**MAGYARORSZÁG KORMÁNYA**

Közli: Magyar Közlöny

**A Kormány**

**…….**

**rendelete**

**a honvédelmi célú elektronikus információs rendszerek korai figyelmeztető rendszeréről**

A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *m)* pontjában kapott felhatalmazás alapján az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

## 1. A rendelet hatálya

**1. §** A rendelet hatálya a honvédelmi célú elektronikus információs rendszert használó vagy üzemeltető szervezetre terjed ki.

## 2. Értelmező rendelkezések

**2. §** E rendelet alkalmazásában

1. *biztonsági jelzés*: a jelforrásból származó üzenet, amely valamely rendszerelem biztonságában bekövetkezett negatív változásra figyelmeztet,
2. *biztonsági naplóállomány:* a honvédelmi célú elektronikus információs rendszerelembe épített, annak üzemelése közben keletkező naplóállomány, amelyben a gyűjtött metaadatok és összefüggéseik segítik a honvédelmi célú elektronikus információs rendszerelem által nyújtott funkció bizalmasságának, sértetlenségének megőrzését, valamint rendelkezésre állásának folyamatos ellenőrzés alatt tartását,
3. *hálózati eszköz:* a hálózat fizikai összekötését biztosító – hardverelemet és szoftvert is magában foglaló – rendszerelem,
4. *hálózati forgalom:* a hálózati eszköz egy meghatározott pontján keresztül áramló adatfolyam,
5. *hálózati forgalomkicsatoló eszköz:* a honvédelmi célú elektronikus információs rendszerben vagy a határán elhelyezett eszköz, amely a hálózati forgalom másolatát elvezeti a honvédelmi ágazati korai figyelmeztető rendszer szenzorjához,
6. *hálózati forgalom kivonata*: a hálózati forgalomból előállított műszaki adat, amelyből a hálózati forgalom nem állítható helyre,
7. *honvédelmi ágazati korai figyelmeztető rendszer:* a honvédelmi célú elektronikus információs rendszer érdekében működő olyan központosított védelmi megoldás, amely a védett rendszer eseménynaplóinak, a jelforrás biztonsági jelzésének, szenzorral gyűjtött és feldolgozott hálózati forgalma kivonatának automatizált elemzése alapján azonosítja a honvédelmi célú elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának sérülésére utaló kockázati tényezőket, valamint biztonsági esemény kísérletét vagy tényét,

8. *információs kapcsolatrendszer*: a két vagy többoldalú együttműködési megállapodáson alapuló nemzeti és nemzetközi együttműködés által biztosított adat és információ szervezett rendje,
9. *jelforrás:* a honvédelmi célú elektronikus információs rendszer védelmét ellátó biztonsági jelzés kiadására és továbbítására alkalmas eszköz, amely magába foglalja a védendő hálózati szegmens, valamint a végpontvédelem és riasztási rendszer eseménynapló jelzését biztosító eszközt,
10. *központi elem:* a köztes elemből érkezett adatot, valamint a támogató adatforrás adatát elemző és értékelő rendszerelem, amely az elvégzett művelet eredményeképpen a korai figyelmeztetés kiadásának folyamatát elindítja és elérhetővé teszi a korai figyelmeztetésre vonatkozó adatot,
11. *központi rendszer:* központosított, egységesen szabályozott üzemeltetés alá vont infrastruktúrájú és szervezési elvű modulárisan felépített informatikai rendszer, amelyben a rendszer kialakítási elve biztosítja a honvédelmi célú elektronikus információs rendszert üzemeltető és használó szervezet részére az egyedi csatlakozás lehetőségét és a testreszabott funkciók elérését,
12. *köztes elem:* a honvédelmi ágazati korai figyelmeztető rendszernek a védett intézménynél telepített része, amely a metaadatokon feldolgozást végez és annak eredményét továbbítja a központi elem felé,
13. *metaadat:* a honvédelmi célú elektronikus információs rendszer eleme által kezelt adatot leíró információk összessége, amely szabványos formátumban leírja az adat minőségét, állapotát és egyéb jellemzőjét, és amely oly módon mentes törvény által védett adatoktól, hogy azokat kizárólag a védett intézmény tudja helyreállítani,
14. *szakfeladat szerint elkülönülő eseménykezelő központ:* az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet 6. § (1) bekezdése szerinti szakfeladat szerint elkülönülő eseménykezelő központ,
15. *szenzor:* a honvédelmi ágazati korai figyelmeztető rendszer végponti elemébe integrált, a hálózati forgalmat monitorozó hardver és szoftver elemek együttese, amely a védett infrastruktúra felől a köztes elem felé logikailag egyirányú hálózati kapcsolattal rendelkezik, és a hálózati forgalom más módon nem elérhető kivonatát állítja elő,
16. *támogató adatforrás:* kiberfenyegetettségi helyzetképet leíró információt tartalmazó adatbázis,
17. *védett intézmény:* a honvédelmi ágazati korai figyelmeztető rendszer szolgáltatását igénybe vevő szervezet,
18. *védett rendszer:* a védett intézmény elektronikus információs rendszere,
19. *végponti elem:* a honvédelmi ágazati korai figyelmeztető rendszernek a védett intézménynél telepített része, amely a védett rendszer eseménynaplójából, a szenzor által előállított adatból, valamint a jelforráso biztonsági jelzéséből metaadatot képez,
20. *végpontvédelem és riasztási rendszer:* olyan védelmi szoftvermegoldás, amely a védelme alatt álló végponton károskód jelenlétére utaló jelzés észlelésére és elsődleges automatikus beavatkozásra képes,
21. *vizsgált esemény:* veszélyre utaló adatok, jelenségek és folyamatok összessége.

## 3. A honvédelmi ágazati korai figyelmeztető rendszer felépítése

**3. §** A honvédelmi ágazati korai figyelmeztető rendszer központi-, köztes- és végponti elemekből, az azokat összekötő hálózati infrastruktúrából, támogató adatforrásból, valamint az információs kapcsolatrendszerből épül fel.

**4. §** (1) A jelforrás a végponti és a köztes elemen keresztül kapcsolódik a honvédelmi ágazati korai figyelmeztető rendszer központi eleméhez.

(2) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet a végponti elem és a védett rendszer jelforrásai között adminisztratív vagy technikai eljárás útján a védett rendszerbe történő közvetlen beavatkozást kizáró egyirányú kapcsolatot alakít ki.

(3) A jelforrás, a hálózati forgalomkicsatoló eszköz és a szenzor felett kizárólag a honvédelmi célú elektronikus információs rendszert üzemeltető szervezet vagy a szervezet vonatkozásában illetékes szakfeladat szerint elkülönülő eseménykezelő központ rendelkezhet olyan jogosultsággal, amely a forgalmi adathoz való hozzáférést, illetve a hozzáférési jogosultság módosítását biztosítja.

(4) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet az eseménykezelési feladatát a szakfeladat szerint elkülönülő eseménykezelő központ szakmai irányítása és koordinációja alatt ellátó védett intézményre vonatkozó köztes elem által előállított adathoz a szakfeladat szerint elkülönülő eseménykezelő központ részére hozzáférést biztosít.

**5. §** (1) A szenzor elektronikus információs rendszerben elfoglalt helyét, rendszerszintű beállítását a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet és a védett intézmény egyeztetést követően határozza meg.

(2) A védett intézmény részletes elemzéssel vagy dokumentációval alátámasztva kérheti a szenzor elhelyezésének mellőzését, rendszerszintű beállításának módosítását, ha az az elektronikus információs rendszer működését ellehetetleníti.

(3) A szenzor elhelyezésének, rendszerszintű beállításának módosítása esetén a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet az (1)-(2) bekezdés szerint jár el.

## 4. A honvédelmi ágazati korai figyelmeztető rendszer szolgáltatásának üzemeltetése és igénybevétele

**6. §** A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény és végrehajtására kiadott jogszabályok szerinti honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére a Katonai Nemzetbiztonsági Szolgálatot jelöli ki (a továbbiakban: honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet).

**7. §** A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet felelős a honvédelmi ágazati korai figyelmeztető rendszer kiépítésének koordinálásáért, a központi-, a köztes és a végponti elemei kiépítéséért, működtetéséért, az általa kezelt biztonsági jelzés, valamint az információs kapcsolatrendszerből származó, vagy azzal kapcsolatba hozható adat elemzéséért, értékeléséért, valamint a kiértékelés eredményétől függően riasztás kiadásáért a védett intézmény irányába.

**8. §** (1) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet
*a)* elemzi és értékeli a központi rendszerbe beérkező adatot,

*b)* korai szakaszban azonosítja a védett rendszerbe való behatolás kísérletét, és
*c)* azonosítja a fejlett támadási módszert hosszútávon alkalmazó támadást.

(2) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet a honvédelmi korai figyelmeztető szolgáltatás nyújtásának részletes szabályát a védett intézménnyel egyeztetve szolgáltatási szabályzatban rögzíti.

(3) A honvédelmi ágazati korai figyelmeztető rendszer működtetéséhez szükséges képzést a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet biztosítja.

**9. §** (1) A (2) bekezdésben foglalt kivétellel a honvédelmi ágazati korai figyelmeztető rendszer igénybevételére a honvédelmi célú elektronikus információs rendszert üzemeltető vagy használó szervezet jogosult.

(2) A honvédelmi célú elektronikus információs rendszert üzemeltető és használó szervezet számára a honvédelmi ágazati korai figyelmeztető rendszer bevezetése és használata a nyílt központi rendszerek vonatkozásában kötelező.

**10. §** A honvédelmi célú elektronikus információs rendszert üzemeltető biztosítja
*a)* a végponti elem üzemben tartását és rendelkezésre állását, valamint
*b)* a honvédelmi ágazati korai figyelmeztető rendszer működtetése érdekében a védett intézményben telepített rendszerelem, hálózati eszköz alapvető üzemeltetési feltételét.

**11. §** (1) A honvédelmi célú elektronikus információs rendszert üzemeltető a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet számára minden olyan, a rendszer felépítésével és a rendszeren nyújtott szolgáltatással kapcsolatos információt, valamint az abban bekövetkezett változást bejelent, amely a honvédelmi ágazati korai figyelmeztető rendszer működésére hatással van, azt korlátozná, kizárná vagy más módon ellehetetlenítené.

(2) A honvédelmi célú elektronikus információs rendszert üzemeltető – a (4) és az (5) bekezdésben foglalt kivételekkel – nem végezhet olyan rendszer-, illetve szolgáltatásfejlesztést, valamint nem hajthat végre olyan szervezeti átalakítást, amely a honvédelmi ágazati korai figyelmeztető szolgáltatás nyújtását előreláthatóan korlátozza, kizárja, vagy más módon ellehetetleníti.

(3) A (2) bekezdésben foglaltak teljesülése érdekében a honvédelmi célú elektronikus információs rendszert üzemeltető a rendszer-, illetve szolgáltatásfejlesztésről legkésőbb a fejlesztés tervezési szakaszát lezáró döntést megelőzően 15 nappal tájékoztatja a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezetet.

(4) A honvédelmi ágazati korai figyelmeztető szolgáltatás nyújtását előreláthatóan korlátozó, kizáró vagy azt más módon ellehetetlenítő rendszer-, illetve szolgáltatásfejlesztésről a (3) bekezdés szerinti tájékoztatással egyidőben a honvédelmi célú elektronikus információs rendszert üzemeltető egyeztetést kezdeményez.

(5) A honvédelmi ágazati korai figyelmeztető rendszert üzemeltető hozzájárul a (4) bekezdés szerinti rendszer- és szolgáltatásfejlesztéshez, ha annak elmaradása a honvédelmi célú elektronikus információs rendszert üzemeltető szervezet alapvető működését jelentősen korlátozná.

**12. §** (1) A honvédelmi ágazati korai figyelmeztető rendszerből a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet a (2) bekezdés szerinti adatot szolgáltatja
*a)* a szakfeladat szerint elkülönülő eseménykezelő központ,
*b)* a védett rendszer elektronikus információ biztonságáért felelős személy, szervezet, szervezeti egység,
*c)* a kibertér műveleti feladatot ellátó személy, szervezet, szervezeti egység, és
*d)* a Kormányzati Célú Elkülönült Hírközlő Hálózat hálózatgazdai feladatokat ellátó személy, szervezet
részére.

(2) Az (1) bekezdés szerinti személy, szervezet, szervezeti egység a felelősségi körébe tartozó riasztásra vonatkozóan jogosult megismerni
*a)* a honvédelmi ágazati korai figyelmeztető rendszer által előállított riasztási jelzést,
*b)* a vizsgált esemény állapotát, és
*c)* a honvédelmi célú elektronikus információs rendszer működésére, a vizsgált eseményre és a kiadott figyelmeztetésre vonatkozó időszakos, statisztikai adatot.

(3) Az eseménykezelési feladatát a szakfeladat szerint elkülönülő eseménykezelő központ szakmai irányítása és koordinációja alatt ellátó személy, szervezet, szervezeti egység részére a honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet a szakfeladat szerint elkülönülő eseménykezelő központ útján szolgáltat adatot.

(4) A honvédelmi korai figyelmeztető rendszert üzemeltető szervezet a (2) bekezdés *a)* pontja szerinti jelzésről haladéktalanul tájékoztatja a szakfeladat szerint elkülönülő eseménykezelő központot.

**13. §** (1) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet a hálózati forgalom kivonatát, a metaadatot, a biztonsági jelzést és a biztonsági naplóállományt legfeljebb öt évig tárolja.

(2) A honvédelmi ágazati korai figyelmeztető rendszer üzemeltetésére kijelölt szervezet az (1) bekezdés szerinti időtartam lejártát követően a honvédelmi ágazati korai figyelmeztető rendszerből törli az adatot.

## 5. Záró rendelkezések

**14. §** Ez a rendelet a kihirdetését követő 30. napon lép hatályba.

Orbán Viktor s.k.
miniszterelnök