TF-CSIRT – Collaboration of Security Incident Response Teams

Update

Baiba Kaskina

TERENA

baiba@terena.nl

Agenda

- CSIRT Task Force (TF-CSIRT)
  - Creation
  - The way of working
  - Involved countries
- Deliverables & projects, including:
  - Trusted Introducer
  - IRT database object
  - Training course for CSIRTs
- Questions

Creation of TF-CSIRT

- TERENA Task Force:
  - Operation defined by Terms of Reference
  - Two years recurring lifecycle with review
  - Members and non-members of TERENA
  - No membership fee, just travel & hotel costs
  - Active participation by members
  - Success depends on members’ commitment
  - TERENA plays role of professional facilitator:
    - Secretarial tasks
    - Logistical support

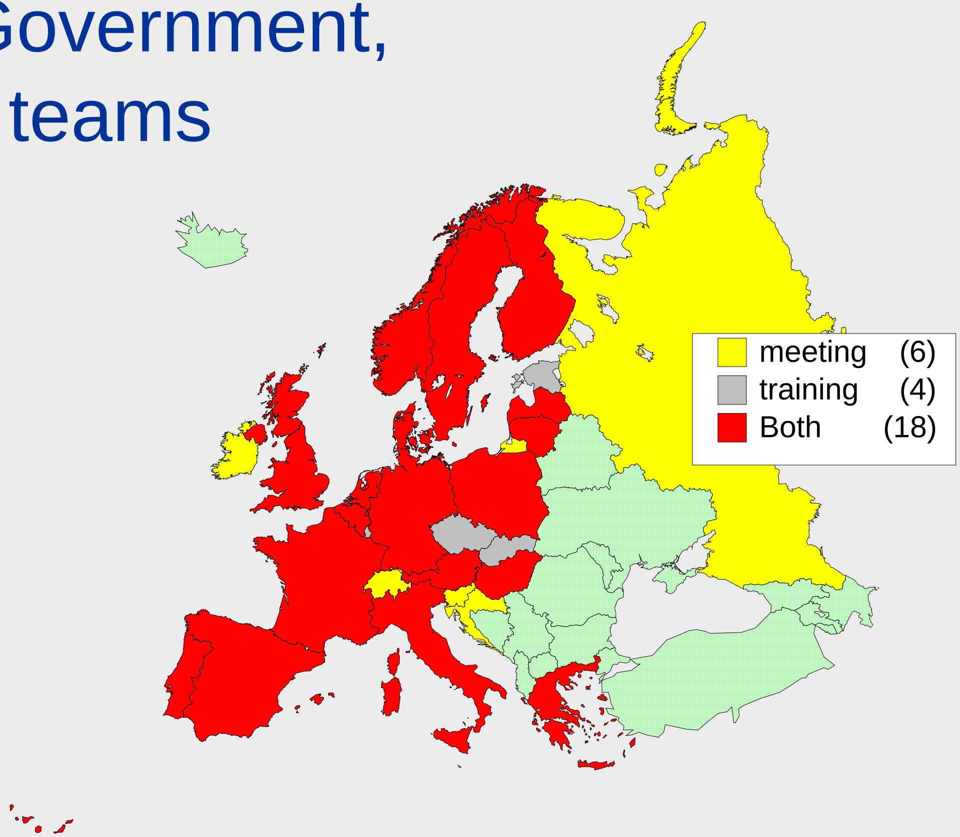
TF-CSIRT way of working

- Meeting every four months
- Venue rotates among members who volunteer to host
- Two days:
  - 1st day for seminars and presentations
  - 2nd day for Task Force official meeting
- Evening in-between: social event organised by the hosting member
- Contacts between meetings provided by mailing list and project groups

Next meeting – 25-26 September, Amsterdam

Who is involved?

- Academic, Government, Commercial teams
- 28 countries



Deliverables and Projects

- Trusted Introducer Service & Directory
- Incident Object Description & Exchange Format
- RIPE IRT object
- Clearing House for Incident Handling Tools
- CSIRT training course (TRANSITS)

Under development

- Incident Information Exchange (eCSIRT.net)
- Vulnerability information exchange (EISPP)
- Assistance to new CSIRTs
- Incident Handling Procedures

Deliverables – Trusted Introducer (http://www.ti.terena.nl/)

- Notion of ‘trust’ – is a contact trustworthy?
- Currently, no scheme generically applicable
- TF-CSIRT to work out a model of which it believes it fulfills criteria needed at operational level
- Feasibility and sanity checks
- Now, outsourced to a 3rd party
- TF-CSIRT retains control by TI Review Board

Deliverables – IRT database object

- Commonly perceived problem: correct points of contact in (RIPE) database
- Practical approach:
  - what do we miss now?
  - how can we design it
  - how can we implement it?
- Wishlist followed by discussion in RIPE database group
- Lots of iterations, but eventually implemented and populated

Deliverables – TRANSITS

(http://www.ist-transits.org/)

- Teams were seeking relevant training
- Idea: best transfer of knowledge is from operational people to operational people
- Conclusion: best people to write it are TF-CSIRT members
- Two day course developed in modules:
  - Operational, legal, technical, organisational, vulnerabilities
- EC funding for delivery and updating
  - Six presentations over three years
  - Materials available to members for own use

Questions?