



# CSIRT/CERT

Andrea Kropáčová (CESNET)

3. 4. 2008



# CSIRT/CERT

- **CERT**

- **C**omputer **E**mergency **R**esponse **T**eam

- **CSIRT**

- **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam



# CSIRT/CERT

- Poskytuje služby a podporu v oblasti bezpečnosti počítačových sítí a služeb a to především v oblasti *řešení bezpečnostních incidentů*
- Je **infrastruktura**, která umožňuje
  - Rychlejší a efektivnější reakci
  - Prevenci
  - Spolupráci



# Hlavní role CSIRT

- Nástroj ke zvyšování bezpečnosti síťové infrastruktury
- Edukační – pro provozovatele sítí, uživatele i poskytovatele obsahu
- **CSIRT není nástrojem ani prostředkem represe, kontroly a regulace!**



# Co dělá CSIRT CSIRTem?

- Jasně definovaná „**constituency**“ :
  - Za co zodpovídá (část kyberprostoru/Internetu)
  - Kontaktní informace
  - Poskytované služby - minimem je **řešení incidentů**  
(**RESPONSE**)
- Připravenost na bezpečnostní incident:
  - Plány obrany, obnovy a zvážení rizik

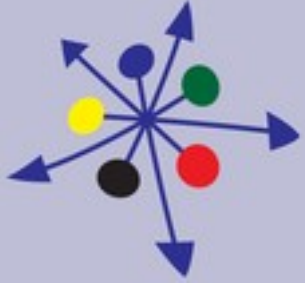


# Čím je zaručena



## důvěryhodnost CSIRTu?

- Musí být plně **transparentní**
- Musí mít **konzistentní** vystupování
- Důraz kladen na **komunikaci** a **spolupráci**
- Otevřenost ke komunitě CSIRTů
- Spolupráce s organizacemi:
  - **FIRST** (<http://www.first.org>)
  - **TERENA** (<http://www.terena.org>)



# CESNET-CERTS

- Oficiálně vznikl v lednu 2004
- Operuje nad sítí národního výzkumu CESNET2
- Má 4 členy
- Status „**accredited**“ přiznán v lednu 2008
- **Přijímá hlášení a reaguje na hlášení bezpečnostních incidentů týkajících se ostatních sítí provozovaných v ČR**

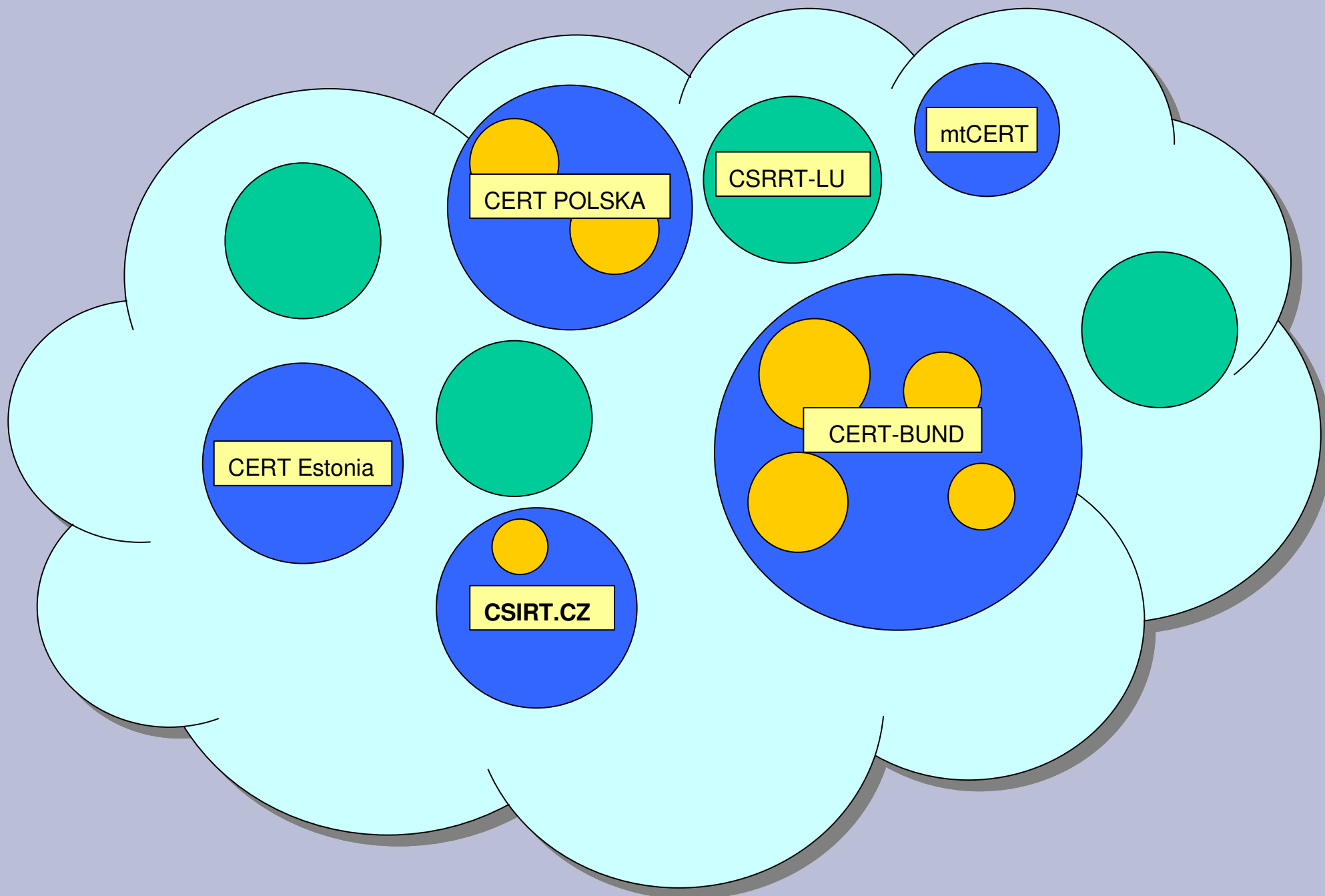


# CSIRT.CZ

- Modelové řešení CSIRT týmu
- Fórum pro výměnu zkušeností a diskusi
- Služby:
  - Proaktivní (varování)
  - Reaktivní - koordinační role při řešení BI
  - Edukativní – školení, publikační a jiná osvětová činnost



# Kyberprostor / Internet





Děkuji za pozornost.