Computer Security Cooperation in Europe

Gorazd Božic, SI-CERT, ARNES, Slovenia
gorazd.bozic@arnes.si

Jacques Schuurman, CERT-NL, SURFnet bv, The Netherlands
jacques.schuurman@surfnet.nl

Andrew Cormack, UKERNA, United Kingdom
a.cormack@ukerna.ac.uk
Agenda

• Roles of CSIRT / CERT / IRT
• A bit of history
• European CSIRT cooperation: TF-CSIRT
• Questions
Acronyms

• CSIRT – Computer Security Incident Response Team
• CERT – Computer Emergency Response Team
• IRT – Incident Response Team

All do similar things
Roles of CSIRT

• Proactive
  – Technical expertise
  – Information dissemination

• Reactive
  – Assistance for recovery from attack
  – Cooperation with other CSIRTs
Historical perspective

• Pre-1990: CSIRTs in isolation (if at all)
• During 1990s: FIRST provides binding:
  – Members meet members
  – Basic notion of trust
  – Exchange of operational information
  – Less powerful in initiating innovation
• Mid 1990s: EuroCERT pilot service:
  – Top-down approach
  – Operational work outsourced to 3rd party
• 2000: TF-CSIRT established
TF-CSIRT
http://www.terena.nl/tech/task-forces/tf-csirt/

- TERENA Task Force:
  - Two years recurring lifecycle with review
  - Members and non-members of TERENA from research & education, commercial and governmental sectors
  - Active participation by members
  - Success depends on members’ commitment
  - TERENA plays role of professional facilitator:
    - Secretarial tasks
    - Logistical support
TF-CSIRT members

Complete listing available at http://ti.terena.nl/
Why is cooperation essential

• Internet has no borders
• Assistance in incident resolution
• Sharing information, know-how and resources
• Learn from other teams
• Create standards and best practices
TF-CSIRT projects

<table>
<thead>
<tr>
<th>Developed</th>
<th>Under development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Introducer Service &amp; Directory</td>
<td>Incident Information Exchange (eCSIRT.net)</td>
</tr>
<tr>
<td>Incident Object Description &amp; Exchange Format</td>
<td>Vulnerability information exchange (EISPP)</td>
</tr>
<tr>
<td>RIPE IRT object</td>
<td>Assistance to new CSIRTs</td>
</tr>
<tr>
<td>Clearing House for Incident Handling Tools</td>
<td>Incident Handling Procedures</td>
</tr>
<tr>
<td>CSIRT training course (TRANSITS)</td>
<td></td>
</tr>
</tbody>
</table>
Trusted Introducer
http://ti.terena.nl/

- European CSIRT directory
- Notion of ‘trust’ – is a contact trustworthy?
- Feasibility and sanity checks
- Outsourced to a 3rd party
- TF-CSIRT retains control by TI Review Board
• Training workshops
  – 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
Other activities

- Collaboration with European Commission
  - eEurope action plans
  - ENISA (European Network Information Security Agency) project
Questions?