#SECFEST2017

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Řešení bezpečnostních incidentů na ZČU

Jiří Čepák / 29. 11. 2017

Úvod

- 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

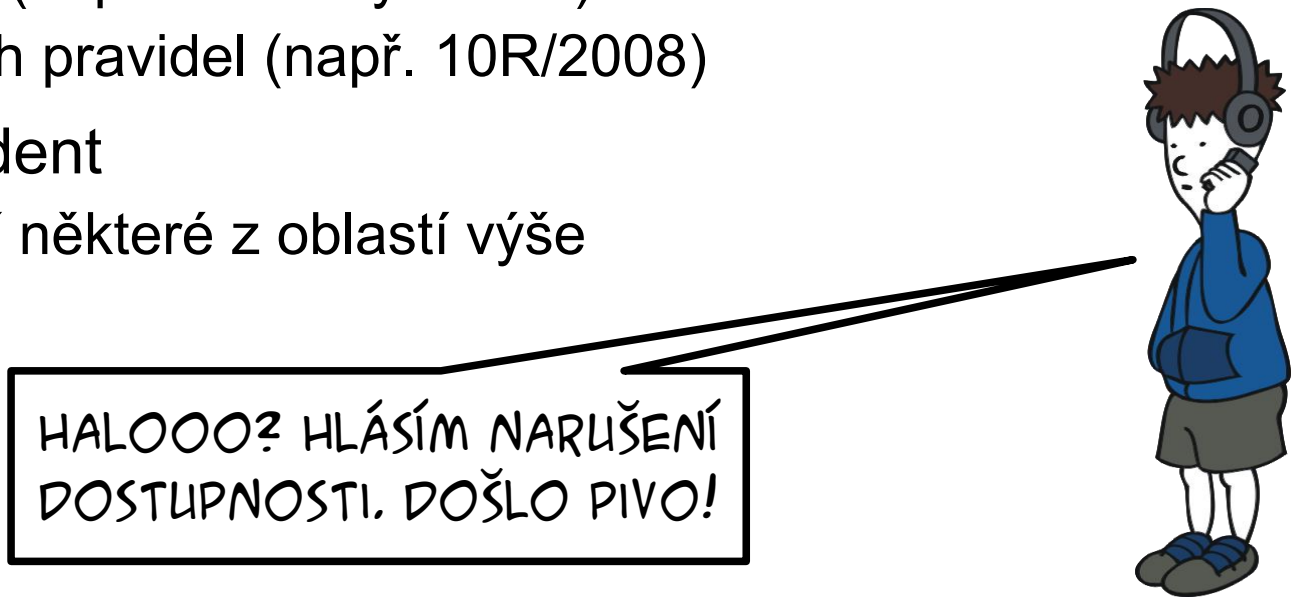
Ideální stav

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

Reálný stav
opak ideálního

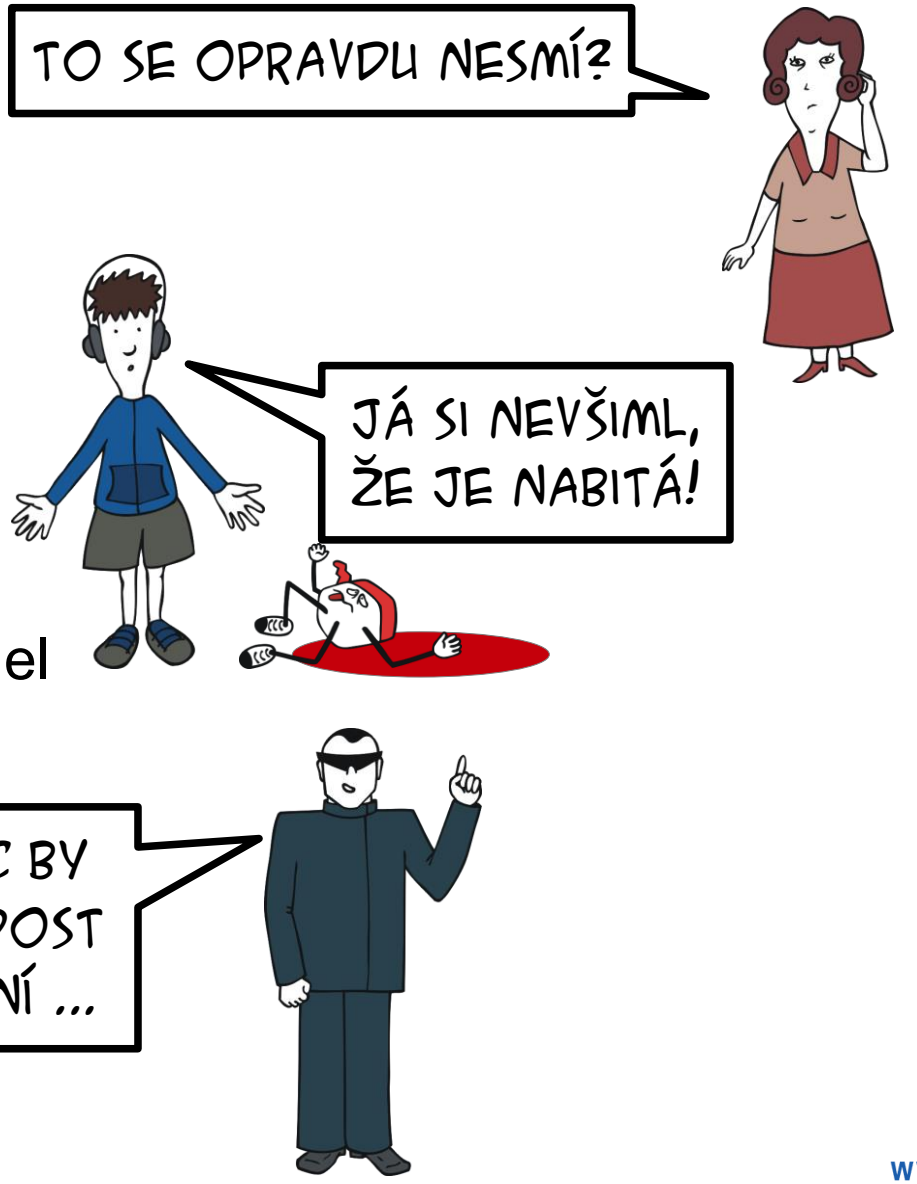
Co se může pokazit

- Oblasti možných problémů
  - Dostupnost (např. DoS/DDoS útok)
  - Integrita (např. zavirování počítače)
  - Důvěrnost (např. neoprávněný přístup)
  - Porušení zákonů (např. autorský zákon)
  - Porušení vnitřních pravidel (např. 10R/2008)
- Bezpečnostní incident
  - Obecně narušení některé z oblastí výše

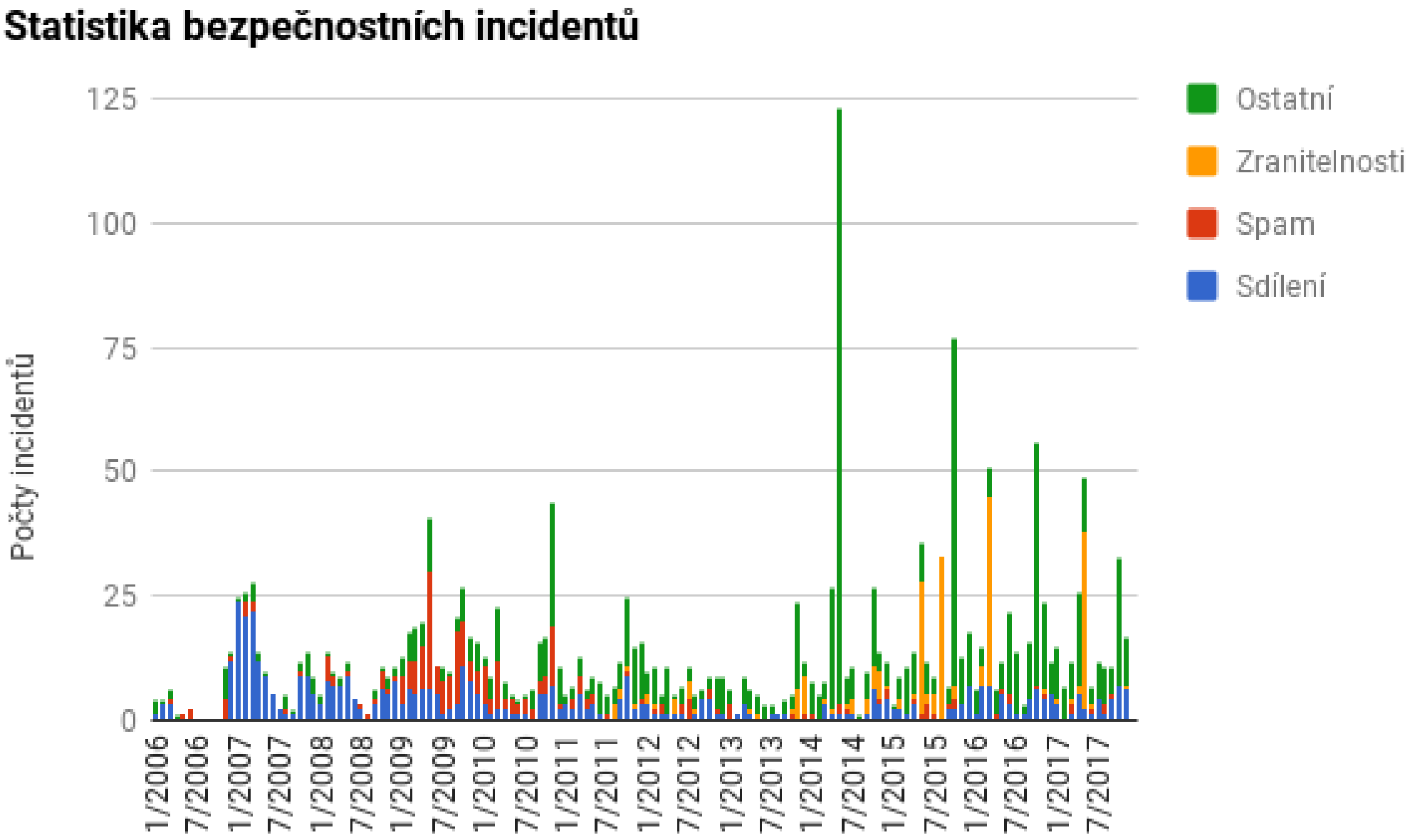


Z čeho pramení vznik incidentu

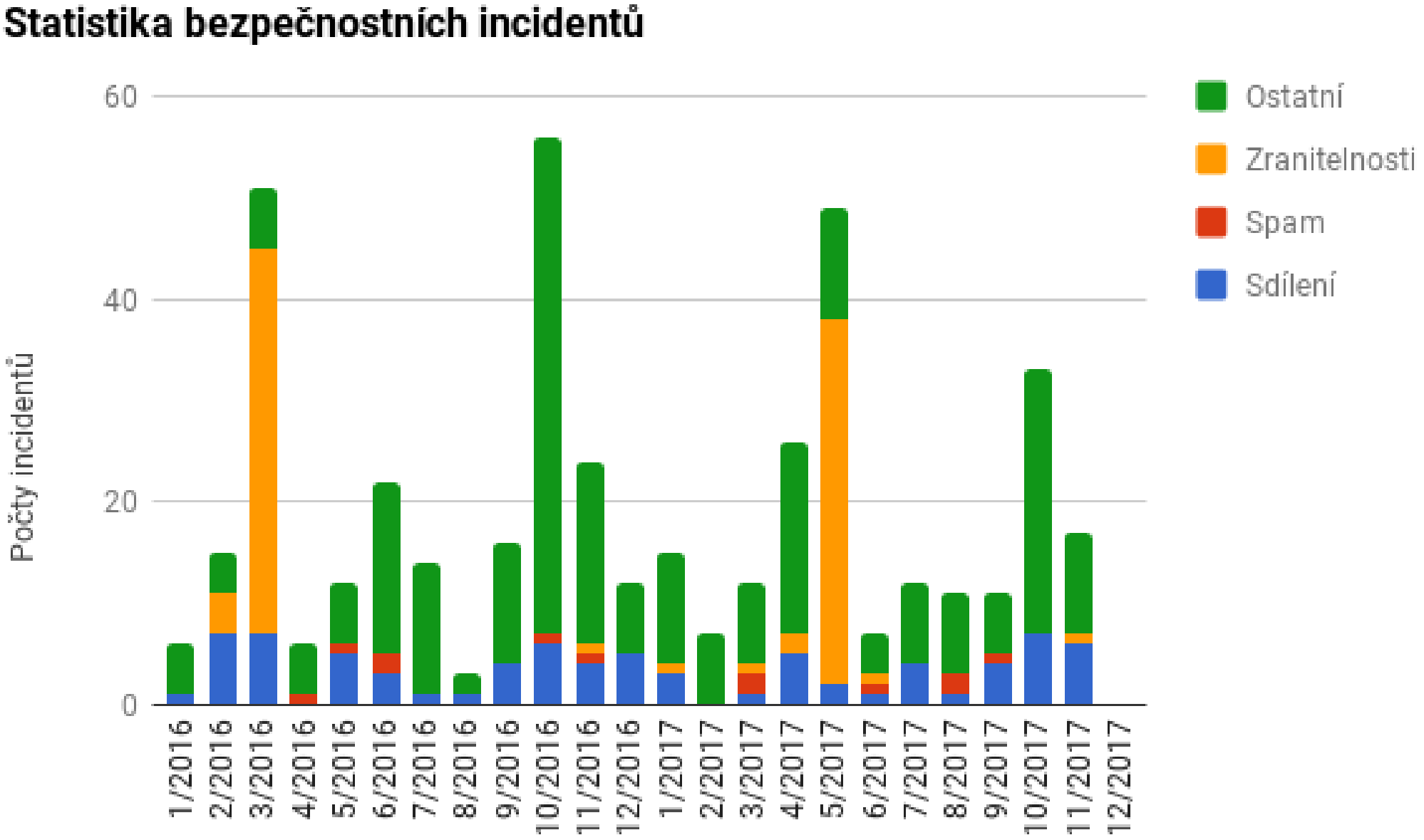
- Neznalost
  - Nemám ponětí, co dělám
  - Neznám důsledky
- Nedbalost
  - Opomenutí
- Úmysl
  - Záměrná aktivita
  - Záměrné ignorování pravidel



Statistika 2006-2017



Statistika 2016-2017 (k 27.11.2017)



Řešení incidentu

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, honeypoty, Mentat, …
     - Bezpečnostní tým jiné organizace
     - Dotčená fyzická/právnická osoba
     - Zástupci držitelů autorských práv

Příklad stížnosti zástupce vlastníka autorských práv

Dear Sir or Madam:

We are contacting you on behalf of Paramount Pictures Corporation (Paramount). Under penalty of perjury, I assert that IP-Echelon Pty. Ltd., (IP-Echelon) is authorized to act on behalf of the owner of the exclusive copyrights that are alleged to be infringed herein.

IP-Echelon has become aware that the below IP addresses have been using your service for distributing video files, which contain infringing video content that is exclusively owned by Paramount.

IP-Echelon has a good faith belief that the Paramount video content that is described in the below report has not been authorized for sharing or distribution by the copyright owner, its agent, or the law. I also assert that the information contained in this notice is accurate to the best of our knowledge.

We are requesting your immediate assistance in removing and disabling access to the infringing material from your network. We also ask that you ensure the user and/or IP address owner refrains from future use and sharing of Paramount materials and property.

In complying with this notice, Zapadoceska univerzita v Plzni should not destroy any evidence, which may be relevant in a lawsuit, relating to the infringement alleged, including all associated electronic documents and data relating to the presence of infringing items on your network, which shall be preserved while disabling public access, irrespective of any document retention or corporate policy to the contrary.

Please note that this letter is not intended as a full statement of the facts; and does not constitute a waiver of any rights to recover damages, incurred by virtue of any unauthorized or infringing activities, occurring on your network. All such rights, as well as claims for other relief, are expressly reserved.

Should you need to contact me, I may be reached at the following address:

Adrian Leatherland
On behalf of IP-Echelon as an agent for Paramount
Address: 7083 Hollywood Blvd., Los Angeles, CA 90028, United States
Email: p2p@copyright.ip-echelon.com

Evidentiary Information:
Protocol: BITTORRENT
Infringed Work: Baywatch
Infringing FileName: Baywatch (2017) [YTS.AG]
Infringing FileSize: 940417015
Infringer's IP Address: 147.228.121.121
Infringer's Port: 13769
Initial Infringement Timestamp: 2017-10-14T21:38:06Z

Postup řešení incidentu

2) Ověření

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

3) Minimalizace dopadů

- Cílem je 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, revokace certifikátů, …
- Interakce s uživateli
  - Informace o incidentu
  - Instrukce k (vy)řešení incidentu
  - Osobní návštěva WIRT

Osobní návštěva

- Pohovor s uživateli
  - U závažných incidentů
  - U opakovaných incidentů
  - Na žádost uživatele
- Standardní postup
  - Vysvětlení problému
  - Vysvětlení správného chování
  - Upozornění na následky

Následky

- Dopady vlastního incidentu
  - Napadený počítač – zneužití dat, přístupů, …
  - Odpojení od sítě
- 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)
    - Známe všechny
  - Nabízet úplatky a žádat výjimky
    - Mimo vaše možnosti
    - Máme standardní 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 a řiďte se zdravým rozumem
  - Spolupracujte (když už jste účastníkem bezpečnostního incidentu)

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Dotazy???

Jiří Čepák / cepakj@civ.zcu.cz