GÉANT3 Security activities

Wayne Routly (DANTE)
TF-CSIRT, Heraklion 20.05.2010.
GÉANT3 and SA2/T4

- Started April 1st 2009

- SA2: multi-domain services
  - Extending / engineering GÉANT2 developments
  - IP Network monitoring, Layer2 or wavelength circuit setup, cross border fibre activation

- SA2/T4: support the secure development and deployment of multi-domain services
How?

- Preventing problems: **SED** (Security Expertise Delivery)
  - Help developers to embed security in the design and implementation of GN3 services
  - Help administrators and NOC engineers to embed security in the deployment and operations of GN3 services
  - Educate users of services to good security practices (strong passwords, understand certificates, phishing, etc.)

- Preparing for the worse: **MDSEC** (MultiDomain SECurity)
  - Help NRENs security teams (all, not only those involved in T4) to better prepare to solve incidents related to GN3 services
SED: some more details

**Educational component**
- Cookbooks, training
  - *Cookbook v1*
  - *Security coding training* (Poznan, 22-23 June 2010; 20 places, already full!; code developers in GN3 project)

**Security Consultancy**
- Team of “experts” who can consult on demand on specific topics
- For people working in GN3 project or operationally supporting GN3 services
- developers, administrators, NOCs, and NREN CERT people
- sort of “**L3 support**” for security in GN3
- 3 cases already dealt with
MDS: some more details

**Tools:** Help NREN CERTs to deploy a (functionally) consistent set of security tools
- Web questionnaire circulated late 2009, results presented at Jan. 2010 TF-CSIRT (18 answering entities)
- Now more details asked about tools: ≈ 40 answers received
- Analysis process just started: goal is identify gaps and help CERTs to overcome them, by providing e.g. installation guidelines, examples of deployments and usage, etc.

**Workflows:** Define a Multi-Domain Services security incident handling workflows that enhances current practice
- 5 Sections – Modular
- Notification through till Dissemination
MDS: Multi-domain Handling Process - Investigation & Resolution

- Investigation & Resolution
  - NREN Operations Team
    - Forensic Investigations
    - Notify Affected Domains
  - Procedures over incident (Operations)
  - Virtual Security Team
    - Notify Other Domains
    - Consultation
    - Signal Bug
  - Steps taken to return to original status
- Service Development Team
  - Bug Fix
    - New Version
    - The Service Development Team will be taking the needed solutions
  - Procedures over Bug

connect • communicate • collaborate
Conclusion

- SA2 & SA2T4
- SED – Preventing Problems
  - Educational
  - Consultancy
- MDS – Preparation & Mitigating
  - Tools
  - Workflow
  - 5 Sections
Questions?

wayne.routly@dante.net