

Tartalomjegyzék:

1. Információk a dokumentumról

- 1.1 Az utolsó módosítás dátuma
- 1.2 A változtatások bejelentése
- 1.3 A hely ahol ez a dokumentáció megtalálható
- 1.4 A dokumentum eredetisége

2. Elérhetőségek

- 2.1 A csoport neve
- 2.2 Címe
- 2.3 Időzóna
- 2.4 Telefon szám
- 2.5 Fax szám
- 2.6 Egyéb telekommunikációs forma
- 2.7 Elektronikus mailcím
- 2.8 Publikus Kulesok és Titkosítási információk
- 2.9 Csoport tagjai
- 2.10 Egyéb információk
- 2.11 Bejelentési pontok

3. Szabályzat

- 3.1 Célok
- 3.2 Szolgáltatási célcsoport
- 3.3 Működés költségei és a működtető szervezet
- 3.4 Jogosultság

4. Működési politika

- 4.1 Incidens típusok és nyújtott szolgáltatások
- 4.2 Kooperáció, Együttműködés és Információk közzététele
- 4.3 Kommunikáció és partner azonosítás

5. Szolgáltatások

- 5.1 Incidens kezelés
- 5.2 Megelőző szolgáltatások

6. Figyelmeztetések

1. Információk a dokumentumról

1.1 Utolsó módosítás dátuma

Ez a 0.6. változat, ami 2009 október 13-án lett publikálva.

1.2 Változtatások bejelentése

A dokumentumon történő bármilyen változtatás a [hbone-admin listán](#) bejelentésre kerül. A regionális központok biztonságáért felelős személyei automatikusan felvételre kerülnek erre a listára. Erre a listára csak a NIIF tagok üzemeltetésért felelős személyei iratkozhatnak fel.

1.3 A hely ahol ez a dokumentum megtalálható

Az NIIF CSIRT-et leíró dokumentum aktuális változata az NIIF-CSIRT web oldalán található meg. Az URL <http://csirt.niif.hu/>.

1.4 A dokumentáció eredetisége

Ennek a dokumentumnak az eredeti html forrását alá írjuk az NIIF-CSIRT kulcsával. Az aláírás a következő helyen érhető el: csirt-dok-06v20091013.html.asc

2. Elérhetőségek

2.1 A csoport neve

"NIIF-CSIRT": NIIF Computer Security Incident Response Team. NIIF hálózatbiztonsági koordinációs csoport.

2.2 Cím

NIIF-CSIRT
NIIF/HUNGARNET
Victor Hugó u. 18-22
HU-1132 Budapest
Magyarország

2.3 Időzóna

UTC+0100 télen és UTC+0200 nyáron (Nyári időszámítás). A Nyári és Téli időszámítás közötti áttérés az Európai Unióban szokásos szabályok szerint történik. Közép Európai Idő.

2.4 Telefonszám

+36 1 450-3095, munkaidőben (08-18 óra között) (Az NIIF-CSIRT -re hivatkozva) +36 30 9518264, vész esetén, mindig elérhető

Az NIIF-CSIRT vész telefonszáma csak közvetlen hálózatbiztonsági veszély esetén hívható: Az NIIF/HUNGARNET ügyeletési rendszere kezeli a beérkezett telefonhívásokat előre definiált eljárási rendben. Az ügyeletési rendszer képes továbbítani a biztonsági bejelentéseket az NIIF-CSIRT -hez. Az NIIF-CSIRT a bejelentés alapján felveszi a kapcsolatot a bejelentővel.

2.5 Fax szám

+36 1 3506750, csak munkaidőben felügyelt. (Figyelem ez a FAX nem egy biztonságosan felügyelt berendezés)

2.6 Egyéb Telekommunikációs forma

Nincsen.

2.7 Elektronikus Levél Cím

[<csirt@niif.hu>](mailto:csirt@niif.hu); Ez az e-mail cím egy alias, ami tovább küldi a bejelentéseket az összes az NIIF-CSIRT tagnak. Azonban mindig egy NIIF-CSIRT tag van csak "szolgálatban". Ez a tag az aki lekezeli az

összes beérkező levelet.

2.8 Publikus kulcsok és egyéb titkosítási információk

Az NIIF-CSIRT GnuPG-t használ az információk aláírására és titkosítása

2.9 Team Members

Stefán Péter vezeti az NIIF-CSIRT csoportot. Máray Tamás az NIIF/HUNGARNET műszaki igazgató helyettese felügyeli a munkát.

Az összes az NIIF-CSIRT tagja neve megtalálható a <http://csirt.niif.hu/> címen.

2.10 Egyéb Információk

Az NIIF-CSIRT -ről általános információk a <http://csirt.niif.hu/> weboldalon található.

2.11 Bejelentési pontok

A javasolt kapcsolat felvételi mód az NIIF-CSIRT-el az [<csirt_at_niif.hu>](mailto:csirt_at_niif.hu) címre küldött e-mail; Az erre a címre érkezett az NIIF-CSIRT éppen szolgálatban lévő biztonsági felelőse kezeli le. Ha nagyon sürgős beavatkozásra van szükség, akkor a "SURGOS" szöveggel kell ezt jelezni az e-mail tárgyában (subject).

Ha a valamiért az e-mail kommunikáció nem működik, vagy nem lehetséges (biztonsági okok miatt). Akkor az NIIF-CSIRT-el telefonon is el lehet érni munkaidőben.

3. Szabályzat

Az NIIF-CSIRT ezen működési szabályzat alapján működik.

3.1 Célok

Az NIIF-CSIRT projekt és csoport célja, hogy eszközöket és módszereket adjon az NIIF/HUNGARNET hálózatához Magyarországon csatlakozóknak, hogy kezelni és megelőzni tudják a számítógép hálózati problémákat.

Az NIIF-CSIRT célja továbbá, hogy lekezelje és megoldja a jelentkező biztonsági problémákat többnyire koordinálva a feladatokat a NIIF/HUNGARNET regionális központok biztonságért felelős személyeivel. Szintén célja, hogy tájékoztasson (oktasson általánosságban, javaslatokat tegyen a rendszergazdáknak és felhasználóknak információ közreadásával).

Az NIIF-CSIRT egyik legfontosabb célja, hogy biztonsági problémák megoldásába és megelőzésébe aktívan bevonja az intézményeket és bizonyos biztonsági feladatokat delegáljon.

3.2 Szolgáltatási célcsoport

Az NIIF-CSIRT szolgáltatási célcsoportjai azok a site-ok, melyek az [NIIF/HUNGARNET](#) hálózatához kapcsolódnak.

3.3 Működés költségei és a működtető szervezet

NIIF finanszírozza az NIIF-CSIRT működési költségeit valamint biztosítja azokat a technikai feltételeket és fejlesztéseket amelyek a hatékony működéshez szükségesek.

3.4 Hatáskör

Az NIIF-CSIRT az NIIF igazgatójának és igazgató helyetteseinek támogatásával és hatáskör delegációjával működik.

Az NIIF-CSIRT megpróbál a rendszergazdákkal, a hálózati rendszergazdákkal, és NIIF/HUNGARNET-hez kapcsolódó intézmények felhasználóival maximálisan együttműködni és amennyire lehetséges elkerülni a működéséből fakadó hatalommal való visszaélést. Amennyiben a körülmények úgy kívánják, akkor az NIIF-CSIRT -nek lehetősége van olyan intézkedések megtételére, amelyek szükségesek a felmerült hálózatbiztonsági problémák megoldásához.

NIIF/HUNGARNET-hez kapcsolódó intézmények, amelyek panasszal kívánnak élni az NIIF-CSIRT ellen, NIIF műszaki igazgató helyetteséhez fordulhatnak.

Ha ez nem hoz kielégítő megoldást, akkor ezzel az NIIF igazgatójához lehet fordulni.

4. Működési politika

4.1 Incidens típusok és nyújtott szolgáltatások

Az NIIF-CSIRT jogosult kezelni és/vagy koordinálni minden hálózatbiztonsági problémát, amely szolgáltatási célcsoportjában (lásd 3.2) keletkezett, keletkezik vagy feltehető, hogy keletkezik. Az NIIF-CSIRT abban az esetben cselekedhet, ha kérés érkezik egy NIIF/HUNGARNET felhasználótól (lehetőség szerint rendszergazdától), vagy ha bármely NIIF/HUNGARNET felhasználónak hálózat biztonsági incidense keletkezett, vagy nagy valószínűséggel fog keletkezni.

Az NIIF-CSIRT által nyújtott támogatás nagymértékben függ az incidens vagy probléma súlyosságától, a felhasználói csoport méretétől, és az NIIF-CSIRT rendelkezésére álló erőforrásoktól. Minden incidensre valamilyen választ kell adni egy napon belül.

Az NIIF-CSIRT alapvetően elfogad minden biztonsági incidens bejelentést, ami NIIF/HUNGARNET felhasználókat érint, akár mint szenvedő alanya a biztonsági incidensnek, akár mint gyanúsítottja a biztonsági incidensnek. Minden felhasználótól elfogadunk bejelentést akik az NIIF/HUNGARNET hálózatához kapcsolódnak. Az NIIF-CSIRT minden problémával megkeresheti az NIIF/HUNGARNET hálózatához kapcsolódó intézmény hálózatbiztonságért felelős személyét, hogy segítsen megoldani a problémát. Az NIIF-CSIRT lehetővé teszi, hogy kompetens, és biztonsági problémákban jártas személyek az érintett intézményből részt vegyenek a folyamatban. Amennyiben szükséges, Az NIIF-CSIRT felveszi a kapcsolatot az érintett intézmény biztonsági felelőseivel, abban az esetben is ha ezt a felhasználó nem tette.

Az NIIF-CSIRT tudja, hogy a rendszergazdák és biztonsági felelősök tapasztalata és tudása nagy mértékben különbözik az NIIF/HUNGARNET-hez kapcsolódó intézmények esetén, és az NIIF-CSIRT tagjai megpróbálják a szükséges információkat és támogatást a biztonsági felelősöknek megadni, de az NIIF-CSIRT tagjai nem tudják azonnali oktatásban részesíteni a rendszergazdákat és nem tudják a szükséges változtatásokat elvégezni a rendszergazdák helyett. A legtöbb esetben az NIIF-CSIRT hivatkozásokkal (URL, könyv, cikk stb.) segíti a biztonsági felelősök munkáját, hogy el tudják hárítani a biztonsági problémát.

Az NIIF-CSIRT határozott szándéka, hogy az ügyfélkör előbb értesüljön a potenciális sérülékenységekről, veszélyforrásokról, és ha ez lehetséges akkor értesíti a közösséget mielőtt azt el kezdték kihasználni. Ezért az NIIF-CSIRT listát fog vezetni azokról az intézményekről és személyekről, amelyek az NIIF-CSIRT-el együtt működve el fogják hárítani a biztonsági problémát. Ez a lista alapvetően a biztonsági felelősökre fog alapulni.

4.2 Kooperáció, Együtműködés és Információk közzététele

Jogi és etikai korlátai vannak bizonyos információk az NIIF-CSIRT -en keresztüli közzétételének. Ezek a korlátok részben a HUNGARNET-hez csatlakozó intézmény biztonságpolitikai elveiben, részben [HUNGARNET AUP](#)-ben vannak lefektetve. Az NIIF-CSIRT elkötelezte magát ezeknek a korlátoknak figyelembe vételére és kijelenti, hogy kooperatív módon kíván hozzájárulni a biztonsági problémák megoldásához. Ilyenformán, a szükséges lépéseket megtéve a HUNGARNET tagok jogainak védelmében az információk szabad áramlásában érdekelt, és ebben segít másokat is, hogy biztonsági problémákat meg lehessen oldani és meg lehessen előzni.

A fentiekben megfogalmazott jogi, etikai és adatvédelmi szabályok azonban csak a legális felhasználókra, üzemeltetőkre és az érintett számítógépet használó felhasználókra vonatkozik. Nem vonatkozik az adatvédelem az illetéktelen felhasználókra, vagy illegális tevékenységet folytatókra, különösen a Btk 300C-E paragrafusát kimerítő bűncselekmények elkövetőire.

Az NIIF-CSIRT kifejezetten szándékozik együttműködni a HUNGARY CERT-el és az Európában működő más CSIRT csoportokkal.

4.3 Kommunikáció és Partner azonosítás

Az kezelt információt figyelembe véve a telefon elegendően biztonságosnak minősített még akkor is, ha az nem titkosított. A titkosítatlan e-mail nem minősíthető elegendően biztonságosnak, de elegendő alacsony biztonsági besorolású információk cseréjére. Amennyiben szükséges nagy biztonságú e-mail küldése, akkor erre a célra a GnuPG/PGP titkosításon alapuló kommunikációt alkalmazunk. Hálózati adatmozgatás (fájl transzfer) az e-mailhez hasonlóan minősíthető: biztonságra érzékeny adatot titkosítás nélkül tilos továbbítani. Erre akár a megfelelően használt SSH illetve az SSL/TLS is alkalmas lehet.

5. Szolgáltatások

5.1 Incidens kezelés

Az NIIF-CSIRT segíti a hálózati rendszergazdákat az incidensek technikai és szervezeti kezelésében.

Az NIIF-CSIRT statisztikákat készít azon incidenseket illetően, amelyek az NIIF/HUNGARNET hálózatában, hálózathoz kapcsolódó intézményekben történnek, vagy ezekhez kapcsolódnak. Az incidens típusokra vonatkozó statisztikát nyilvánosságra hozza.

5.2 Megelőző szolgáltatások

Az NIIF-CSIRT koordinálja és támogatja a következő szolgáltatásokat olyan szinten, ahogy az erőforrásai megengedik:

- Információ szolgáltatás
 - Levelezési lista a biztonsági felelősök számára, amelyen olyan információkat teszünk

közzé, amelyek a működési környezetük biztonsága számára fontos lehet.

- Archiválási szolgáltatás
 - A biztonsági incidensek logjai archiválásra kerülnek. Ezek a logok bizalmasan kezeltek, de statisztikai célból felhasználásra kerülnek.
- Oktatás
 - Az NIIF-CSIRT rendszeresen kezdeményezhet és támogathat oktatásokat, melyeknek az a célja, hogy az NIIF/HUNGARNET-hez kapcsolódó intézmények informatikai infrastruktúrája biztonságosabb lehessen. Ha körülmények úgy kívánják akkor az NIIF-CSIRT felkérhet szakértőt akár az NIIF/HUNGARNET tagintézményekből, akár külső intézményekből is, hogy tartson előadást az oktatáson.

6. Felelősség korlátozása és kizárása

Az NIIF-CSIRT a lehető legkörültekintőbben kíván eljárni az információk, értesítések és felhívások kiadásánál, de nem vállal felelősséget az esetleges hibákért, figyelmetlenségekért, vagy károkért amelyeket a közölt információk okoznak.