

**Puskás Tivadar Közalapítvány CERT-Hungary  
Nemzeti Hálózatbiztonsági Központ**

**INCIDENSKEZELÉSI ELJÁRÁSREND**

Az eljárásrend hatályának kezdőnapja:	2010. július 1.
Verziószám:	v2
Oldalak száma:	10
Copyright Puskás Tivadar Közalapítvány	Minden jog fenntartva
Jóváhagyta:	Bódi Gábor ügyvezető igazgató
Jóváhagyás dátuma:	2010. június 30.

## Verziókövetés

Verziószám	Változás leírása	Hatálybalépés dátuma
v1		2010. január 5.
v2		2010. július 1.

# Tartalomjegyzék

1. Az incidens bejelentése.....	6
2. Sorrendbe állítás (priorizálás).....	7
3. Bejelentés visszaigazolása.....	7
4. Az incidenskezelés/koordináció folyamata.....	8
5. Az incidens lezárása.....	9
6. Technikai információk, Irányelvek, felelősség.....	10

## Adatok, elérhetőség

**Puskás Tivadar Közalapítvány  
CERT-Hungary  
Nemzeti Hálózatbiztonsági Központ**

**Képviseli:** Bódi Gábor ügyvezető igazgató  
**Székhely:** 1063 Budapest, Munkácsy M. u. 16.  
**Telephely:** 1063 Budapest, Munkácsy M. u. 22.  
**Nyilvántartási szám:** Fővárosi Bíróság 9222.  
**Adószám:** 18044380-2-42  
**Telefon:** 0036 (1) 301-2080  
**Fax:** 0036 (1) 353-1937  
**E-mail:** [info@cert-hungary.hu](mailto:info@cert-hungary.hu)  
**Web:** [www.cert-hungary.hu](http://www.cert-hungary.hu)

## **Bevezetés**

Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X.14.) Kormányrendelet 9. § (1) a) és b) pontja határozza meg a Nemzeti Hálózatbiztonsági Központ (NHBK) szolgáltatásai közül az internetet támadási csatornaként felhasználó beavatkozások kezelését és elhárításának koordinálását, azaz az incidenskezelési szolgáltatást:

„ 9. § (1) A Központ szolgáltatásai:

a) A Központ a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúravédelmi szervezetek felé magyar Nemzeti Kapcsolati Pontként (a továbbiakban: NKP), kormányzati számítástechnikai sürgősségi reagáló egységként (kormányzati CERT) működik, folyamatos rendelkezésre állással;

b) A Központ, mint NKP ellátja a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé az internetet támadási csatornaként felhasználó beavatkozások kezelését és elhárításának koordinálását;”

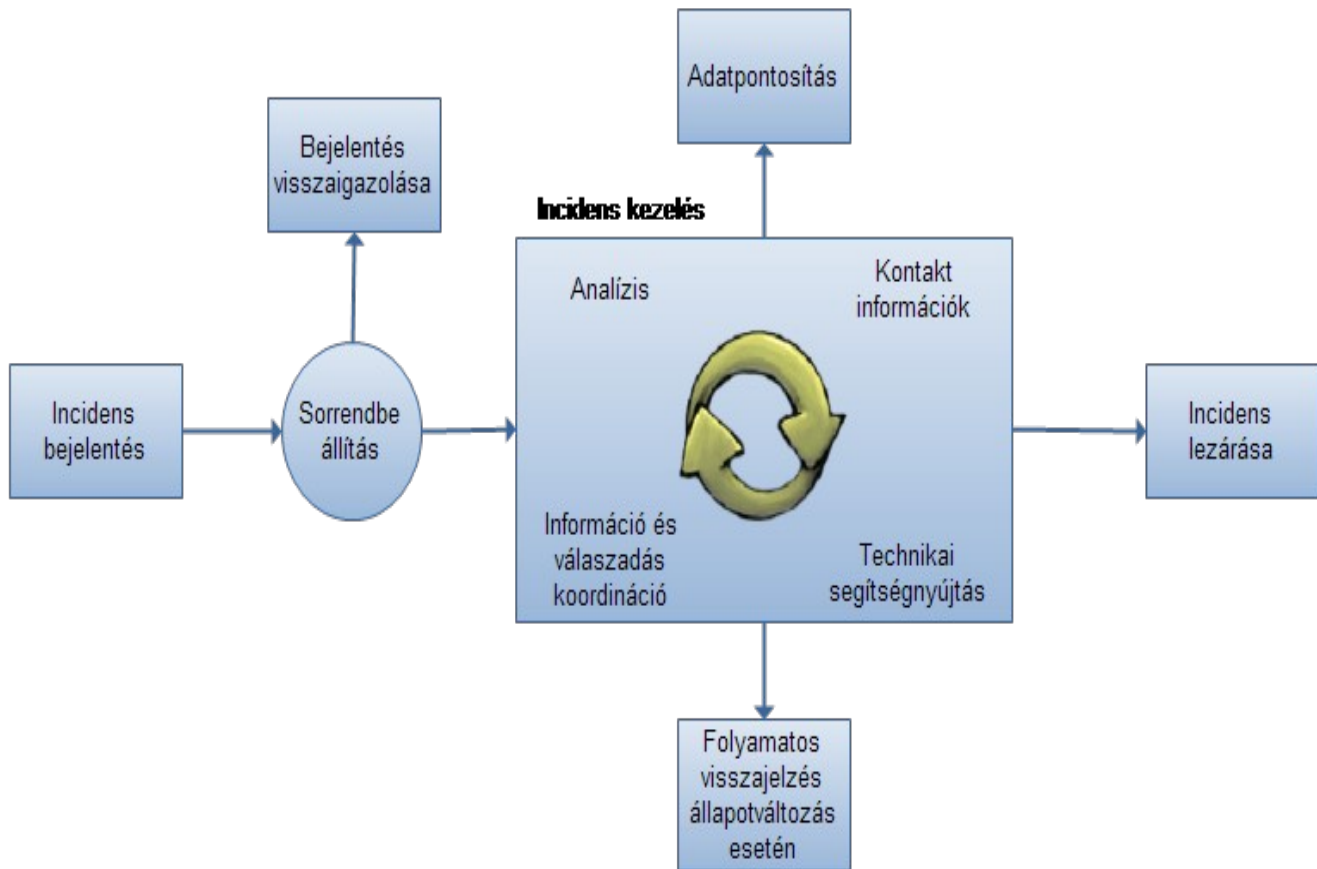
Jelen dokumentum célja, hogy a Nemzeti Hálózatbiztonsági Központ incidens-kezelési szolgáltatását igénybe vevők (a továbbiakban: Bejelentő/Megrendelő) megbízható információkhoz jussanak az incidenskezelés folyamatáról, az NHBK által végrehajtott lépésekről, illetve azokról a szolgáltatási paraméterekről, amelyek az incidenskezelés során előtérbe kerülnek.

*Incidens:* bármely, a Bejelentő / Megrendelő informatikai rendszerét az internet felől fenyegető rosszindulatú megnyilvánulás és a Bejelentő / Megrendelő internet alapú szolgáltatásainak működését gátló vagy eltérítő próbálkozás (így különösen az IT eszközökkel megkísérelt csalás, a szolgáltatás megtagadás támadások, a behatolási próbálkozások, adathalászat, személyiség lopás.)

*Incidenskezelés:* az incidensek észlelésének, analizálásának, helyreállításának a szervezett folyamata, amelynek célja a károk minimalizálása és a további károk elkerülése.

A Nemzeti Hálózatbiztonsági Központ a hálózatbiztonsági központok világszervezetének (FIRST - Forum of Incident Response Teams) és európai szervezetének (TF-CSIRT) akkreditációja (Trusted Introducer) révén az Incidensek nemzetközi szinten történő kezelése során kizárólag a [www.first.org/members/teams](http://www.first.org/members/teams) honlapon feltüntetett tagországokkal történő együttműködését biztosítja.

Az alábbi ábra és folyamatleírás a Nemzeti Hálózatbiztonsági Központ nyilvános incidenskezelési eljárásrendjét mutatja be:



**Az incidenskezelés folyamatábrája**

## **1. Az incidens bejelentése**

A Nemzeti Hálózatbiztonsági Központ ügyelete az év minden napján a nap 24 órájában fogadja az incidens bejelentéseket. Informatikai biztonsági incidenseket elsősorban a [cert@cert-hungary.hu](mailto:cert@cert-hungary.hu) elektronikus levelezési címen fogadunk, de lehetőség van telefonon (0036 (1) 301 2079) vagy faxon (0036 (1) 353 1937) is bejelentést tenni.

## **2. Sorrendbe állítás (priorizálás)**

A Nemzeti Hálózatbiztonsági Központ a beérkezett incidens bejelentések alapján minden esetben a következő prioritási sorrendet követi:

1. Hazai kritikus információs infrastruktúrákat – elsősorban kormányzati központi rendszereket - fenyegető incidensek
2. Szerződéses partnerek információs infrastruktúráját fenyegető incidensek
3. Nemzetközi partnerek, partnerszervezetek által bejelentett vagy őket fenyegető incidensek
4. Együttműködő szervezetek által bejelentett vagy őket fenyegető incidensek
5. Egyéb (mint például lakossági bejelentések, segítségkérések)

## **3. Bejelentés visszaigazolása**

3.1. A Nemzeti Hálózatbiztonsági Központ - a bejelentéstől számított 4 órán belül - minden esetben visszajelzést ad írásban (e-mailben vagy faxon) a bejelentés fogadásáról a Bejelentő/Megrendelő felé, amelyben tájékoztatást kap a szükséges intézkedések megtétele felől (angol vagy magyar nyelven).

3.2. Amennyiben a Bejelentő/Megrendelő az NHBK által a visszajelzésben kért szükséges intézkedéseket nem tette meg, vagy a kért szükséges információkat az NHBK-nak nem adta meg, az NHBK nem vállal felelősséget az incidenskezelés teljesítéséért.

A Bejelentő/Megrendelő felelősséggel tartozik az NHBK-nak adott utasításokért, az átadott adatokért. Amennyiben bármilyen kár keletkezik a Bejelentőnek / a Megrendelőnek az NHBK felé tett utasításából, tájékoztatásából, annak ellenére, hogy azok szakszerűtlenségére az NHBK a figyelmet felhívta, azért az NHBK nem felelős.

3.3. A bejelentéssel a Bejelentő / Megrendelő hozzájárulását adja, hogy az NHBK az incidenssel érintett adatokhoz, információkhoz hozzáférjen, azokat kezelje, az NHBK által az incidenskezelés eljárásba bevont hazai és nemzetközi szervezetek részére továbbítsa. Az eljárásba az NHBK hazai részről a CERT szervezeteket, valamint a Nemzeti Nyomozóirodát, nemzetközi részről a [www.first.org](http://www.first.org) oldalon mindenkor található CERT tagokat jogosult bevonni.

Az NHBK az adatok kezelése során „A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról” szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően jár el.

#### **4. Az incidenskezelés/koordináció folyamata**

4.1. Az incidenskezelési/koordinációs folyamat azzal kezdődik, hogy az NHBK a bejelentés adatait megvizsgálja, megállapítja az incidenst, illetve analizálja az adatokat (pl. a bejelentett IP címek lokalizálása)

4.2. Amennyiben az incidenskezelési/koordinációs intézkedések megtételéhez további információk szükségesek vagy a meglévő információk pontosítása szükséges, úgy az NHBK felveszi a Bejelentővel /Megrendelővel a kapcsolatot adatpontosítás céljából. Az NHBK nem vállal felelősséget az incidenskezelés sikertelenségért, illetve a Bejelentőt / Megrendelőt az incidenskezeléssel összefüggésben ért kárért, amennyiben az bizonyíthatóan abból adódik, hogy a Bejelentő / Megrendelő az incidenskezeléshez szükséges információkat az NHBK részére nem vagy késedelmesen adta meg.

4.3. A pontos információk alapján meghatározásra kerül az incidensben érintettek köre, akik felé, valamint az incidenskezelésbe bevont hazai és nemzetközi szervezetek felé az NHBK megteszi a szükséges incidens kezelési lépéseket (pl. a releváns információk eljuttatása, intézkedések megtételére való felszólítás, stb.)

4.4. Ameddig az incidens nincs lezárva, az NHBK folyamatosan nyomon követi az incidensek állapotának változásait, amelyről folyamatosan, legalább 24 óránként értesítést küld a Bejelentő / Megrendelő felé.

## **5. Az incidens lezárása**

- 5.1. Egy incidens akkor tekinthető lezártnak, ha az incidens kezelésében érintettek visszajeleznek a Nemzeti Hálózatbiztonsági Központ felé, hogy a bejelentés tárgyát képező problémát megoldották, és / vagy a Nemzeti Hálózatbiztonsági Központ úgy értékeli, hogy az adott incidens megoldódott (például a káros tartalmat eltávolították az érintett oldalról). Az incidens lezárásának tényéről az NHBK az incidens lezárását követő 4 órán belül írásban tájékoztatja mind a Bejelentőt/Megrendelőt, mind pedig az incidens kezelésében érintetteket.
- 5.2. Az incidens lezárását követően az NHBK az incidenskezelési folyamat egészéről 3 munkanapon belül Összefoglaló jelentést készít, amelyben az incidens kezelésével kapcsolatos tevékenységét és annak eredményét rögzíti.
- 5.3. Az NHBK a Bejelentőtől/Megrendelőtől kapott dokumentumokat, adathordozókat hiánytalanul visszaszolgáltatja, a Bejelentőt/Megrendelőt közvetlenül érintő (pl. user info) védett adatokat a saját eszközeiről törli.
- 5.4. A Bejelentő/Megrendelő által tett bejelentésnek kizárólag azon része, amely a Bejelentőt/Megrendelőt közvetlenül érintő védett információkat nem tartalmaz, az NHBK incidenskezelési ún. ticketing adatbázis rendszerében (RTIR) - ügykezelési és statisztikai felhasználás céljából - tárolásra kerül.

## **6. Technikai információk, Irányelvek, felelősség**

- 6.1. Az incidens bejelentési pontra ([cert@cert-hungary.hu](mailto:cert@cert-hungary.hu) címre) küldött e-mail csak abban az esetben tekinthető bejelentettnek a Nemzeti Hálózatbiztonsági Központ incidens kezelési informatikai rendszerébe, ha a bejelentésre válaszul küldött (angol nyelvű) megerősítő üzenetre a Bejelentő/Megrendelő válaszol. Ez az ellenőrzés azért került bevezetésre, hogy a bejelentési ponton elkerüljük a levélszemét (SPAM) nagy számú megjelenését. A megerősítő üzenet csak egy alkalommal kerül kiküldésre, miután a bejelentő válaszolt a megerősítő üzenetre, az e-mail címe rögzítésre kerül a rendszerben és további megerősítésekre nem lesz szükség.
- 6.2. A titkosítatlan e-mail nem tekinthető különösen biztonságosnak, de elégséges az alacsony érzékenyséű adatok továbbításához. Amennyiben magas érzékenyséű adatok küldése szükséges, úgy az NHBK a PGP titkosítást támogatja. Az NHBK publikus kulcsa elérhető az NHBK honlapján. A hálózati fájlátvitel során, az e-mail-hez hasonlóan a következőket kell teljesíteni: az érzékeny adatokat titkosítani kell az átvitel során, vagy az átvitel alatt titkosított csatornát kell használni.
- 6.3. A Nemzeti Hálózatbiztonsági Központ az információ védelmét a bizalmasság és a sértetlenség (integritás) alapelvek szem előtt tartásával biztosítja, amellyel vállalja, hogy az információk csak az arra felhatalmazottak számára legyenek elérhetőek, és az információk és a feldolgozási módszerek teljességét és pontosságát megőrzi.
- 6.4. A Nemzeti Hálózatbiztonsági Központ felelősséget vállal az incidenskezelési folyamat kellő dokumentáltságáért, amely alkalmas arra, hogy tanúsítsa, hogy az NHBK az incidenskezelés kapcsán a legjobb szakmai gyakorlat szerint járt el.  
Az NHBK nem vállal felelősséget azon hibákért, mulasztásokért vagy azokért a károkért, amelyek a Bejelentő/Megrendelő által az információ helytelen felhasználásából vagy fel nem használásából származnak.