Odpovědnost na obzoru

Můžu si dělat co chci?
Může někdo zjistit co dělám?

Andrea Kropáčová

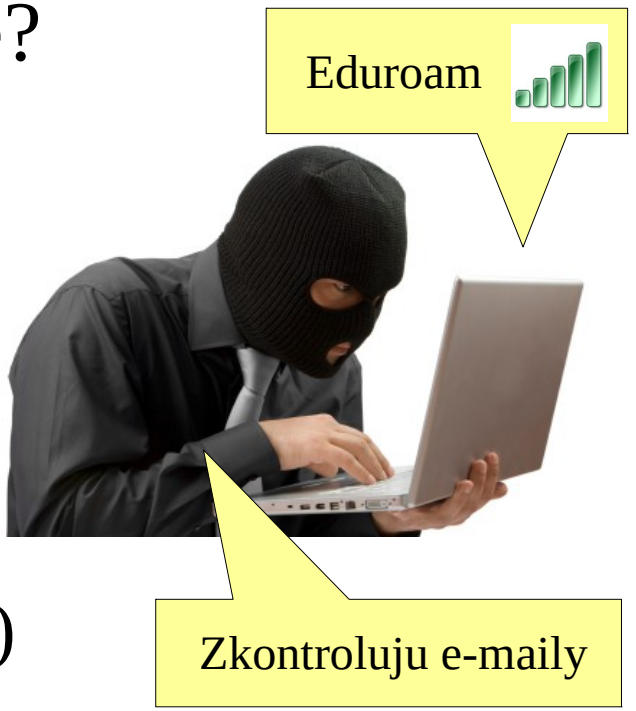
CESNET-CERTS

Úvod

- Univerzitní síť
  - Poskytuje velké možnosti
    - ⇨ přiměřené chování
- Omezení / motivace
  - Morální
    - „To se přeci nedělá!“
  - Technická
    - „To mi nejde ...“
  - Legislativní
    - „To je zakázáno … a trestáno“

Anonymita

- Ale … na síti jsem anonymní, ne?
  - Nikdo neví kdo jsem?
  - Nikdo neví co dělám?
  - Častý omyl
- Přístup do sítě
  - Registrace počítače (pevná síť)
  - Přihlášení (koleje, eduroam)
- Přístup ke službám
  - Přihlášení
  - IP adresa uživatele



Anonymita

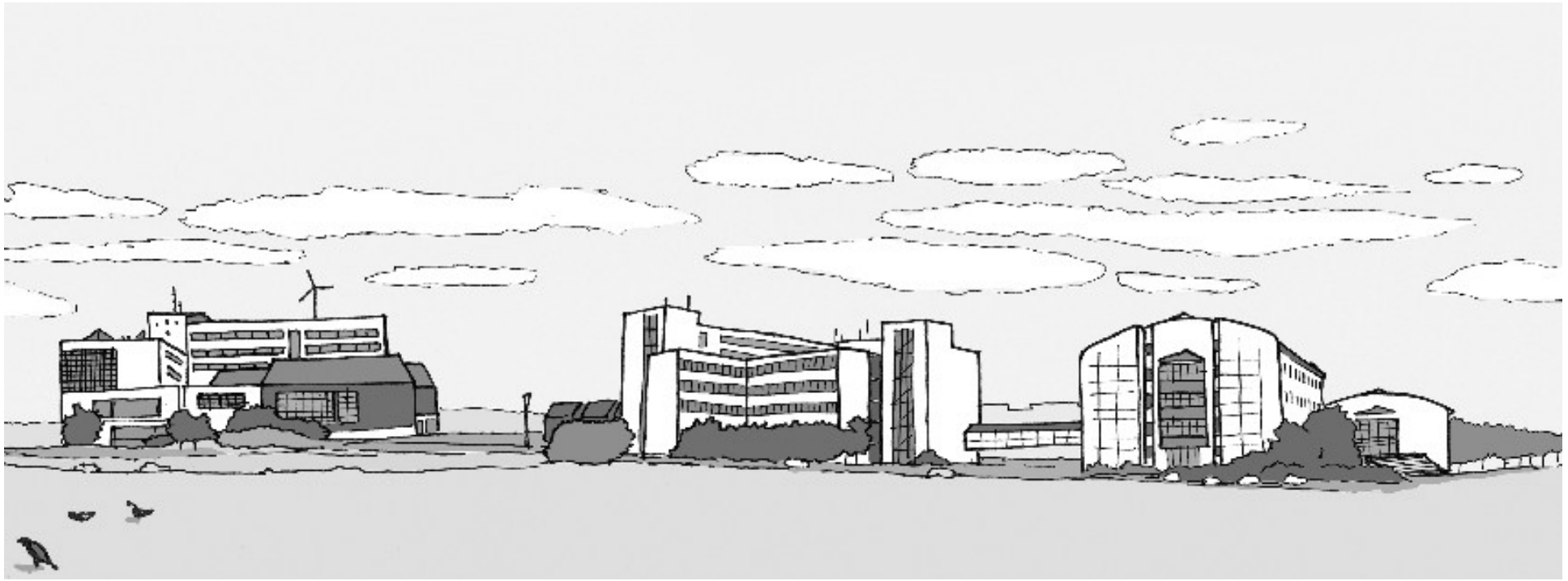
- Záznamy o činnosti
  - Provozní údaje
  - Datová spojení (odkud, kam, kdy, kolik)
  - Audit IS (kdo, co, kdy dělal)
- Vyšetřování incidentu
  - Data k dispozici
  - Kdo, kdy, co, jak, ...
  - Prokázání činnosti
  - Legislativní postihy
- Zodpovědnost je vymahatelná

ZÁPADOČESKÁ UNIVERZITA V PLZNI

A jak je to na ZČU?

Aleš Padrta

WEBnet Incident Response Team



Mantinely chování

- Morální zábrany
  - Uživatelé jsou vzdělaní lidé
  - Rozhled, uvědomění si důsledků
- Technické
  - Pouze základní
  - Akademické prostředí = otevřenost
- Legislativní
  - Pro černé (a šedé) ovce
  - Porušení pravidel tvrdě postihováno

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Legislativní okénko

- Univerzitní směrnice, vyhlášky, provozní řády
  - Jistě sami pilně studujete
  - Neznalost neomlouvá
- **Statut ZČU**
  - Používání univerzitní poštovní schránky
- **10R/2008 Pravidla používání sítě WEBnet**
  - Kdo může síť využívat
  - K čemu všemu se síť smí používat
  - Co je zakázáno provádět
  - Postihy za porušení

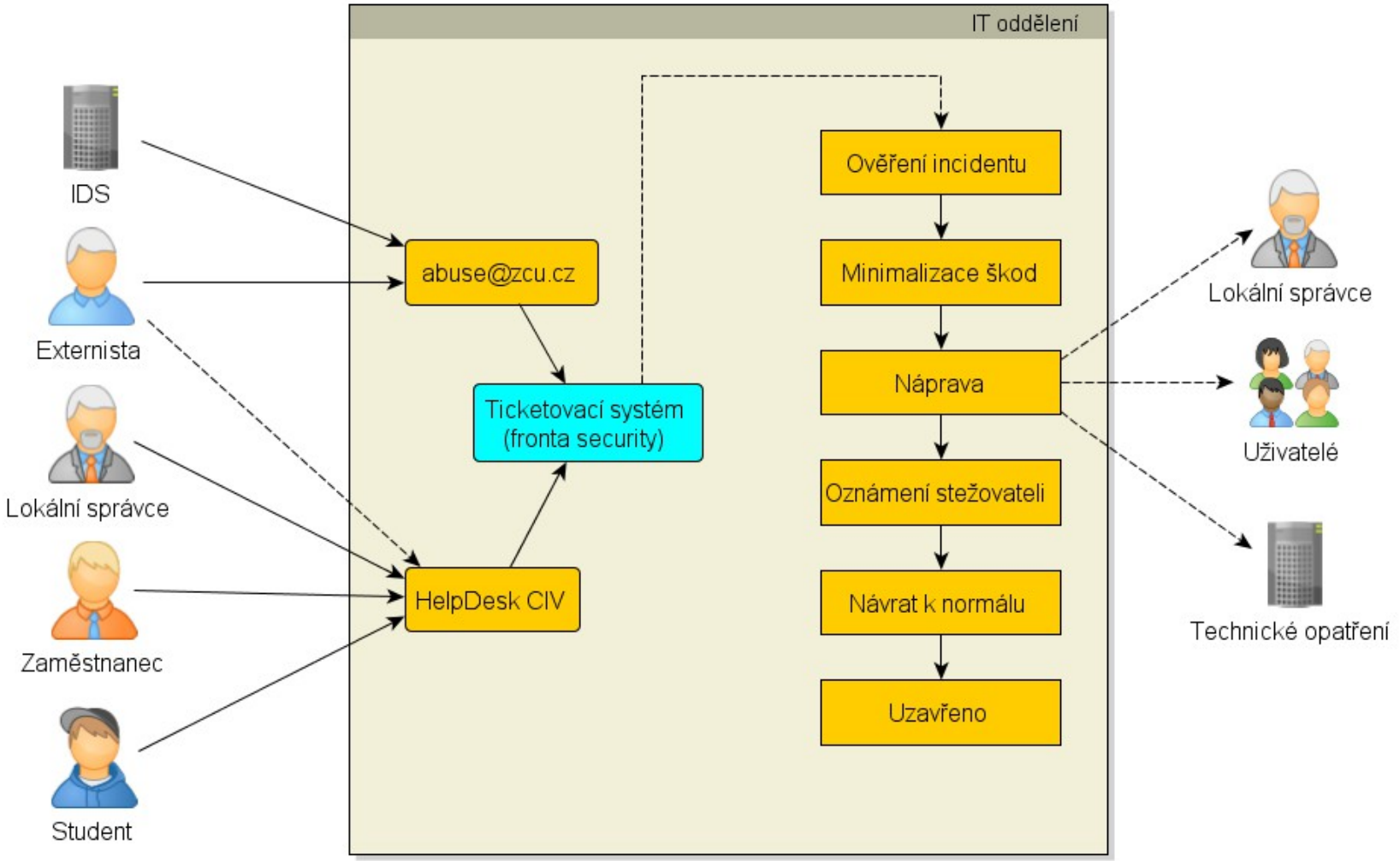
ZÁPADOČESKÁ UNIVERZITA V PLZNI

Legislativní okénko

- **Provozní řád pro připojování mobilních zařízení**
  - Kdo smí používat bezdrátové sítě
  - Zákaz poskytovat připojení dále
  - Řádné zabezpečení
- **Provozní řád kolejních sítí ZČU**
  - Specifika umožňující provoz „komunitní sítě“
  - Registrace, studentská samospráva
  - Řádné zabezpečení
- **Provozní řád veřejných počítačových učeben CIV**
  - Skloubení s výukou
  - Bezproblémový chod (nedrobit do klávesnice apod.)

Řešení bezpečnostních incidentů

- Standardní postup (podle CSIRT)



ZÁPADOČESKÁ UNIVERZITA V PLZNI

Řešení bezpečnostních incidentů

- Nejčastější incidenty
  - Napadené počítače
  - Porušování autorského zákona (P2P)
  - Jiné
    - DoS útok (máme 10Gb/s linku)
    - Poškozování dobrého jména ZČU
    - Rozesílání spamu
    - … porušování dalších článků pravidel
- Upozornění a postup
  - Univerzitním e-mailem (viz povinnost ve Statutu)
  - Lze kontaktovat také HelpDesk (přepošle)

Řešení bezpečnostních incidentů

- Co vás čeká?
- Napadený počítač
  - Občas se stane každému
  - Žádost o nápravu
- Ostatní
  - Osobní návštěva v UI402
- Postihy
  - Domluva
  - Blokování nadstandardních činnosti
  - Eskalace (podnět disciplinární komisi, ...)

Řešení bezpečnostních incidentů

- Přesah mimo ZČU
  - Porušování zákonů ČR
  - Vyšetřování PČR
  - Spolupráce s OČTŘ
  - Medializace ZČU
  - …

- Běží paralelně, nelze ovlivnit
  - Více se dozvíte od trojjediného odborníka

    … ajťák … bezpečák … a právník

Zdroje obrázků

- http://en.wikipedia.org/
- http://jwik.tumblr.com/
- http://www.ynaija.com/
- http://kiwicommons.com/
- http://www.lindakristiansen.dk/
- http://colbycriminaljustice.wikidot.com/