Milyen információkat kell a hatóságnak bejelenteni kiberbiztonsági incidens esetén?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/4

VERZIÓKÖVETÉS

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

1. VEZETŐI ÖSSZEFOGLALÓ

Jelen dokumentum a magyar szervezetek számára nyújt hiteles iránymutatást a kiberbiztonsági incidensek hatósági bejelentési rendjéről, a 2024. évi LXIX. törvény (Kiberbiztonsági tv.) és a végrehajtására kiadott 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.) előírásai alapján. A szabályozás célja a nemzeti kibertér ellenálló képességének növelése gyors és strukturált információcsere révén.

A bejelentési folyamat több kötelező, határidőhöz kötött lépcsőből áll:

- Korai riasztás (legkésőbb 24 órán belül), az incidensről való tudomásszerzést követően haladéktalanul, de legkésőbb 24 órán belül "első bejelentést" kell tenni a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI), a honvédelmi célú elektronikus információs rendszereket érintő események esetén a Katonai Nemzetbiztonsági Szolgálat felé. Ennek célja a gyors riasztás, még minimális információk birtokában is.
- Fertőzöttségi mutatók bejelentése, a Vhr. külön nevesíti a fertőzöttségi mutatók bejelentésére vonatkozó kötelezettséget, amelyet akkor kell közölni, „amint rendelkezésre állnak”. A jogszabály szövegéből az következik, hogy ez a bejelentési kötelezettség független a többi bejelentéstől.
- Eseménybejelentés (legkésőbb 72 órán belül), a második fázisban egy részletesebb jelentés benyújtása szükséges, amely tartalmazza az incidens súlyosságának értékelését, a hatásokat. Fontos, hogy a technikai paraméterek (pl. SHA-256 lenyomatok, IP-címek) megosztása kritikus a védekezéshez.
- Zárójelentés (1 hónapon belül), az előző pontban írt jelentést követő 1 hónapon belül zárójelentést kell benyújtani, amely a kiváltó okokat és a jövőbeli kockázatcsökkentő intézkedéseket összegzi. Ha ebben az időpontban még folyamatban van a kiberbiztonsági incidens, az addig elért eredményekről kell jelentést benyújtani, és a zárójelentésaz incidens kezelését követő egy hónapon belül nyújtandó be.

Amennyiben az incidens elhúzódik, vagy a hatóság kéri, közbenső helyzetjelentés készítése is kötelező. Kiemelt jelentőségű vagy nagy kiterjedésű incidens esetén a jogszabály a szakrendszeri bejelentés mellett az azonnali telefonos tájékoztatást is előírja. A bejelentések elsődleges csatornája az NKI által üzemeltetett szakrendszer (incidens.nki.gov.hu). A szervezeteknek saját incidenskezelési tervüket ezen határidőkhöz kell igazítaniuk a jogszabályi megfelelés biztosítása érdekében.

2. A VIZSGÁLANDÓ KÉRDÉS

Milyen információkat kell a hatóságnak bejelenteni kiberbiztonsági incidens esetén?

3. VÁLASZ

A kiberbiztonsági incidens bejelentésének kötelező tartalmi elemeit a 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.) 77. §-a határozza meg. A bejelentési kötelezettség a szervezetet terheli, amelyet a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (a továbbiakban: NKI, a Vhr. alkalmazásában: Központ) részére kell teljesíteni.

> *77. § (1) A Kiberbiztonsági tv. 66. §-a szerinti bejelentés keretében a szervezet benyújt a Központ részére: [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés]*

A bejelentést az NKI által meghatározott módon, elektronikus úton, a Központ által üzemeltetett szakrendszeren (incidens.nki.gov.hu) keresztül kell megtenni, de elfogadható e-email vagy telefonos forma is.

> *A fenyegetés, a kiberbiztonsági incidensközeli helyzet és a kiberbiztonsági incidens bejelentése a Központ – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági incidenskezelő központ – által meghatározott módon, elektronikus úton – amennyiben elérhető, a Központ által meghatározott elektronikus felületen – történik. Ha a szervezet elektronikus információs rendszere oly mértékben sérül, hogy az elektronikus úton történő bejelentés nem lehetséges, a bejelentés bármely más módon is megtehető. [418/2024. (XII. 23.) Korm. rendelet 78. § (1) bekezdés]*

A felület elérhetősége és bővebb infromáció:
https://incidens.nki.gov.hu vagy **https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/**

3.1 Az incidens bejelentés szakaszai

3.1.1 Az első bejelentés (24 órán belül)

A folyamat első lépése az „első bejelentés”, amelyet a tudomásszerzéstől számított legkésőbb 24 órán belül kell megtenni. Ennek célja a gyors riasztás és az alapvető információk átadása.

> *1. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül egy első bejelentést, amelyben – amennyiben az információk rendelkezésre állnak – fel kell tüntetni [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. pont]*

Az első bejelentésnek – amennyiben az információk rendelkezésre állnak – az alábbi adatokat kell tartalmaznia:

- az érintett elektronikus információs rendszer megjelölését;

- a kiberbiztonsági incidens rövid leírását, annak jelzésével, hogy az incidens üzemeltetési kiberbiztonsági incidensnek minősül-e;
- a kiberbiztonsági incidens státuszát;
- a kiberbiztonsági incidens időtartamát;
- a szolgáltatás helyreállításának várható időpontját;
- a kiberbiztonsági incidens által érintett adatok fajtáját, jellegét;
- a kiberbiztonsági incidens által érintett felhasználók számát;
- a szolgáltatás működésében támadt zavar mértékét;
- a kiberbiztonsági incidens kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit;
- közvetítő szolgáltató vagy központi szolgáltató igénybevétele esetén a közvetítő szolgáltató vagy központi szolgáltató megnevezését, elérhetőségét;
- annak jelzését, hogy a kiberbiztonsági incidens szándékolt incidensnek minősül-e;
- a kiberbiztonsági incidens által érintett terület földrajzi kiterjedését;
- annak jelzését, hogy lehet-e a kiberbiztonsági incidensnek határokon átnyúló hatása;
- minden olyan információt, amely lehetővé teszi a Központ (NKI) számára, hogy meghatározza az esemény határokon átnyúló hatásait;

> *(1) A Kiberbiztonsági tv. 66. §-a szerinti bejelentés keretében a szervezet benyújt a Központ részére: 1. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül egy első bejelentést, amelyben – amennyiben az információk rendelkezésre állnak – fel kell tüntetni(...) a)-n) alpontok*
> *[418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. pont a)-n) alpont]*

3.1.2 A fertőzöttségi mutatók bejelentése

Amint rendelkezésre állnak, be kell jelenteni a fertőzöttségi mutatókat.

A fertőzöttségi mutatók (angolul: Indicators of Compromise vagy IoC) a kiberbiztonságban olyan digitális nyomokat, jeleket vagy bizonyítékokat jelentenek, amelyek arra utalnak, hogy egy rendszerbe illetéktelenek hatoltak be, vagy azt kártékony szoftver fertőzte meg.

> *(1) A Kiberbiztonsági tv. 66. §-a szerinti bejelentés keretében a szervezet benyújt a Központ részére: (...) 2 . amint rendelkezésre állnak, a fertőzöttségi mutatókat*
> *[418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 2. pont]*

A gyakorlatban ilyen mutatók ezek például:

- Kártékony fájlok lenyomatai (Hash, egy vírus vagy malware egyedi digitális „ujjlenyomata” (SHA-256 kód).
- Hálózati címek, azok az IP-címek, URL-ek vagy domain nevek, ahonnan a támadás érkezett, vagy ahová a fertőzött gép adatokat próbál küldeni (C2 – Command & Control szerverek).
- Fájlútvonalak, ahol a kártékony kód a rendszerben elrejtőzött.
- Rendszermódosítások, a regisztrációs adatbázisban (registry) végzett gyanús módosítások, új, ismeretlen felhasználói fiókok létrehozása.

A 418/2024. (XII. 23.) Korm. rendelet azért írja elő ezek kötelező jelentését, mert ezek az információk a legértékesebbek a védekezés szempontjából. Segítenek az NKI-nak beazonosítani, hogy milyen típusú támadásról van szó (pl. egy ismert zsarolóvírus-kampány része-e). Ha az NKI megkapja ezeket a mutatókat, figyelmeztetni tud más szervezeteket is, hogy blokkolják az adott IP-címet vagy keressék az adott fájlt, így megakadályozható a támadás továbbterjedése. A jogszabály ezen információk fontosságára tekintettel elválasztja ezt a bejelentést más bejelentésektől (pl. a korai riasztástól vagy a 72 órán belüli eseményjelentéstől, és előírja, hogy a bejelentésnek meg kell történnie „amint rendelkezésre állnak” a fertőzöttségi mutatók.

3.1.3 Eseménybejelentés (72 órán belül)

A következő lépés az úgynevezett „eseménybejelentés”, amely frissíti az első bejelentés adatait és tartalmazza az incidens első értékelését.

> *3. Indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja az 1. pontban említett információkat, és tartalmazza az incidens első értékelését, beleértve annak súlyosságát és hatását; [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 2. pont]*

3.1.4 Közbenső helyzetjelentés

A „közbenső helyzetjelentés a kiberbiztonsági incidens-bejelentési folyamat egy speciális, nem automatikus eleme. Ez a jelentés a folyamatos kapcsolattartást szolgálja súlyos vagy elhúzódó incidensek esetén, biztosítva, hogy a hatóság naprakész képpel rendelkezzen a kockázatokról.

Míg a 24 órás (első) és a 72 órás (esemény) bejelentés minden jelentős incidensnél kötelező, addig ez a jelentéstípus csak külön felhívásra válik esedékessé.

Ezt a jelentést akkor kell elkészíteni, ha a hatóság (a Nemzeti Kiberbiztonsági Intézet) ezt kifejezetten kéri. Általában az első bejelentés (24 óra) és a zárójelentés (1 hónap) közötti időszakban, az incidens elhárítása közben fordulhat elő.

Mivel ez egy helyzetjelentés, a tartalma az aktuális szituációtól függ, de jellemzően a korábbi bejelentések óta történt változásokra fókuszál. Lehetséges tartalom:

- Státuszfrissítés, hol tart az elhárítás? Sikerült-e izolálni a támadót?
- Új információk, felmerültek-e új fertőzöttségi mutatók ?
- Hatásváltozás: súlyosbodott-e az incidens hatása (pl. több adat szivárgott ki, nőtt a kiesés ideje)?
- Kérdések megválaszolása, az NKI által feltett konkrét technikai kérdésekre adott válaszok.

3.1.5 Zárójelentés (egy hónapon belül)

A folyamat lezárása a „zárójelentés", amelyet – tipikus esetben - legkésőbb a 3.1.3. pontban írt eseménybejelentést követő egy hónapon belül kell benyújtani.

> *5. zárójelentést, legkésőbb a 3. pont szerinti eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:*
> *a) a kiberbiztonsági incidens részletes leírása, beleértve annak súlyosságát és hatását,*
> *b) a kiberbiztonsági incidenst valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa,*
> *c) alkalmazott és folyamatban lévő mérséklési intézkedések,*
> *d) adott esetben a kiberbiztonsági incidens határokon átnyúló hatása;*
> *[418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 5. pont]*

Amennyiben az incidens a jelentés benyújtásának időpontjában még folyamatban van, zárójelentés helyett újabb közbenső helyzetjelentést kell adni.

> *6. ha a zárójelentés benyújtásának időpontjában még folyamatban van a kiberbiztonsági incidens, az addig elért eredményekről szóló jelentést;*
> *[418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 6. pont]*

Ebben az esetben a végleges lezárást követően kell benyújtani a zárójelentést.

> *7. a 6. pont szerinti esetben a kiberbiztonsági incidens kezelését követő egy hónapon belül egy zárójelentést. [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 7. pont]*

3.2 Kiemelt jelentőségű incidensek

Jelentős vagy nagy kiterjedésű incidens esetén a jogszabály előírja a rövid úton (azaz telefonon) történő tájékoztatást is.

> *Jelentős vagy nagykiterjedésű kiberbiztonsági incidens esetén a szervezet a bejelentést a Központ felé haladéktalanul rövid úton, telefonon is megteszi.*
> *[418/2024. (XII. 23.) Korm. rendelet 78. § (2) bekezdés]*

A telefonos bejelentésre használható telefonszámok a következő oldalon érhetőek el: **https://nki.gov.hu/intezet/tartalom/Kapcsolat/** (Incidensbejelentés rész).

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról