#SecFest 2016

Řešení bezpečnostních incidentů na ZČU

Aleš Padrta
apadrta@civ.zcu.cz

Motivace

- Síť WEBnet
  - Bezdrátová síť Eduroam, zcu-mobile
  - Pevná síť (učebny, katedry, koleje)
- Západočeská univerzita v Plzni
  - Odpovědnost za svou síť
    - Funkční pro uživatele
    - Bezproblémová pro zbytek Internetu
  - Pravidla používání sítě WEBnet (10R/2008)
    - … základní návod co (ne)dělat

Ideální stav

- Uživatelé dodržují pravidla
  - Zákony platné v ČR
  - Licenční a jiná ujednání
  - Univerzitní směrnice
  - Pravidlo „zdravého rozumu“
- Připojená zařízení
  - Pečlivě udržovaná
  - Zabezpečená
- Nikdo nemá zlé úmysly

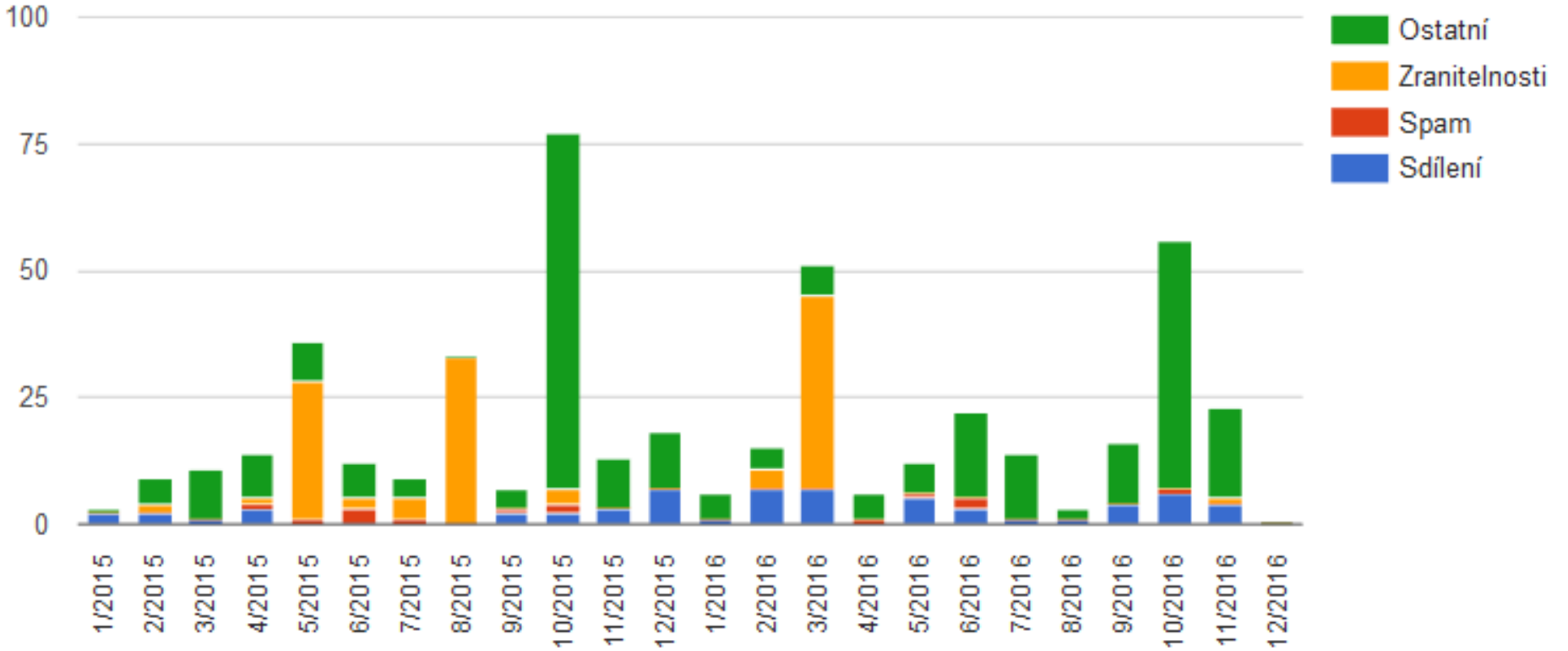
Co se může pokazit

- 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)
- Bezpečnostní incident
  - Obecně = narušení bezpečnosti

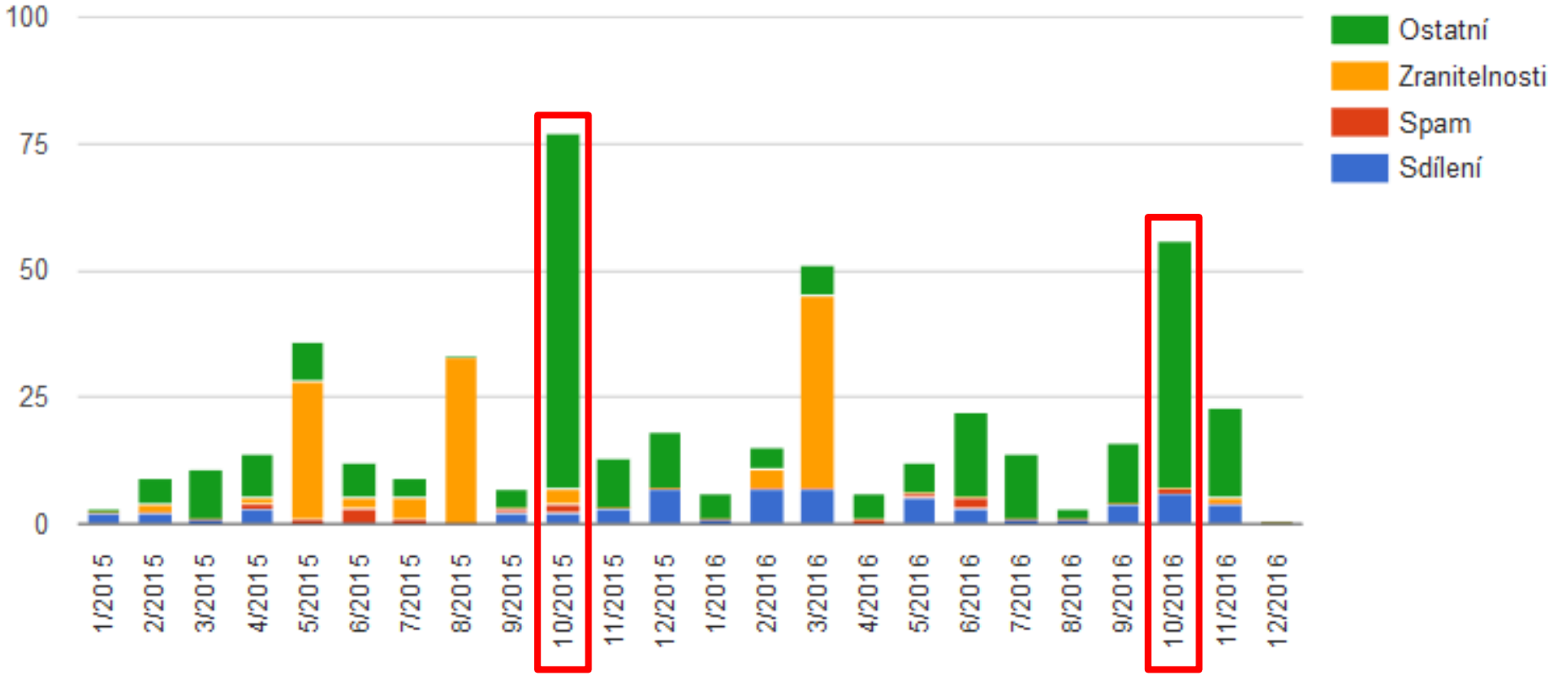
Na počátku byla ...

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

Počty incidentů 2015-2016



Počty incidentů 2015-2016



Říjen – měsíc kybernetické bezpečnosti? No tak určitě!

Řešení incidentu

- ZČU má zodpovědný přístup
  - Bezpečnostní tým WIRT
    (WEBnet Incident Response Team)
  - Reakce na bezpečnostní incidenty
- Cílem je chránit
  - Vlastní uživatele
  - Okolní Internet
  - Pověst sítě WEBnet (resp. ZČU)

Postup řešení incidentu

1) **Zjištění (detekce)**

- Zjištění vlastními silami
  - IDS, McAfee, DeathRay, logy, ...
- Ohlášení třetí stranou
  - CESNET NetFlow, IDS, Mentat, ...
  - Bezpečnostní tým jiné organizace
  - Zástupci držitelů autorských práv
  - Dotčená fyzická/právnická osoba

Postup řešení incidentu

2) **Ověření**

- Informaci může poslat každý
  - Řešíme jen skutečné události
- Naše záznamy
  - Potvrdí výskyt incidentu
  - Doplní podrobnosti

Postup řešení incidentu

3) **Minimalizace dopadů**

- Cíl: Zastavit zhoršování situace
  - Odpojení napadeného počítače
  - Zablokování služby
  - Zablokování zneužitého konta
  - Odebrání přístupových práv
  - …
- Dočasné řešení do provedení nápravy

Postup řešení incidentu

4) **Provedení nápravy**

- Technická opatření
  - Odvirování, reinstalace, rekonfigurace, …
  - Změna hesla, klíčů, certifikátů, ...
- Interakce s uživateli
  - Informace o incidentu
  - Zaslání e-mailu s instrukcemi
  - Osobní návštěva WIRT

Pohovor s uživateli

- Osobní návštěva
  - U závažných incidentů
  - U opakovaných incidentů
  - Na žádost uživatele
- Standardní postup
  - Vysvětlení problému
  - Vysvětlení správného chování
  - Upozornění na následky

Pohovor s uživateli

- Dopady vlastního incidentu
  - Napadený počítač – zneužití dat, přístupů …
  - Odpojení od sítě + nemožnost používat služby
- Vymáhání dodržování univerzitních směrnic
  - Disciplinární komise / porušení pracovní kázně
  - Omezení „nenárokových“ služeb
- Vymáhání dodržování zákonů platných v ČR
  - Trestně právní řízení
  - Občansko právní řízení

Pohovor s uživateli

- Čeho se při pohovoru rozhodně vyvarovat
  - Zapírat
    - Víme víc, než si myslíte
  - Vymýšlet si historky
    - DLP (dojemný lidský příběh)
    - Za ta léta už známe všechny
  - Nabízet úplatky a žádat výjimky
    - Mimo vaše možnosti
    - Máme standarní postupy
    - Průběh incidentu je zaznamenán v interních systémech

Shrnutí

- Svět není ideální
  - Bezpečnostní incidenty
- ZČU
  - Odpovědnost za univerzitní síť WEBnet
  - WEBnet Incident Response Team
  - Reakce na bezpečnostní incidenty
- Doporučení
  - Dodržujte 10R/2008, řiďte se zdravým rozumem
  - Spolupracujte (když už jste účastníkem incidentu)

Dotazy

???

Použité obrázky

- http://www.happyschools.com
- http://www.referralcarpetcare.com
- http://www.clker.com