



Connect. Communicate. Collaborate

GÉANT2 Security: Year 1 (aka JRA2)

Christoph Graf, SWITCH

TF-CSIRT, Lisbon

16 September 2005





Connect. Communicate. Collaborate

Introduction

- JRA2 aims at:
 - improving the overall security within the GÉANT2 community
- JRA2 fits into GÉANT2 project by:
 - engaging existing security teams of GÉANT2 partners
- Number of partners: 12
- Main partners: CESNET, DANTE, GARR, GRNET, SURFnet, SWITCH





Connect. Communicate. Collaborate

Introduction

- JRA2 consists of the following Work Items:
 - WI-0: Management (SWITCH)
 - WI-1: Securing GÉANT2 network elements and services (DANTE)
 - WI-2: Building of security services (SURFnet)
 - WI-3: Designing and establishing an infrastructure for co-ordinated security incident handling (GARR)
 - WI-4: Relationship with TF-CSIRT (SWITCH)
 - WI-5: Establishment of advisory panel (SWITCH)





Connect. Communicate. Collaborate

Year 1 - Objectives

- O-1: Equip GÉANT2 and NREN networks with capabilities to become more proactive...
- O-2: ... and co-ordinated
- O-3: Enable intervention on the GÉANT2 backbone network on behalf of and to assist security experts protecting their users
- O-4: Use results of existing initiatives, namely: TF-CSIRT, eCSIRT.net
- Guiding principles:
 - Motivate security teams to take responsibility for their own domain!
 - Show the teams how to do that!





Connect. Communicate. Collaborate

Year 1 - Achievements

- A-1: Set of tools identified, tested and assessed (WI-2)
 - >>> (separate slide)
- A-2: Co-ordination infrastructure designed and tested (WI-3)
 - >>> (separate slide)
- A-3: Traffic cleaning capability proposed to GÉANT2 backbone (WI-1)
 - >>> (separate slide)
- A-4: Clear definition of roles with TF-CSIRT (WI-4)
- A-5: Work of JRA2 assessed by Advisory Panel (WI-5)

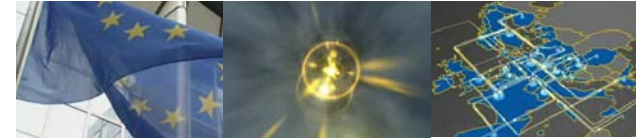


A-1: The “Swiss-Army-Knive” for security teams



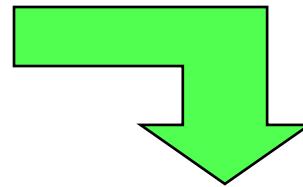
Connect. Communicate. Collaborate

- Set of tools identified, tested and assessed
- “The Toolset” elements:
 - The Netflow probe (by CESNET, prototype stage)
 - The traffic scanner (by CESNET, architecture defined)
 - NERD (by Surfnet, in production by several teams)
 - NFSEN (by SWITCH, in production by several teams)
- Assessment of productive elements
 - Good functionality, documentation needs improvement
 - Not easily deployable
 - Tuning required to address interworking and overlap issues

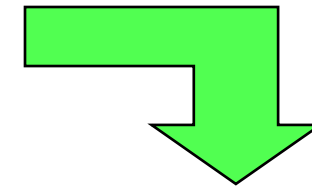


Connect. Communicate. Collaborate

Toolset element: nfsen



From the big picture to the needle in the haystack



A-2: The operational framework for “the toolset”



Connect. Communicate. Collaborate

- Co-ordination infrastructure designed and tested (M13)
- Surveys made on:
 - Incident handling practices
 - Automated/standardised information exchange between CSIRTs
 - Tools/protocols in use & experiences
 - Electronic credentials used for incident handling
- Definitions made on:
 - Incident severity classification and response time expectation
 - Incident exchange format
- Alert mailing list set up



A-3: The wish list of the JRA2 partners



Connect. Communicate. Collaborate

- Traffic cleaning service proposed to GÉANT2 backbone operator
- Proposed customer triggered DoS mitigation services (GÉANT2 core):
 - Traffic black holing service:
 - Goal: reduce collateral damage, but breaks service under attack
 - To be realised with standard GÉANT2 core components
 - Traffic cleaning service:
 - Goal: maintain service, even under attack
 - Requires additional GÉANT2 core equipment (funding requested)





Connect. Communicate. Collaborate

Year 2 + 6 months

- Objectives changed how?
 - WI-2: Tools: from “what’s there?” to “what’s missing?” & “make it!”
 - WI-1/3: Co-ordination: Moving from “design” towards “service”, covering training, BCP statements and policy requirements
- Future risks:
 - Major incidents may dramatically shift priorities and interests within the security community



Connect. Communicate. Collaborate

Conclusions/Summary

- JRA2 is about helping security teams to do a better job
 - By enhancing their capabilities (WI-2)
 - By embedding the teams in a partner network (WI-3/4)
 - By offering additional central services (WI-1)
- But the security teams need to protect *their* network *themselves*!
- In order to protect the GÉANT2 community, *all* partners have to do it!
- To mitigate risk, GÉANT2 will *require* its partners to do it!
- Without GÉANT2, this would not happen, or happen much later

