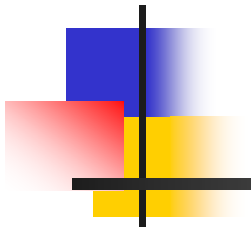


European Governments CSIRTs (EGC)

Hedy van der Ende, GOVCERT.NL
David Parker, NISCC
Johan Mårtensson, SITIC

CERTs in Europe – Lessons Learned and Good Practices
Dec 13 2005, Brussels, Belgium

Contents

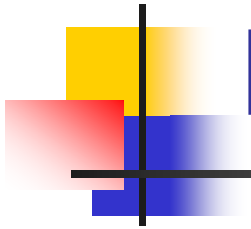
- Objectives of the presentation
- Background
- EGC Members
- EGC activities & objectives
- TF-CSIRT, FIRST and ENISA
- Future cooperation

Objectives of the presentation

- Describe what EGC is and what it is not
- Describe the reasons behind forming the EGC group
- Describe how EGC relates to other organisations

Background

- Worldwide - Large number of CSIRTs involved in incident management
  - Most primarily interested in purely technical issues
  - Many are not capable of responding to regional or global requirements for incident management
  - Vast majority have no involvement in national policy for protecting CNI structures
- Need for higher level of trust at a national level in dealing with such issues
- Therefore regional national groupings have emerged
  - AP-CERT
  - OAS activity
  - European Government CSIRTs Group (EGC)
  - Africa ????



EGC members

- CERTA (France)
- CERT-Bund (Germany)
- CERT-FI (Finland)
- GOVCERT.NL (The Netherlands)
- NorCERT (Norway)
- SITIC (Sweden)
- UNIRAS/NISCC (UK)

EGC activities

- Operational group
  - Government related topics
  - Information exchange
  - Meetings every 4 months approximately
  - Establish standards and best practices
  - Formalised through Mutual agreement of scope

Scope of EGC activities

- EGC is technically focused on incidents and vulnerabilities
- EGC represents common views of the members on CSIRT matters
- The aims of EGC are supported by the parent organisations

Objectives of EGC (1)

- Jointly developing measures to deal with large-scale or regional network security incidents
- Facilitating information sharing and technology exchange
- Identifying areas of specialist knowledge and expertise

Objectives of EGC (2)

- Identifying areas of collaborative research and development on subjects of mutual interest
- Encouraging formation of governmental CSIRTs in European countries
- Communicating common views with other initiatives and organisations

Achievements

- Established trusted relationships between Governments that allow the exchange of sensitive material in relation to incidents
- Established cooperative working relationships
- Actively inform each other on incidents (24*7 mailing list and telephone)
- Members leverage other global international relationships in order to benefit the EGC group
- Keep track of international projects and take part where possible

Relationship to TF-CSIRT

- EGC supports TF-CSIRT and other CSIRT activities in Europe
- EGC teams are members of TF-CSIRT
- EGC recognises that TF-CSIRT:
  - has been and is successful in establishing CSIRT cooperation in Europe
  - has an important role in developing technical CSIRT initiatives in Europe
  - is successful in developing a number of collaborative projects between CSIRTs in Europe

Relationship to FIRST

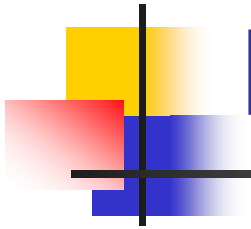
- EGC supports FIRST
- EGC teams are members of FIRST
- EGC recognises that FIRST:
  - is the only worldwide CSIRT forum
  - is successful in providing access to best practises, tools and trusted communication with member teams
  - constitutes a neutral interconnect for CSIRTs and vendors

Relationship to ENISA

- EGC supports ENISA – “the same parents” and mutual interests
- EGC member teams participate actively in ENISA activities
- EGC contributes deliverables to the ENISA portfolio

Future Cooperation

- Share CIIP information
- Work on projects/sharing knowledge
- Support ENISA activities and similar initiatives
- Establish a trusted relationship with other regions
- Establish operational contacts with and within the AP-region
- Establish EGC web site



EGC

- CERTA (France)
- CERT-Bund (Germany)
- CERT-FI (Finland)
- GOVCERT.NL (The Netherlands)
- NorCERT (Norway)
- SITIC (Sweden)
- UNIRAS/NISCC (UK)