RoCSIRT

Agency ARNIEC / RoEduNet CSIRT

Manuel ŞUBREDU – Istambul, 16-09-2010
About RoCSIRT

History:
- Late start
- First participation to TRANSITS course in July 2007 (Sofia)
- Discussions about the service started in August 2008
- First public ‘announce’ of the new service at RoEduNet International Conference (August 2008)
- Service became operational on January 2009
- TI listed status in April 2009
- TI accredited status in August 2009
- First participation to TI closed meeting in September 2009 (Tallinn)

Constituency:
- all RoEduNet connected institutions (mostly higher education, education and research institutes)
- all .ro (just for incident coordination)
Services

- Most used:
  - Incident handling
  - Incident response coordination for .ro
  - Alerts and warnings (distribution of some of the information received from outside sources)
  - Technical assistance for constituents in incident handling
  - RT::IR for incident management

- In test:
  - RBL
  - DarkNet
Our first year (2009, in numbers)

- ~ 600 incidents reported via email
- ~ 110 Copyright Infringement
- ~ 440 spam reports
- ~ 20 compromised machines
- 8 international incidents
- 90% awareness rate (and possible success rate) in copyright infringement incidents
- 5% success rate in spam incidents
- ~ 15 stable and reliable contacts (banks, commercial ISP’s)
This year

- Some numbers:
  - ~ 1600 reported incidents
    - 70% reported to constituents, from which 30-40% were solved)
    - 30% - no answer or insufficient data for us or the constituent

- What we focus on:
  - implementing new services
  - knowing our constituency better
  - more participation on the CSIRT community
  - development of custom tools
  - integrating NREN services into RoCSIRT (eg: flow analysis)

- Problems:
  - VERY short on man power
  - Difficult constituency
Work in progress

- Advertise ourselves (and the provided services) to our constituency (connected institutions)

- Custom tools:
  - RT::IR custom modules for:
    - Automated incident handling (copyright infringement reports, spam reports)
    - Improved statistics
    - Using external information (custom databases)
  - Tool to manage and distribute security advisories
  - Distribution of security advisories from vendors
  - Use of other sources of information (flow analysis, honey pots, etc)

- Establish as much contact as possible within our constituency
Thank you!

RoCSIRT – team@csirt.ro