

# Bezpečnostní tým na VŠB-TUO

Radomír Orkáč  
VŠB-TUO, CIT 872  
21.5.2009, Praha

[radomir.orkac@vsb.cz](mailto:radomir.orkac@vsb.cz)



# O nás

- Bezpečnostní tým
  - Martin Pustka, Jiří Grygárek, Pavel Jeníček, Radomír Orkáč
  
- Sít' VŠB-TUO má název TUONET
  - 158.196.0.0/16
  - 2001:0718:1001::/48
  - 23312 studentů (31.10. 2008)
  - 11574 registrovaných zařízení (k 1. 5. 2009)
  - 681 klientů wifi sítě (maximum, podzim 2008)

# Historie

- Srpen 2008
  - ostrý provoz IDS Snort
  - tvorba návodů (odvirování, aktualizace OS, ..)
- Září 2008
  - helpdeskový systém (Request Tracker)
  - definice postupů a formalizace stávajícího stavu
  - detekce sdílení dat (porušování autorského z.)
- 17.12. 2008 - provozní řád

# Co řešíme..

- Řešení bezpečnostních incidentů
  - Malware
  - Porušování zákona a pravidel pro připojení
  - Napadání, skenování
  - Rozesílání spamu
  - Zneužívání diskuzních fór a návštěvních knih
  - Krádeže IP adres (užití bez registrace)

# Postup při řešení

- Přijetí incidentu
- Zdokumentování pracovníkem bezp. týmu.
- Závažné ohrožení -> blokace stanice.
- Kontaktování uživatele/správce.
- Řešení incidentu provádí uživatel stanice, popř. příslušný správce stanice (např. fakultní, rektorátní). Po vyřešení informuje o způsobu a výsledcích pracovníka bezp. týmu.

# Postup při řešení

- Pracovník CSIRT týmu dohlíží na řešení problému. Po přijetí informace o vyřešení od oprávněné osoby a po ověření tohoto faktu může incident uzavřít.
- Při uzavření incidentu vyrozumí pracovník CSIRT o tomto faktu uživatele i správce koncové stanice a zajistí publikaci tohoto faktu v informačních systémech.

# Informace pro řešení BI

- DHCP log
  - přiřazení IP adres v čase
- Logy z radius serveru
  - wifi a VPN
- Evidenční systém Netis (vlastní)
  - koleje, CIT
  - 3Q 2008 všechny nové (ruční) registrace
  - IP, MAC, login, čas

# Informace pro řešení BI

- IDS Snort (pf\_ring)
  - signatury pro detekci malware
  - automatizovaná analýza logu (**vlastní**)
  - databáze IS Netis (**vlastní**)
  
- IDS/IPS Fortigate
  - wifi a VPN
  - automatizovaná analýza logu (**vlastní**)

# Informace pro řešení BI

- Vlastní skripty
  - sdílení dat (hlavně P2P)
  - zneužívání diskuzních fór
  - krádež IP
  - měření přenesených dat

# Denní sestavy

158.196.xxx.xxx | pcx333x.vsb.cz

MAC: ab:cd:ab:cd:ab:cd

Login: abc107 (Andrea Kropacova)

Kalkulace: 129

Pocet: 169

Cil.IP: 1

Cil.nonDNS: 0

Ohodn: 1/1

Kalkul: 169.00

Incident: Downadup/Conficker A or B Worm reporting

158.196.xxx.xxx | pcx333x.vsb.cz

MAC: ab:cd:ab:cd:ab:cd

Login: abc107 (Andrea Kropacova)

Upload: 1 GB

torrent: The Frames [9 Albums] + The Swell Season + Once OST

torrent: X-Men.Origins.Wolverine-RELOADED

dcpp: Pinnacle Studio Ultimate v12 0 0 6163 with Plug-Ins

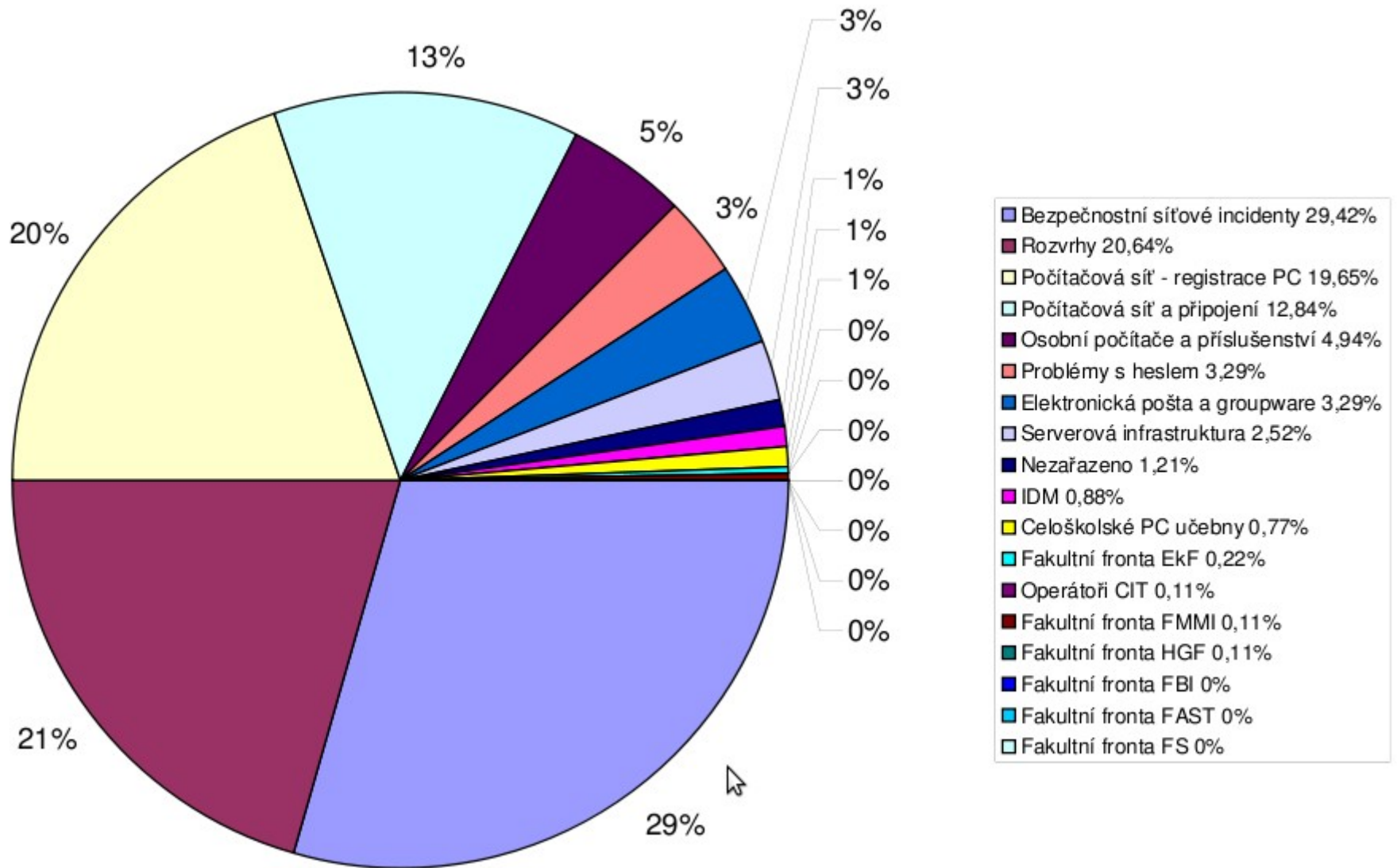
# Provozní řády a pravidla

- Provozní řád bezpečnostního týmu
  - zdroje incidentů
  - detekce
  - přijímání incidentu
  - postup při zpracování
  - technické a personální zajištění provozu
- Pravidla pro připojení do sítě
  - práva, povinnosti, sankce

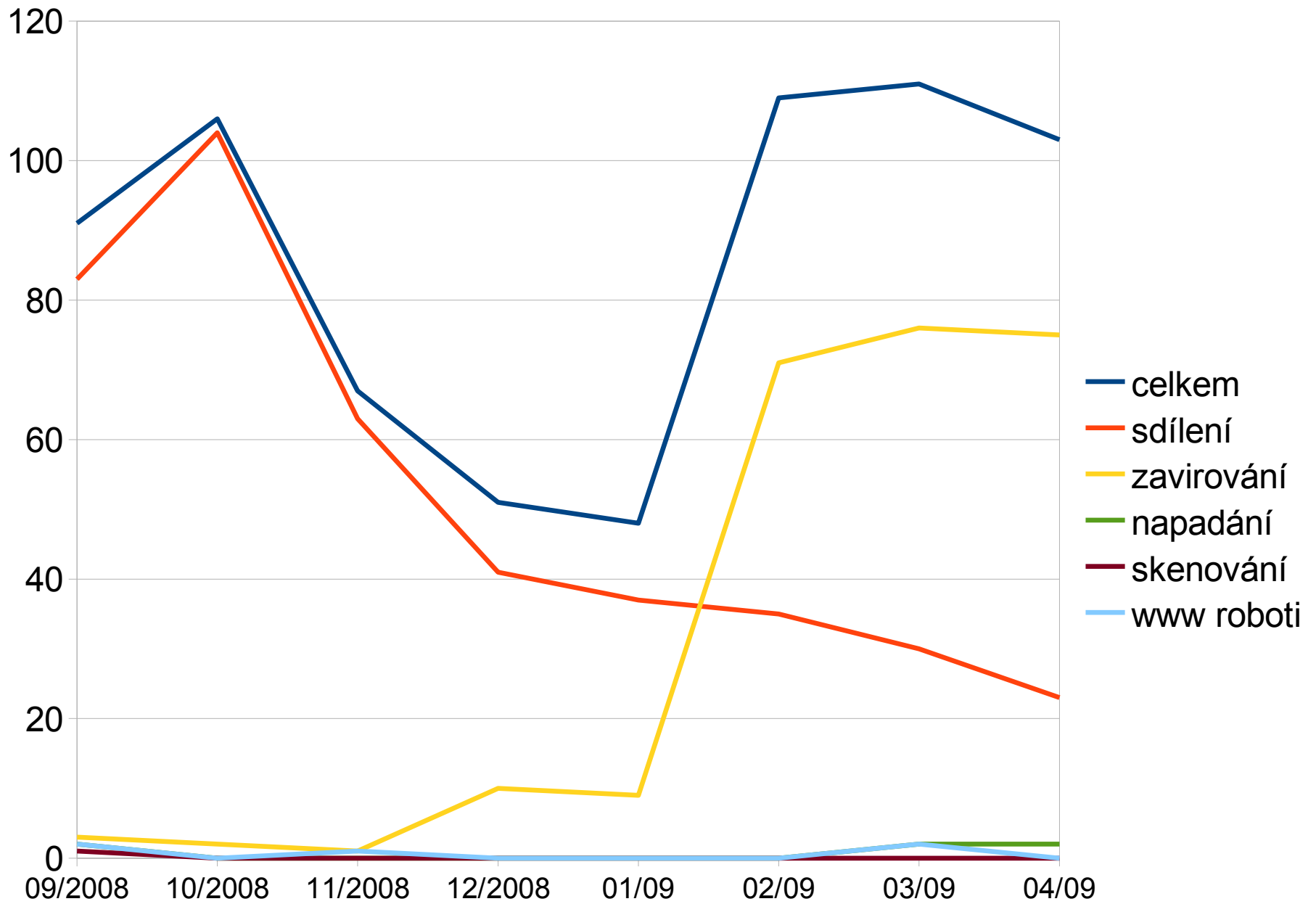
# Zkušenosti

- **Institucionální podpora**
  - vymahatelnost, schválení postupu řešení BI
- **Návody, dokumentace, vzor zasílaných zpráv**
  - konkrétní postupy, FAQ, pravidelná revize
- **Evidence BI**
  - zodpovědnost za řešení
  - zastupitelnost
  - archiv vyjádření
  - recidiva

# Helpdeskový systém



# Ohlédnutí



# Shrnutí

- Vyšetřování
  - bez logů to nejde
- Evidence incidentů
  - dohledatelnost, statistika, kooperace
- Návody
  - odrazový můstek uživatele
- Prevence