The Spanish case

ENISA Workshop: “The role of CERT teams in National incident response plans” 29th May 2008, Athens, Greece

Joaquin Castillejo. TB-Security CEO

Agenda

- National context
- Lessons learned
- Conclusions

National context

- Background:
  - At national level, we have four “community focused” players, CCN-CERT, CNPIC, INTECO-CERT, IRIS-CERT, each of one serves respectively:
    - The Government
    - The Critical Infrastructures
    - The SMEs and Citizens
    - The Academic sphere
  - And a fast growing regional government sponsored initiatives with a “broad community” model, serving all communities in their region
  - Limited development of private or industriy supported initiatives

National context (II)

- Established CSIRTs
  - National level:
    - CCN-CERT (2007): National Government
    - INTECO-CERT (2007): SMEs & Citizens
    - IRIS-CERT (1997): Academic sphere
  - Autonomic (Regional) level:
    - CSIRTCV: Valencia's Government, SMEs and Citizens
- Other CSIRT initiatives:
  - Regional Governments: Cataluña, Andalucia, etc.
  - Private: e-La Caixa (Bank)
- Related activities at national level
  - CNPIC: Critical Infraestucture Protection

National context (III)

- Government/Legislative support
  - Plan Avanza:
    - Spanish ICT Strategic Plan (2006-2010) supports the “creation of a national network of information security coordination centers”
- Coordination activities
  - One formally established coordination group:
    - ABUSE-ES (2005): Sponsored by IRIS-CERT. Aimed at ISP and technician focused. Objetive: Information and good practice sharing about typical ISP threads (spam, virus, troyans,...). E-COAT member
  - Mainly informal and/or bilateral relationships between players starting at 2008

Lessons learned

- Sorry, we can't talk about “good established” practices, which are just being started right now!
  - CCN-CERT is working on a “National good practice guide” to help other initiatives to create their owns CSIRTs, and to establish a first common cooperation/coordination model, collecting needs and comments from others CSIRTs
- Main needs:
  - Framework and formal criteria to coordinate incidents between national CSIRTs
  - Knowledge and trainning about CSIRT funding, creation and operation
  - “Shared services”, especially those which require larger investments

Lessons learned (II)

- First ideas:
  - Promote a National Spanish CSIRT Association
    - Possible Members: Public & private, established or new CSIRTs, inviting other related key players: Defense, Homeland Security Forces, Security Industry, ICT Associations
  - Promote private sector and industry specific CSIRTs
    - Priority: Critical Infraestructure Operators
  - Rethink “national community focused CSIRTs” strategy, as a Coordination Centers of their respective constituencies
    - Developing, coordinating, and offering value added services to other regional/specific CSIRTs initiatives
      - Quality information fees: help detecting, warning, responding and recovering from incidents
      - Trainning services for CSIRT creation and operation
      - Created a trusted community and promoting a good practice exchange between members
      - Support Incident Response Services for constituencies without specific CSIRT

Conclusions

- We are in a first stage, but moving fast!
- We need an agreed national CSIRT framework in the next months
- We need to develop our national CSIRT market
- We really need to share good practices with others nations! Comments are welcome!