

# **CESNET-CERTS**

**14. 11. 2005**

**Andrea Kropáčová**

**7275 7E6F 39E4 261D FF15 8973 BE2B 53A7 D874 7FE5**

# CESNET-CERTS

- provozovaný sdružením CESNET z.s.p.o.
- členové – Andrea Kropáčová, Pavel Kácha, Pavel Vachek
- založen v lednu 2004
- základní informace na <http://www.cesnet.cz/csirt>

# CESNET-CERTS

## Základní činnosti:

- příjem a řešení bezpečnostních incidentů
- provoz IDS a Audit systému
- antispamová strategie sdružení
- osvěta = podpora zabezpečených způsobů komunikace
- iniciování vzniku **abuse** adres (týmů)
- řešení aktivity CESNET CSIRT

# CESNET-CERTS

## Interní politika vyřizování incidentů:

- příjem adres **abuse**, **certs** a **master** adres domén
- komunikujeme z adresy ***certs@cesnet.cz***
- snažíme se komunikovat anglicky, příp. dvojjazyčně
- používáme el. podpis týmovým PGP klíčem
- pod naši přímou **zodpovědnost** spadají všechny stroje v doménách *cesnet.cz*, *cesnet2.cz*, *eduroam.cz*, *czechlight.cz*, *ipv6.cz*, *acad.cz*, *ces.net* a adresové bloky použité na infrastrukturu CESNET2
- naším **polem působnosti** je celá síť CESNET2

# CESNET-CERTS

## Zpracování přijatého incidentu:

- ověříme jeho relevantnost
- týká-li se naší “**zodpovědnosti**”, kontaktujeme správce daného prvku se žádostí o vyřešení, odpovíme na incident
- týká-li se sítě CESNET2 tzn. naší “**působnosti**”, report přepošleme správci zodpovědnému za danou síť
- další pravidla viz přednáška “Bezpečnostní incidenty ...”

# CESNET-CERTS

## Odpovídání na ohlášené incidenty:

- **odpovídáme** na ty incidenty, u kterých **NENÍ** explicitně uvedeno, že odpověď **není žádoucí**
- v okamžiku přijetí incidentu, který spadá pouze do naší “působnosti”, odpovídáme, že jsme incident přijali a řešíme jej
- v případě, že správce pošle odpověď pouze nám, přepošleme ji autorovi stížnosti

# Štábní kultura CESNET-CERTS

- sdílíme jeden mailbox a jeden PGP klíč
- neaplikujeme antispamovou ochranu
- odchozí i příchozí pošta v jedné složce
- pro odpovědi používáme připravené šablony
- přijaté incidenty archivujeme podle dvou kritérií
  - cílové sítě
  - statusu incidentu (**closed**, **unresolved**, **warn**, **autoreply**)
- veškerou komunikaci archivujeme
- týdenní služby

# Štábní kultura CESNET-CERTS

## Předávání služeb:

- v úterý
- končící služba napíše stručný report o uplynulém “týdnu”
- končící služba zatřídí všechny incidenty ve stavu “closed”, “autoreply” a “warn”
- končící služba zatřídí všechny incidenty starší 14 dní ve stavu “unresolved”

# Další cíle CESNET-CERTS

## Interní:

- zapojit do příjmu a základního zpracování incidentů Cesnet Monitoring Centrum
- užší spolupráce s právním oddělením
- akreditace týmu CESNET-CERTS

## Veřejné:

- posílání urgencí při chybějící odezvě od cílového správce
- podporovat vznik dalších bezp. týmů v CESNET2
- dosáhnout větší interní organizovanosti při řešení bezpečnostních otázek v síti CESNET2