Řešení bezpečnostních incidentů

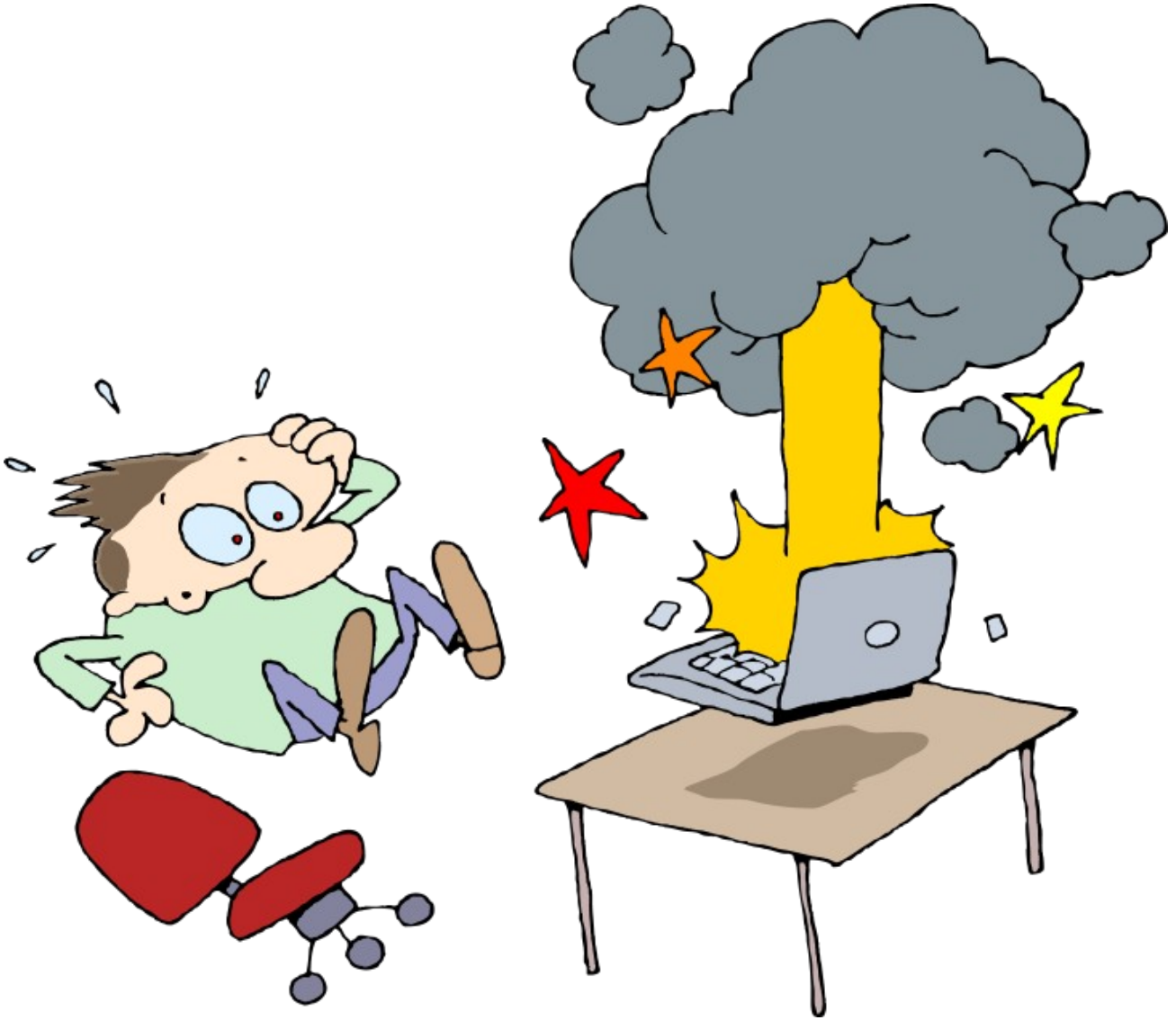
Andrea Kropáčová
(CESNET-CERTS)

Aleš Padrta
(WEBnet Incident Response Team)

Obsah

- Co je to incident
- Hlášení incidentů
- Kdo se incidenty zabývá?
  - CESNET
  - Univerzita
- Reakce na incident
- Dopad na uživatele
- Shrnutí

Bezpečnostní incidenty

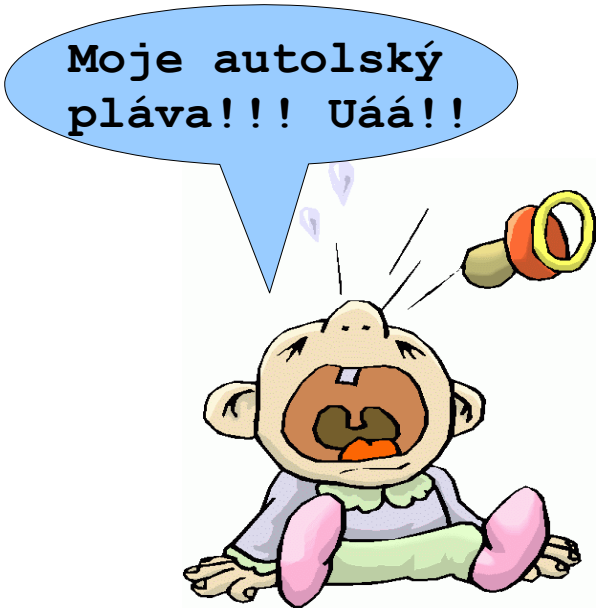


Bezpečnostní incidenty

- Incident = narušení bezpečnosti IT/IS
  - Dostupnost
    - Systémy přestanou fungovat
  - Integrita
    - Došlo ke změně dat nebo funkčnosti systému
  - Důvěrnost
    - K datům/systému se dostal někdo nepovolaný
- Porušení platných pravidel
  - Zákony ČR
  - CESNET AUP
  - Směrnice ZČU
  - Provozní řády

Hlášení incidentů

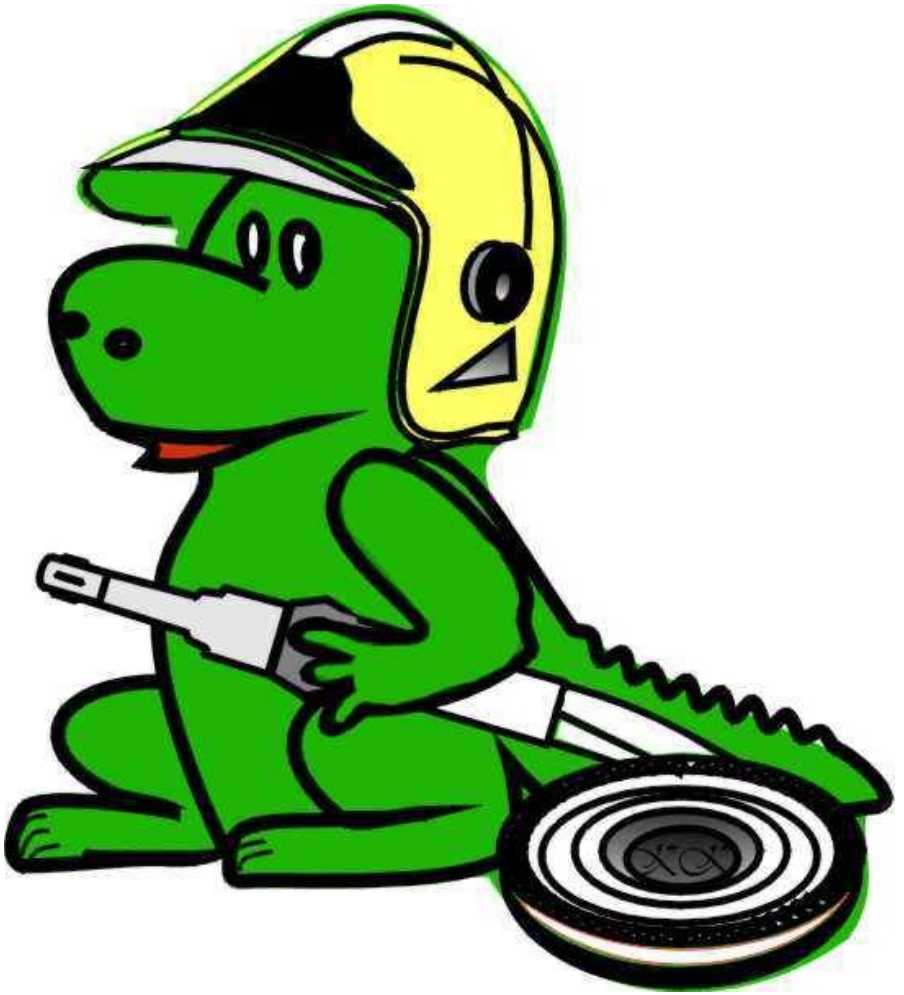
- Kdo incidenty hlásí?
  - Oběť
    - Posíláte mi spam, útočíte mi na server, ...
  - Zainteresovaná osoba (např. BSA)
    - Detektor porušování autorských práv na P2P, ...
  - Vlastní automaty
    - Různé varianty IDS
    - Problém se řeší „doma“
- Komu jsou hlášeny?
  - Správci příslušné IP adresy



Kdo se incidenty zabývá?

- Bezpečnostní týmy
  - CSIRT, CERT
- CESNET (ISP) – abuse@cesnet.cz
  - Dohled nad svěřeným rozsahem
  - Přeposílání dále
  - Zásah v krajním případě
- ZČU (organizace) – abuse@zcu.cz
  - Dohled nad svou sítí
  - Ochrana dobrého jména
  - Řešení problému

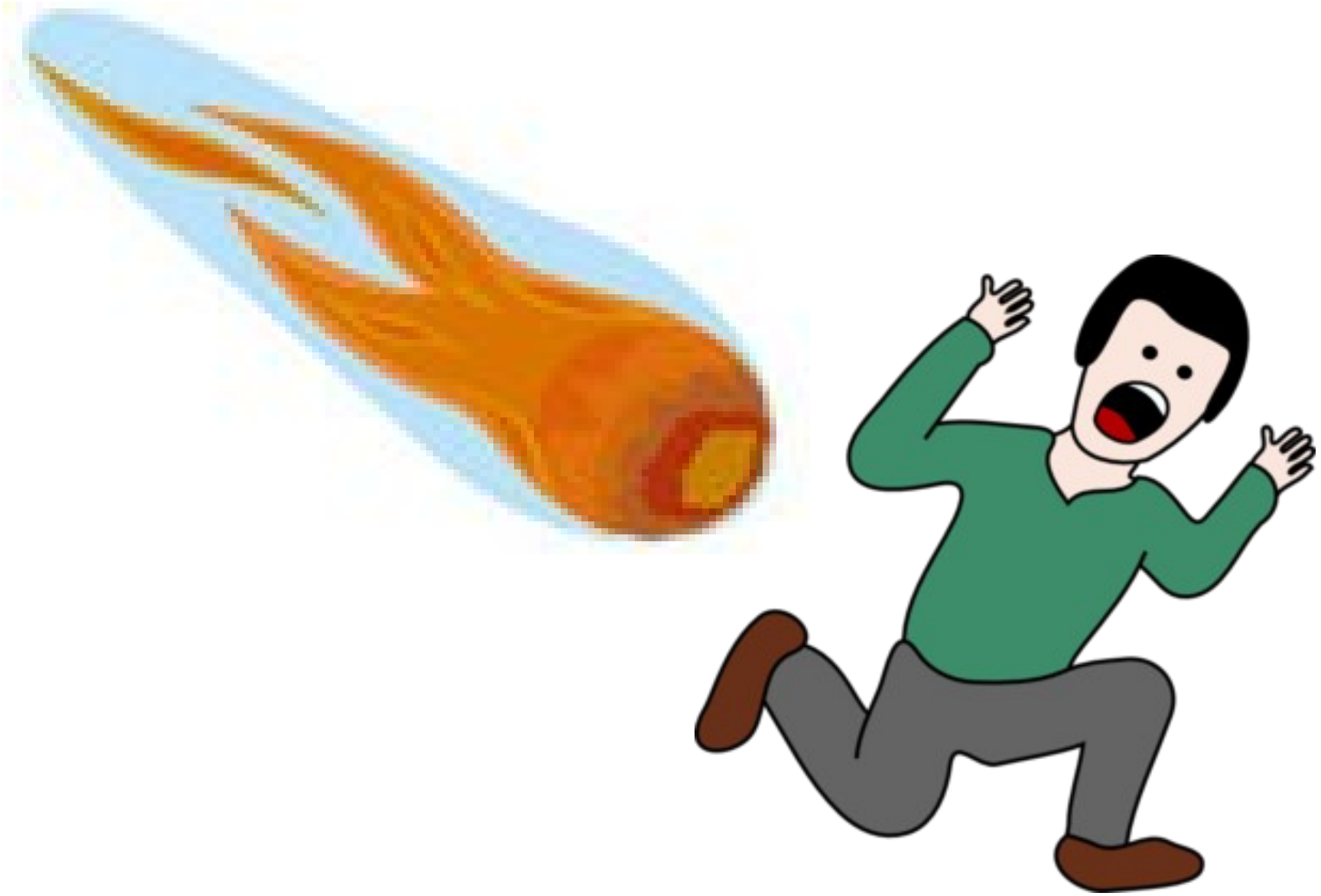
Reakce na incident



Reakce na incident

- Ověření
- Minimalizace dopadů
  - Zablokování konta, odpojení od sítě, vypnutí serveru, ...
- Zajištění nápravy
  - Odvirování, aktualizace, ...
- Ponaučení
  - Proškolení uživatele / správce
- Opětovné připojení/odblokování
- Odpověď stěžovateli

Dopad na uživatele



Dopad na uživatele

- Vlastní incident
  - Napadený počítač – zneužití dat, přístupů …
  - Odpojení od sítě
  - Nemožnost používat (dočasně) služby
- Univerzitní směrnice
  - Disciplinární komise / porušení pracovní kázně
  - Omezení „nenárokových“ služeb
- Stát a jeho zákony
  - Autorský zákon, trestní zákon
  - Více v samostatné prezentaci

Pozvánka k pohovoru?

- WEBnet Incident Response Team
  - Kolem 100 incidentů ročně (až 215)
  - Pohovory s uživateli
- Stále stejný průběh
  1) Já to nebyl(a)
  2) Co mi asi můžete
  3) Poslední z tragédií
  4) Nabídka prospěchu
- Standardní proces
  - Stejný metr pro všechny

Shrnutí

- Bezpečnostní incidenty
  - Jsou detekovány
  - Jsou hlášeny
  - Jsou řešeny
- Uživatelé
  - Jsou odpovědní za své chování
  - Neznalost neomlouvá
  - Nevyhnou se postihu
  - Možná soudní dohra
- Univerzita – ochrana dobrého jména

Dotazy

???