Milyen kiberbiztonsági incidensek esetén kötelező a hatósági bejelentés?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/3

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.23	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) és a végrehajtására kiadott jogszabályok alapján a kiberbiztonsági incidensek bejelentési rendje alapvetően két ágra oszlik. A jellemzően állami, vagy állami érdekeltségű kiemelt szervezetek (a törvényben felsorolt állami és önkormányzati szervek, többségi állami befolyás alatt álló bizonyos gazdálkodó szervezetek, a nemzeti kiberbiztonsági hatóság vagy a honvédelmi kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezetek, illetve a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok) teljes körű jelentéstételre kötelezettek. Nem csupán a tényleges incidenseket, hanem a kiberfenyegetéseket és az incidensközeli helyzeteket is haladéktalanul jelenteniük kell a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI) mint nemzeti kiberbiztonsági incidenskezelő központ felé. A honvédelmi célú elektronikus információs rendszereket érintő incidenseket pedig a Katonai Nemzetbiztonsági Szolgálat felé kell bejelenteni.

A kiemelten kockázatos, valamint a kockázatos ágazatokban működő, jellemzően a gazdálkodó szférába tartozó szervezetek (középvállalkozások, valamint bizonyos méret- illetve árbevételi/költségvetési bevételi feltételeket teljesítő szolgáltatók és szervezetek, valamint méretüktől függetlenül az elektronikus hírközlési szolgáltatók, a bizalmi szolgáltatók, a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartó vagy a doménnév-regisztrációt végző szolgáltatók) esetében a jogalkotó a jelentési kötelezettséget a jelentős kiberbiztonsági incidensekre korlátozza, azzal, hogy e szervezetek a nem jelentésköteles kiberbiztonsági incidenseket is bejelenthetik. Jelentősnek az az esemény minősül, amely a szervezet működésében súlyos zavart vagy vagyoni hátrányt okoz vagy másoknak okoz jelentős vagyoni vagy nem vagyoni kárt.

Azok a szervezetek vagy személyek, amelyek nem tartoznak sem a kiemelt, sem a nem kiemelt szervezetek körébe, önkéntes alapon bejelenthetik az olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket, illetve kiberbiztonsági incidenseket, amelyek jelentős hatást gyakorolnak vagy gyakorolhatnak a magyar kibertér biztonságára.

A 7/2024. (VI. 24.) MK rendelet értelmében minden érintett szervezet köteles belső jelentési mechanizmusokat kialakítani, az automatizált jelentési rendszerek alkalmazása azonban csak a Magas biztonsági osztályba sorolt rendszereknél kötelező.

2. A VIZSGÁLANDÓ KÉRDÉS

Milyen kiberbiztonsági incidenseket kell bejelenteni a hatóságnak,

A) A kiemelten kockázatos, valamint a kockázatos ágazatokban működő szervezetek esetében (Kiberbiztonsági tv. 1. § (1) bekezés d) és e) pont alá tartozó szerveztek);

B) A kiemelt szervezetek esetében (Kiberbiztonsági tv. 1. § (1) bekezés a), b), c) és f) pont alá tartozó szerveztek) estében?

3. VÁLASZ

3.1 Bejelentendő incidensek köre

A törvényi szabályozás markáns különbséget tesz a bejelentési kötelezettség terjedelmét illetően egyrészről a kiemelt, másrészről pedig a kiemelten kockázatos, valamint a kockázatos ágazatokban működő szervezetek között.

3.2 A kiemelten kockázatos, valamint a kockázatos ágazatokban működő szervezetek bejelentési kötelezettsége

Jelen állásfoglalásban kiemelten kockázatos, valamint a kockázatos ágazatokban működő szervezetnek a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pont hatálya alá tartozó szervezeteket nevezzük.

E szervezetek körét a Kiberbiztonsági tv. az alábbiak szerint határozza meg: kiemelten kockázatos, valamint a kockázatos ágazatokban működő

- középvállalkozások,
- azon szervezetek, amelyeknek vagy az összes foglalkoztatotti létszáma az 50 főt eléri vagy meghaladja, vagy pedig az éves nettó árbevétele vagy éves költségvetési bevételi előirányzata meghaladja a 10 millió eurónak megfelelő forintösszeget, és mérlegfőösszege meghaladja a 10 millió eurónak megfelelő forintösszeget,
- méretüktől függetlenül elektronikus hírközlési szolgáltató, bizalmi szolgáltató, DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó vagy doménnév-regisztrációt végző szolgáltató tevékenységet folytató szervezetek.

Kiemelten kockázatos ágazatnak minősül az energetika, közlekedés, egészségügy, ivóvíz és szennyvíz, hírközlés, digitális infrastruktúra, kihelyezett IKT szolgáltatás, valamint az űralapú szolgáltatás; míg kockázatos ágazatnak minősül a postai és futárszolgálat, az élelmiszerelőállítás, -feldolgozás és -forgalmazás, a hulladékgazdálkodás, vegyszerek előállítása és forgalmazása, különböző gépek, berendezések gyártása, a digitális szolgáltatók és a kutatás.

Ezen szervezetek esetében a jogalkotó szűkebb körű, az esemény súlyosságához kötött kötelező bejelentést ír elő. Nem kell minden kisebb zavart jelenteni, kizárólag azokat, amelyek jelentős hatással bírnak a működésre vagy harmadik felekre.

A törvény értelmében ezen szervezetek kötelesek bejelenteni azokat a fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és a kiberbiztonsági incidenseket – beleértve az üzemeltetési incidenseket is –, amelyek:

- súlyos zavart okoznak a szervezet működésében vagy a szolgáltatásnyújtásban;
- vagyoni hátrányt okoznak a szervezetnek;
- jelentős vagyoni vagy nem vagyoni kárt okoznak más természetes vagy jogi személyek számára.

> *„Az 1. § (1) bekezdés d) és e) pontja szerinti szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és*

kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is –, amelyek a szervezet működésében vagy az általa végzett szolgáltatásnyújtásban súlyos zavart vagy vagyoni hátrányt okoz, illetve jelentős vagyoni vagy nem vagyoni kárt okoz más természetes vagy jogi személyek számára kötelesek a kormányrendeletben meghatározottak szerint bejelenteni a nemzeti kiberbiztonsági incidenskezelő központ részére."
[2024. évi LXIX. törvény 66. § (2) bekezdés]

Fontos kiemelni, hogy bár nem kötelező, ezen szervezetek jogosultak azokat a kiberbiztonsági incidenseket is bejelenteni, amelyek nem érik el a fenti súlyossági küszöböt. Ez a lehetőség csak a kiberbiztonsági incidensekre vonatkozik, a fenyegetésekre, kiberbiztonsági incidensközeli helyzetekre nem.

„Az 1. § (1) bekezdés d) és e) pontja szerinti szervezetek a (2) bekezdés szerinti kiberbiztonsági incidensnek nem minősülő kiberbiztonsági incidenst önkéntesen jelenthetik a nemzeti kiberbiztonsági incidenskezelő központ részére."
[2024. évi LXIX. törvény 66. § (3) bekezdés]

3.3 A jellemzően állami, vagy állami érdekeltségű kiemelt tartozó szervezetek bejelentési kötelezettsége

Ebbe a körbe tartoznak

- az ún. közigazgatási ágazathoz tartozó szervezetek (központi államigazgatási szervek, a törvényben nevesített egyéb állami szervezetek (pl. köztársasági elnök hivatala, Országgyűlés Hivatala, Alkotmánybíróság Hivatala, bíróságok, ügyészségek, Magyar Nemzeti Bank, Magyar Honvédség), az önkormányzati szervek, az állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal informatikai és elektronikus hírközlési szolgáltatást nyújtó ún. központi szolgáltató, továbbá az ún. központi rendszer [Kiberbiztonsági tv. 4. § 60. pont] felett rendelkezési jogot gyakorló szervezet;
- a többségi állami befolyás alatt álló egyes gazdálkodó szervezetek (a kiemelten kockázatos, valamint a kockázatos ágazatokban működő szervezetekre vonatkozó létszám és bevételi feltételek szerint);
- a nemzeti kiberbiztonsági hatóság vagy a honvédelmi kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezetek, valamint
- a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok. (Kiberbiztonsági tv. 1. § (1) bekezdés a), b), c) és f) pont hatálya alá tartozó szervezetek)

Ezen szervezetek esetében a jogalkotó teljes körű jelentési kötelezettséget ír elő. Ez azt jelenti, hogy nemcsak a már bekövetkezett és kárt okozó incidenseket kell jelenteni, hanem a potenciális veszélyeket és a "majdnem" incidenseket is.

A bejelentési kötelezettség az alábbi három kategóriára terjed ki:

- Fenyegetések, aza olyan körülmények, amelyek potenciálisan kárt okozhatnak.
- Kiberbiztonsági incidensközeli helyzetek, olyan események, amelyek kárt okozhattak volna, de sikerült megakadályozni, vagy szerencsés véletlen folytán nem következtek be.
- Kiberbiztonsági incidense, ténylegesen bekövetkezett események (beleértve az üzemeltetési hibából eredőket is).

> *„Az 1. § (1) bekezdés a)–c) és f) pontja szerinti szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is – a nemzeti kiberbiztonsági incidenskezelő központ részére kötelesek haladéktalanul, a [418/2024. (XII. 23.) Korm. rendeletben] meghatározottak szerint bejelenteni.” [2024. évi LXIX. törvény 66. § (1) bekezdés]*

Honvédelmi célú elektronikus információs rendszer esetében, bár a bejelentési kötelezettség tárgya megegyezik a többi szervezetével, a címzett eltér. Az említett esetekben nem a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI), hanem a Katonai Nemzetbiztonsági Szolgálat a hatáskörrel rendelkező szerv.

> *„A honvédelmi célú elektronikus információs rendszert érintő fenyegetést, kiberbiztonsági incidensközeli helyzetet és kiberbiztonsági incidenst a szervezet a Kormány rendeletében meghatározott honvédelmi kiberbiztonsági incidenskezelő központnak [jelenleg a Katonai Nemzetbiztonsági Szolgálat] jelenti be.”*
> *[2024. évi LXIX. törvény 66 § (4) bekezdés]*

3.4 Fogalommeghatározások

A jogszabályi megfeleléshez elengedhetetlen a bejelentendő események pontos jogi definíciójának ismerete.

Kiberbiztonsági incidensnek minősülnek nemcsak a rosszindulatú támadások, hanem a véletlen események vagy mulasztások is ide tartoznak, ha azok a bizalmasságot, sértetlenséget vagy rendelkezésre állást veszélyeztetik.

> *„Kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;”*
> *[2024. évi LXIX. törvény 4. § 46. pont]*

A törvény ismeri a jelentős kiberbiztonsági incidens fogalmát is

> *„Jelentős kiberbiztonsági incidens:*

a) a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,
b) közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely
ba) a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;
bb) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy
bc) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;"

[2024. évi LXIX. törvény 4. § 40. pont]

A kiberbiztonsági incidensközeli helyzet fogalma a "majdnem" baleseteket fedi le, amelyek kezelése a közszférában kötelező a prevenció érdekében.

„Kiberbiztonsági incidensközeli helyzet: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;" [2024. évi LXIX. törvény 4. § 49. pont]

Kiberfenyegetés olyan potenciális esemény, amely kárt okozhat.

„Kiberfenyegetés: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat;" [2024. évi LXIX. törvény 4. § 50. pont, utalva az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalomra]

A törvény ismeri a jelentős kiberfenyegetés fogalmát is:

„Jelentős kiberfenyegetés: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;"
[2024. évi LXIX. törvény 4. § 41. pont

3.5 Védelmi intézkedések a 7/2024. (VI. 24.) MK rendelet alapján

A 7/2024. (VI. 24.) MK rendelet 2. melléklete konkrét védelmi intézkedéseket ír elő a szervezetek számára, amelyek támogatják az incidensek felismerését és jelentését. Ezek a követelmények a biztonsági osztálytól függően (Alap - A, Jelentős - J, Magas - M) kötelezőek.

A rendelet előírja, hogy a szervezetnek köteleznie kell a személyzetet a gyanús események jelentésére, és jogszabályi kötelezettség esetén a hatóság felé is jelenteni kell. Ez a követelmény minden biztonsági osztály számára kötelező.

> *„9.27. A szervezet:*
> *9.27.1. Kötelezi a személyzetet arra, hogy jelentse a biztonsági esemény gyanúját vagy bekövetkeztét.*
> *9.27.2. Jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározott szervek felé.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 9.27. pont (A, J, M)]*

Az automatizált jelentési mechanizmusok alkalmazása csak a Magas biztonsági osztályba sorolt rendszerek esetén kötelező, Alap és Jelentős szinten opcionális.

> *„9.28. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági események bejelentésének támogatására.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 9.28. pont (M)]*

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről