#SecFest 2014

Incidenty na ZČU

A co s nimi děláte?

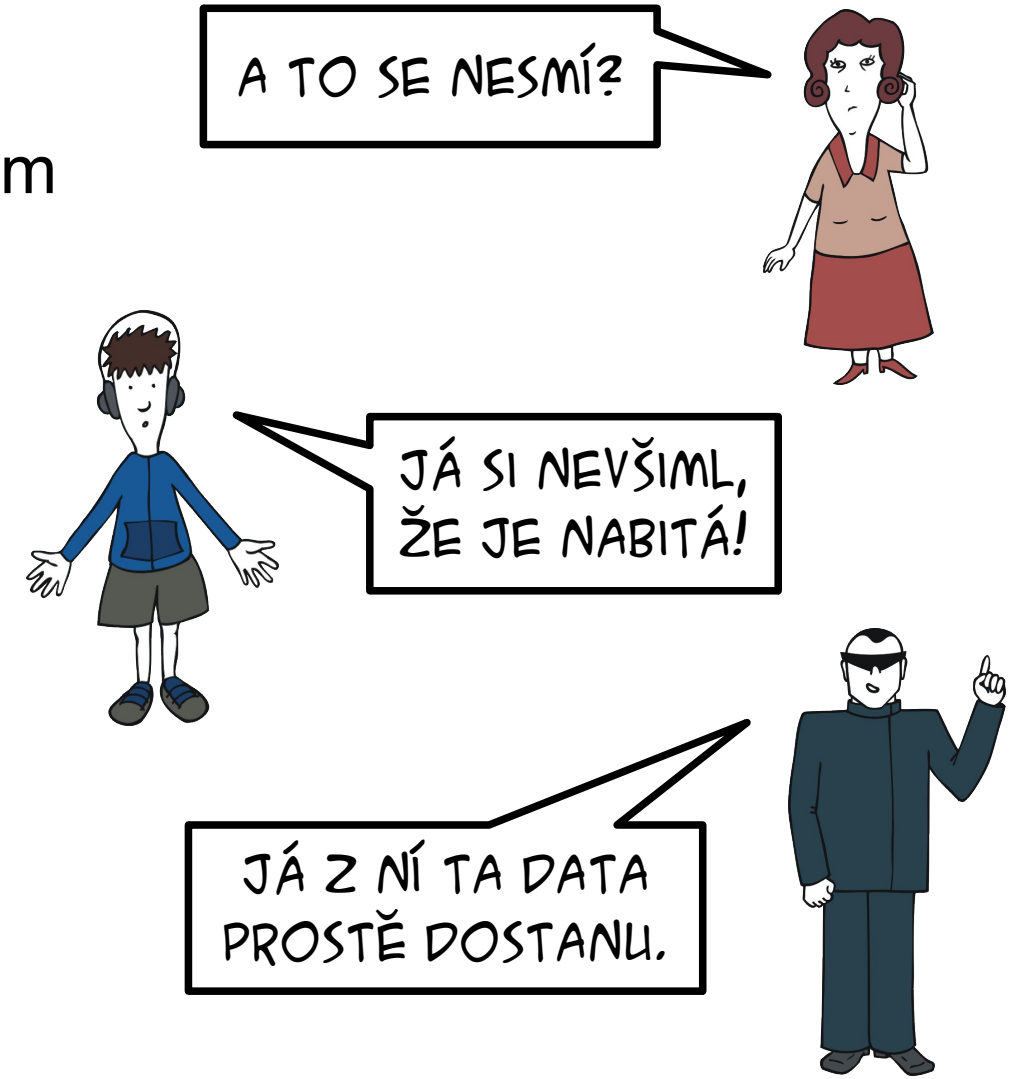
Aleš Padrta
apadrta@civ.zcu.cz

Bezpečnostní incident

- Bezpečnostní incident
  - Obecně = narušení bezpečnosti
- Oblasti problémů
  - Dostupnost (např. DoS útok)
  - Integrita (např. zavirování počítače)
  - Důvěrnost (např. neoprávněný přístup)
  - Porušení zákonů (např. autorský zákon)
  - Porušení vnitřních pravidel (např. 10R/2008)

Jak se to může stát?

- Neznalost
  - Nemám ponětí co dělám
  - Neznám důsledky
- Nedbalost
  - Opomenutí
- Úmysl
  - Záměrná aktivita
  - Záměrné ignorování
  - Uvědomuji si důsledky



Původci a oběti

- Původce = kdo způsobil problém
- Oběť = kdo problémem trpí
- Zaměstnanci a studenti ZČU
  - Někdy původci
  - Někdy oběti
- Jak postupovat
  - Oběť – kontaktovat HelpDesk
  - Původce – dostane instrukce

Postup řešení incidentu

(Původce je ze ZČU)

Postup řešení incidentu

- Zjištění
  - Informace má náš CSIRT
    - WEBnet Incident Response Team
  - Zjištění vlastními silami
    - IDS, McAfee, DeathRay, logy, ...
  - Ohlášení obětí
    - CSIRT dané organizace, fyzická osoba, ...
  - Ohlášení třetí stranou
    - CESNET NetFlow, SpamCop, ...

Postup řešení incidentu

- Ověření
  - Informaci může poslat každý
  - Naše logy potvrzují incident
- Minimalizace dopadů
  - Blokování zneužitého konta
  - Zablokování služby
  - Odpojení napadeného počítače
  - Odebrání práv

Postup řešení incidentu

- Provedení nápravy
  - Interakce s uživatelem
    - Informace o incidentu
    - Zaslání e-mailu s instrukcemi
    - Osobní návštěva WIRT
  - Technická náprava
    - Přeinstalace
    - Změna hesla
- Uzavření incidentu

Postup řešení incidentu

- Pohovory – osobní návštěva
  - Standardní postup
    - Vysvětlení problému
    - Vysvětlení správného chování
    - Upozornění na následky
  - Co je zbytečné
    - Zatloukat
    - Žádat výjimky
  - Záznam v interních systémech
    - Průběh pod dohledem

Postup řešení incidentu

- Eskalace
  - Instrukce v e-mailu
  - Pohovor s pracovníky CIV
  - Disciplinární komise fakulty (studenti)
    Porušení pracovní kázně (zaměstnanci)
  - Trestně právní řízení
  - Občansko právní řízení

Shrnutí

- Řešení bezpečnostních incidentů
  - Standardní postup
  - Interakce s uživateli
- Co dělat?
  - Původce
    - Informace v e-mailu
    - Nefunkční služba → návštěva HelpDesku
  - Oběť
    - Kontaktovat HelpDesk CIV

Dotazy

???