NIIF CSIRT projekt

2003 Április 16.

Mohácsi János <mohacsi@niif.hu>
Németh Ervin <nemethe@niif.hu>

Networkshop 2003

Tartalom

- CSIRT áttekintés
- CSIRT szolgáltatások
- CSIRT tapasztalatok
- Jövő biztonsági kihívásai
- Összegzés

Miért CSIRT?

- CERT <-> CSIRT
  - CERT = Computer Emergency Response Team
  - CSIRT = Computer Security Incident Response Team
- Akutt probléma a HUNGARNET-ben
  - nem kezelt
  - nem koordinált
  - jelentős problémák
  - elszigetelt tűzoltási tevékenységek

Mi az CSIRT?

- Egy szolgáltatás
  - Definiált és dokumentált
- Emberek és munkahelyük
- Kommunkáció
  - Telefon, E-mail, (Fax, …)
- Rendszer
- Eljárások
  - Mindenki tudja mit kell tennie
  - Incidensek megelőzésére, Incidensekre reakció, Incidensek után

HUNGARNET CSIRT célok

1.A HUNGARNET hálózati infrastruktúrájának biztonságossá tétele

- DoS, filtering, tűzfalak, routing, egress/ingress filtering, rendszerek biztonsága

2.A HUNGARNET tagok és dolgozóik hálózat biztonsági problémáinak orvoslása

- SPAM, Virus, Féreg, betörések, incidensek

3.A biztonsági problémák gyűjtése és az ehhez kapcsolódó támogatás és oktatás

- Bejelentések, oktatások

4.Részvétel és együttműködés a nemzetközi CSIRT projektekben és magyar CSIRT szervezet felállítása

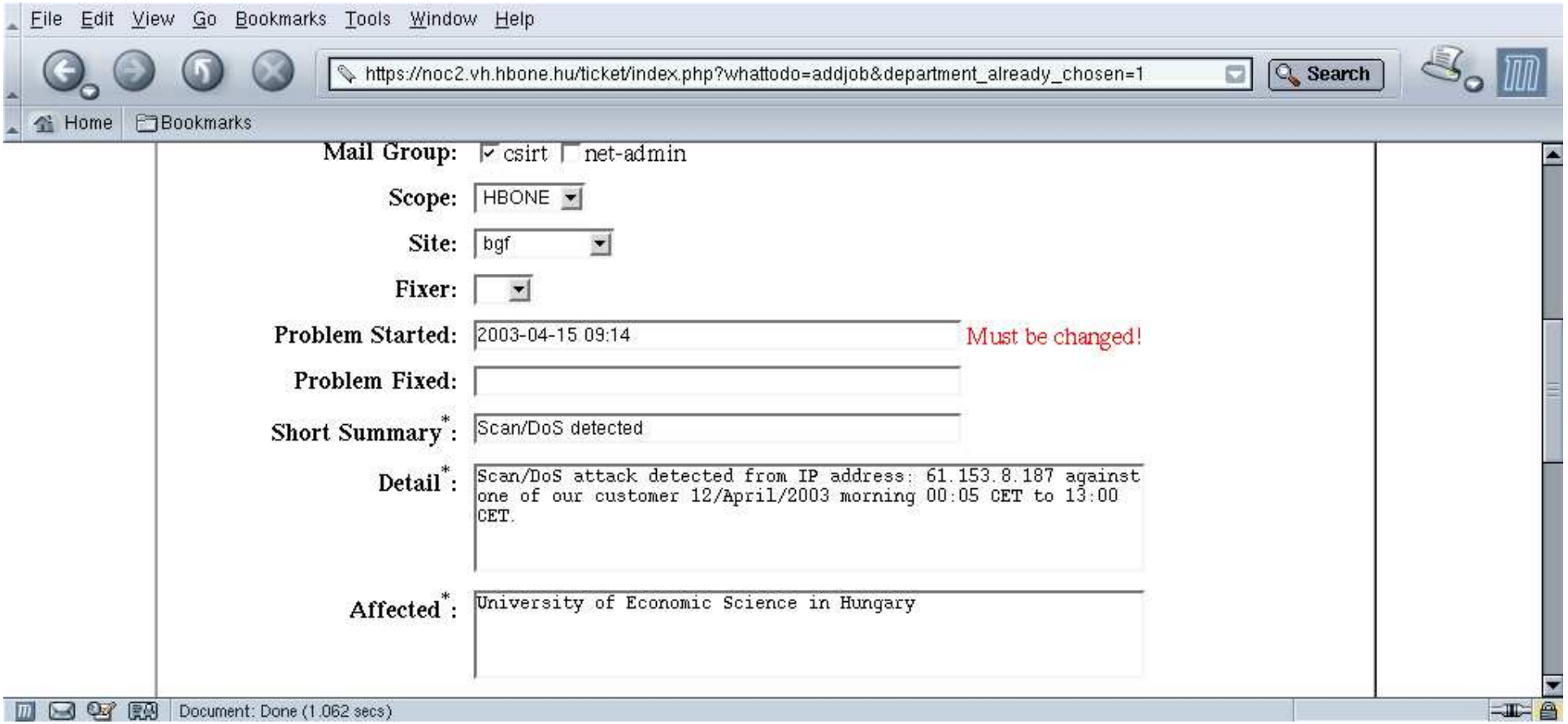
Incidens kezelés

- Jelenlegi ügyeletesi rendszerbe integrált
- Incidens követés:
  - jelenlegi ticketing rendszer
  - tovább fejlesztésre van szükség
- Ügyeletes CSIRT felelős dolgozza fel és koordinálja a beérkező kéréseket.
- Alapértelmezett kommunikációs forma:
  - e-mail
  - telefon

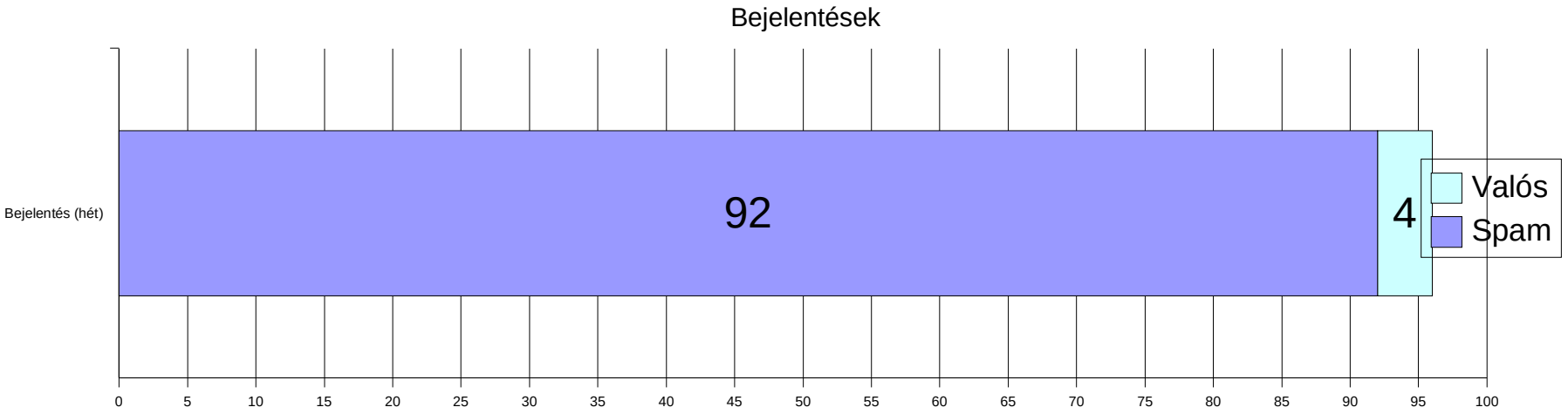
Incidens kezelés /2

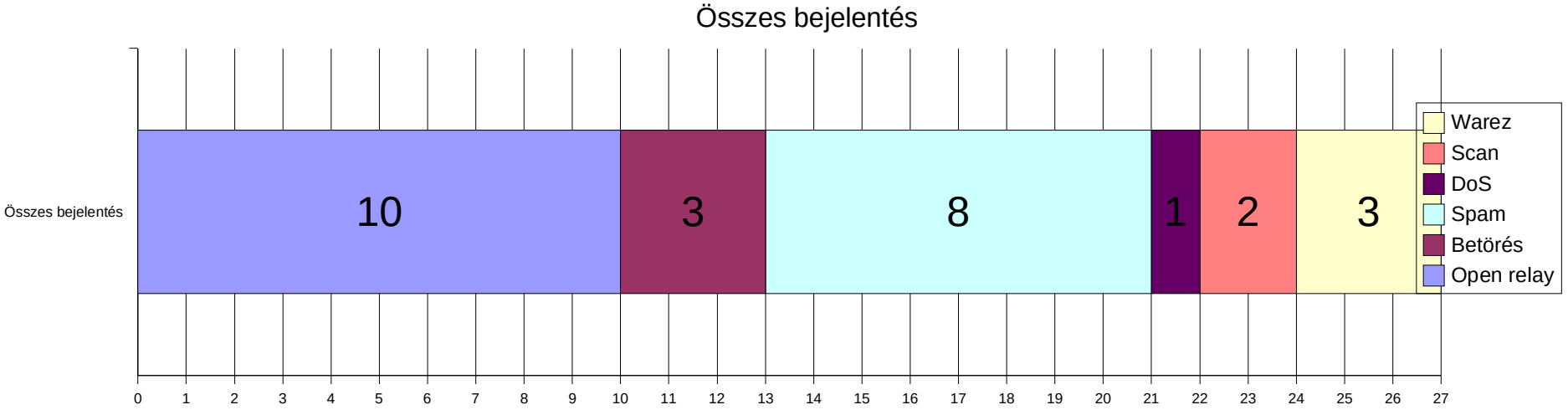
- Kidolgozott forgatókönyvek a leggyakoribb incidensekre.
- Kapcsolat felvétel az érintett site-al
  - RIPE bejegyzések és belső kapcsolati adatbázis alapján
- Bejelentési interfész:
  - csirt@niif.hu

Incidens felvétele



Tapasztalatok az incidens kezelésével kapcsolatban





Tapasztalatok az incidens kezelésével kapcsolatban /2

- Átlagos válasz: körülbelül minden harmadik
- Átlagos incidens idő: 10-12 nap
- Kiugró incidens idők: 53 nap, 1 nap

Incidens koordinációs tapasztalatok

- Hiányosságok
  - Kevés incidens bejelentés
    - Jó a biztonság? vagy ismeretlen?
  - Nincs válasz a levelekre
    - Érdektelenség? Túlterheltség? Rossz e-mail cím?
- Jó tapasztalatok
  - HBONE menedzsment és regionális központok segítőkészek
  - blokkolások jótékonyan hatnak a hiba javításokra
  - SQL slammer nem volt jelentős

Jövő kihívásai

- Oktatás
- Rendszer biztonság (Operációs Rendszer + alkalmazás)
- Vírus
  - Nem lesznek veszélyesebbek, csak gyorsabbak
- Új alkalmazói protokollok
- P2P alkalmazások
  - adminisztratív szabályok
- IPv6
- Magyar SPAM

Feladatok

- Együttműködés erősítése
  - Site Security kapcsolatok azonosítása
  - Oktatási témák kiválasztása és kidolgozása
- Incidens kezelés továbbfejlesztése
- Incidens megelőzés: bejelentések & oktatás
- HBONE infrastruktúra biztonsági átvilágítása
- Nemzetközi együttmüködés

Kérdések?

<mohacsi@niif.hu>
<csirt@niif.hu>