5N | IT & SERVICE

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

állapot:2025. 02. 06.

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

KIRE VONATKOZIK:

E törvény kiberbiztonsági tanúsításra vonatkozó rendelkezéseit az információs és kommunikációs technológiai (a továbbiakban: **IKT) termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsításával kapcsolatos tevékenységre kell alkalmazni olyan szervezetek esetében, akik** Magyarország területén letelepedett vagy letelepedett képviselővel rendelkező (gazdálkodó) szervezetnek minősülnek és az alábbi kategóriákba esnek.

- **közigazgatási ágazathoz tartozó**
  - a fővárosi és vármegyei kormányhivatalok, a vármegyei közgyűlések hivatalai, a megyei jogú városok és a fővárosi kerületi önkormányzatok képviselő-testületének hivatalai
  - a települések képviselő-testületének hivatalai
- **többségi állami befolyás alatt álló** azon gazdálkodó és nem gazdasági szereplőként nyilvántartott **szervezetekre**, melyek törvény szerint meghaladják a középvállalkozásokra vonatkozó küszöbértékeket
- méretüktől függetlenül **az elektronikus hírközlési szolgáltatókra**
- törvények hatálya alá tartozó **közműszolgáltatók és közszolgáltatást nyújtó szervezetek**
- **kockázatos és kiemelten kockázatos** ágazatokban működő **szervezetekre**

KOCKÁZATOS ÁGAZATOK:

- **Postai és futárszolgálatok**
- **Kutatóhelyek**
- **Élelmiszer** (előállítás, nagykereskedelem, ipari termelés, feldolgozás és forgalmazás)
- **Hulladékgazdálkodás**
- **Vegyszer** előállító/gyártó és forgalmazó is
- **Gyártás** (Orvostechnikai eszközök és in vitro diagnosztikai ot. eszközök gyártása, Számítógép, elektronikai, optikai termék gyártása, Villamos berendezések gyártása, Máshova nem sorolt gépek és berendezések gyártása, Gépjárművek, pótkocsik és félpótkocsik gyártása, Egyéb szállítóeszközök gyártása, Cement-, mész-, gipszgyártás)
- **Digitális szolgáltatók** (online-piactér szolgáltatója, közösségi média szolgáltatási platform szolgáltatója, doménnév regisztrációt végző szolgáltató, keresőszolgáltató)

KIEMELTEN KOCKÁZATOS ÁGAZATOK:

- **energiaipar**
- **közlekedés**
- **egészségügy**
- **vízközmű szolgáltatók**
- **hírközlési és digitális infrastruktúra szolgáltatók**
- **űralapú szolgáltatások** nyújtását támogató földi infrastruktúra üzemeltető
- **Kihelyezett IKT szolgáltatások nyújtója:**
  - kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató
  - kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató

BESOROLÁSOK:

ALAPVETŐ SZERVEZETEK

Eredendően minden szervezet ide tartozik, de vannak kivételek
kivéve a 20 000 főt meg nem haladó lakosságszámú települések képviselő-testületének hivatalai

FONTOS SZERVEZETEK

a 20 000 főt meg nem haladó lakosságszámú települések képviselő-testületének hivatalai

JELENTŐS SZERVEZETEK

az általános kijelölő hatóság vagy a honvédelmi ágazati kijelölő hatóság által kijelölt olyan alapvető szolgáltatást nyújtó szervezet, amely elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához.

KRITIKUS SZERVEZETEK

olyan alapvető szolgáltatást nyújtó szervezet, amelyet a kijelölő hatóság a 2024. évi LXXXIV. törvény III. Fejezetben meghatározottak szerint kijelölt és elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához,

ALAPTÉTELEK

A törvény által előírt sérülékenységi vizsgálatokat és kiberbiztonsági incidenskezelésre vonatkozó szabályokat kell alkalmazni az érintett szervezetek elektronikus információs rendszerei esetében.

A szervezetek az elektronikus információs rendszer védelmének biztosítása érdekében **kötelesek az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított** – az informatikáért felelős miniszter, a honvédelmi miniszter vagy az SZTFH elnöke rendeletében meghatározott – **IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot használni.** Az egyes követelményeknek való megfelelés igazolására – ha rendelkezésre áll – európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat alkalmazható.

Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása vonatkozásában a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet.

A szervezet a kiberbiztonsági információk megosztása **meghatározott együttműködések megvalósítása céljából kiberbiztonsági információmegosztási megállapodásokat köthet.** A megállapodás megkötéséről, megállapodásban való részvételéről vagy annak felmondásáról tájékoztatni kell a kiberbiztonsági hatóságot.

Ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy **a közreműködő által** az elektronikus információs rendszerrel kapcsolatosan **ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek**

Az 1. § (1) bekezdés a) és c) pontja hatálya alá tartozó **fontos szervezet** rendelkezésében lévő elektronikus információs rendszerek vonatkozásában:

legalább az „alap" biztonsági osztályra irányadó követelményeket kell teljesíteni,

de nem kell teljesíteni:

teljes körű kockázatmenedzsment keretrendszer működtetése
hatáselemzés és kockázatmenedzsment tevékenységet;
biztonsági osztályba sorolást az elektronikus információs rendszereknél
kiválasztott védelmi intézkedések megfelelőségének értékelése,
legalább kétévente, a biztonsági osztályba sorolás felülvizsgálatával egyidejűleg hajtja végre

Az elektronikus információs rendszer biztonságáért felelős személyt megállapodás megkötése esetén is meg kell jelölni. Feladatait csak olyan személy végezheti, aki

- cselekvőképes, büntetlen előéletű
- kritikus szervezetként és jelentős szervezetként kijelölt szervezet esetében rendelkezik a feladatellátáshoz szükséges, előírt végzettséggel, szakképzettséggel, akkreditált nemzetközi képzettséggel vagy meghatározott szakterületen szerzett szakmai tapasztalattal.
- **nem jelölhető** ki vagy bízható meg **a szervezet gazdasági vezetői feladatait ellátó személy vagy az a személy, aki a szervezeten belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el**, illetve ilyen személy közvetlen alárendeltségébe tartozik. (kivéve: fontos szervezetek)

9. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER FEJLESZTÉSE

13. § (1) **Új elektronikus információs rendszerek fejlesztése, vagy már meglévő elektronikus információs rendszerek továbbfejlesztése** (a továbbiakban együtt: fejlesztés) **vonatkozásában** jelen alcím rendelkezéseit **kell alkalmazni alapvető szervezetnek minősülő szervezetek esetében**

13. § (3) A fejlesztés során **az elektronikus információs rendszer tervezési életciklusában végre kell hajtani** – ahol az adatosztályozási kötelezettséget e törvény előírja – a rendszerben kezelni tervezett **adatok osztályozását** és az elektronikus információs **rendszer biztonsági osztályba sorolását**, amelyet **a nemzeti kiberbiztonsági hatóságnak jóváhagyásra be kell nyújtani**

- belső fejlesztés esetén az erőforrások allokációját megelőzően
- külső fejlesztés esetén az arra irányuló szerződés megkötését megelőzően olyan módon, hogy a nemzeti kiberbiztonsági hatóság által jóváhagyott osztályba soroláshoz kapcsolódó és az információbiztonsági követelmények az elektronikus információs rendszer fejlesztésére irányuló szerződésbe rögzítésre kerüljenek.

13. § (8) Új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer továbbfejlesztése során a megállapított biztonsági osztályhoz tartozó **követelményeket a rendszer használatbavételéig teljesíteni kell.**

14. § (1) A 13. §-ban foglaltaktól eltérően, ha az elektronikus információs rendszer fejlesztése

- **alapvető szervezet által történik**, az alapvető szervezet köteles biztonsági osztályba sorolni az elektronikus információs rendszert és annak megfelelő védelmi követelményeket kell teljesíteni,

- **fontos szervezet által történik**, a fejlesztés során legalább az „alap” biztonsági osztálynak megfelelő védelmi követelményeket kell teljesíteni.

A „jelentős” és „magas” biztonsági osztályba tartozó elektronikus információs rendszer esetében kötelező a teljes körű sérülékenységvizsgálat kezdeményezése.

84. § Az Ibtv. szerinti 1. és 2. biztonsági osztály az „alap”, a 3. és 4. biztonsági osztály a „jelentős”, az 5. biztonsági osztály a „magas” biztonsági osztálynak felel meg.

AZ ELVÉGZENDŐ ÉRTÉKELÉSI TEVÉKENYSÉGEKNEK LEGALÁBB MAGUKBAN KELL FOGLALNIUK:

- **„alap” megbízhatósági szint** esetén
  - a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,
- **„jelentős” megbízhatósági szint** esetén
  - ba) a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,
  - bb) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát, és
  - bc) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően működteti-e a szükséges biztonsági funkciókat,
- „**magas” megbízhatósági szint** esetén
  - ca) a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,
  - cb) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát,
  - cc) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően, a legfejlettebb technika szerint működteti-e a szükséges biztonsági funkciókat, valamint
  - cd) behatolásvizsgálatok révén annak értékelését, hogy az mennyire ellenálló a jól képzett elkövetők által végrehajtott támadásokkal szemben.

86. § (1) Jelen törvény fejlesztésére vonatkozó előírásait kell alkalmazni az e törvény hatálybalépésekor még használatba nem vett fejlesztések esetében

- saját fejlesztésű, fejlesztés alatt álló rendszer esetében, amennyiben az erőforrásigényeket még nem fogadták el,
- külső fejlesztés alatt álló rendszer esetében, amennyiben a fejlesztésre irányuló beszerzési eljárást még nem írták ki, vagy a fejlesztésre irányuló szerződést még nem kötötték meg.

86. § (2) Ha a szervezet fejlesztett rendszere e törvény hatályba lépésekor túljutott az elektronikus információs rendszer fejlesztésének (1) bekezdésben meghatározott lépésein,
    - a szervezet – ha még nem végezte el, – 180 napon belül elvégzi az elektronikus információs rendszer biztonsági osztályba sorolását,
    - az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések teljesítésénél lehetősége van a 10. § (6) bekezdése szerinti fokozatos kivitelezésre, azzal, hogy a vonatkozó határidő számításának alapját e törvény hatálybalépésének napja képezi.