthárítás, megosztás, felvállalás)
- A kockázatelemzés eredményét felhasználja az elektronikus információs rendszer biztonsági osztálya megállapításának, valamint a védelmi intézkedések kiválasztásának és testre szabásának támogatására
- A szervezet folyamatosan nyomon követi az elektronikus információs rendszerrel kapcsolatos kockázatok változásaihoz hozzájáruló tényezőket, és ennek alapján frissíti és naprakészen tartja a kockázatelemzési dokumentumait.