Multi Domain Security - CERTs
Protecting the Project

Wayne Routly, DANTE/GEANT
TF-CSIRT Meeting
Luxembourg.lu, 23 September 2011
Before • • • •

connect • communicate • collaborate

Panic
An intro to what NREN CERT teams are doing, to protect the services in the project
Contents

- GEANT: Who What How
- Who Are We?
- What Security Aspects
- What can we do about this?
  - What are we doing to Handle Incidents?
  - What are we doing to Protect Deployments?
  - What are we doing to improve IH & MDS Tools
- Useful Links & Contacts
- Conclusion
- Questions & Answers
GEANT: Who What How

- State of the Art Pan-European Network
  - Transit Network...ISP
  - 18 Physical Pops
- 40 GB links -> 100GB
  - TB of Data shifted
  - 10 million+ IPs
  - 100 Workstations
  - Unusual Traffic
- Truly Global
  - Interconnects – 5+
  - NRENs - 38
  - Commercial & Commodity Traffic - 8/2
Who Are We?

- Service Activity 2 Task 4 (SA2T4)
  - Multi Domain Security Team
  - 15 CERT Teams
    - +/- 25 Pax
  - 6.60 FTE Year 3
- AutoBAHN, Perfsonar, cNIS, I-SHARE
- Responsible for...
  - Tools
  - Deployments
  - Incident Handling
  - Training
Security Aspects.....

- Software making automated changes to my network!
- Who is allowed to make these changes…are they authorised?
- Is my equipment and software secure?
- How do I handle Multi Domain Security Incidents?
- Who can answer all my security questions and what are they?
- Am I protected?
What are we doing to **Handle** Incidents

**Knowledge Base (KB)**
- Tracks Incidents
- Resource

**MDS Incident Workflow**
- Process for Handling Incidents
- Liaising with NREN CERTS, with Dev Teams
- Informing Community

**Virtual Security Team (VST)**
- Virtual CSIRT
- Provides Technical Knowledge
- Provides Communication Conduit
What are we doing to Protect Deployments

- Security Expertise Consultancy
  - Study results from Risk Assessment & Pen testing
  - Feed results to community through cookbook
  - Provide consultancy to deployments
  - Provide consultancy to developers

- Optional Component
  - Test the defences
  - Look at deployment from an attacker’s perspective

- A Security Guide
  - What areas are affected
  - Where to get advice
  - Get solutions

- Review the Security of Deployments & New Software Versions
  - Provide surety through evaluating risk

connect • communicate • collaborate
What are we doing to **improve** IH & MDS Tools

- Are the processes to handle incidents working?
- Is additional support / expertise needed?

**Security Expertise Consultancy**
- Central contact for security related queries
- Provides consultancy requests
- Supports VST & KB

**Firedrills**

**Secure Code Training**
- Provide best practice
- Provide mitigation techniques
- Increase security awareness amongst developers

GÉANT
Conclusion

- GEANT – Big Network…Big Project
- Multi-Domain Security Team
- Security Aspects
- Handling Incidents
  - Knowledge Base
  - Virtual Security Team
  - MDS IH Workflow
- Protect Deployments
  - Security Cookbook
  - Pen Testing
  - Risk Assessments
- Improving Incident Handling & The Software
  - Secure Code Training
  - Fire Drills
Questions & Answers

QUESTIONS ANSWERED HERE EVEN THE SILLY ONES
Thank You

Wayne Routly – SA2T4 Leader
wayne.routly@dante.net
Key ID: 0x27269182