21st TF-CSIRT Meeting

3 - 4 May 2007

Blue Room
Celetna 20
Prague 1
Czech Republic
CESNET-CERTS

Andrea Kropáčová
CESNET
CESNET

• Is an association of legal entities
• Was established in 1996
• operates Czech academic network CESNET2
• Has 26 members = Czech universities and Czech Academy of Science
• Has about 320 “network participants”
• CESNET2 network can be joined by any institution which:
  - Deals with science, research and development
  - promotes culture and shares knowledge
CESNET provides

- CESNET Monitoring Centre (CMC):
  - 8 members (CESNET employees)
  - Supervises CESNET2 network and coordinates solving of network failures
  - 24/7 service

- Network Operations Centre (NOC):
  - 6 members = administrators of the CESNET2's backbone
  - One-week-shift “on-phone”

- CSIRT Team called CESNET-CERTS:
  - Cooperates with CMC and NOC
CESNET-CERTS

• Basic info - http://www.cesnet.cz/csirt

• Participation at TRANSITS Workshop in Warsaw

• “Listed” CSIRT Team in January 2004

• Three constituent members:
  – Andrea Kropáčová, Pavel Vachek, Pavel Kácha
  – Vladimir Trestik = newcomer

• Main services:
  – Incident handling for CESNET2 network
  – IDS and Audit system
  – Organizing workshops for CESNET2 users and admins
CESNET-CERTS constituency

• Receives addresses
  - abuse@cesnet.cz
  - certs@cesnet.cz
  - *master@cesnet.cz (and other CESNET domains)

• Fully responsible for IP addresses marked as INFRA-AW in RIPE DB – Prague's network node and backbone of CESNET2 network

• We cover the whole CESNET2 network (AS2852)

• We can stop the problem in whole CESNET2 network, but we are not allowed to solve it!
CESNET-CERTS work policy

• On service since 8am until 8pm, Monday to Friday
• Share mail folder
• One-week-shift system
• The shift starts on Tuesday
• Brief shift report drafted on Monday evening

• Use mail templates
• Sign every e-mail by PGP key
CESNET-CERTS work

- Disadvantages of our work:
  - Shared mailbox – strict coordination (1 RW, 2 RO)
  - Mail threading problem – incidents scattered through mailbox
  - Routine and tiresome work :-) , most incidents do not need professional erudition
  - Majority of reported incidents belongs to the CESNET2 members network and must be forwarded to the end-network
  - On duty since 8am until 8pm, Monday to Friday
CESNET-CERTS goals

• To provide non-stop incident handling service for the CESNET2 network

• To negotiate basic rules for incident handling for the CESNET2 network (security policy):
  - CESNET2 Incident Response Policy
  - CESNET2 Incident Handling Policy

• To establish a CSIRT Team in every CESNET2 member's network
How to achieve our goals ...

- CESNET Monitoring Centre (CMC) will provide basic *incident handling* for CESNET2
- We tested – RT, RTIR, Mantis ...
- Tweaking OTRS to our needs
- Tutoring members of CMC on incident handling
- CMC handles basic incidents as follows:
  - Open and read every report
  - Recent reports forwarded to the end-network
  - Complicated reports forwarded to the CESNET-CERTS front
Thank you for your attention.

Any questions?