GÉANT2 - Security (JRA2)

Christoph Graf, SWITCH
TF-CSIRT, Amsterdam
23 January 2006
Recap

• GÉANT2 - Security aims at:
  – improving the overall security within the GÉANT2 community

• Main areas of activity
  – Improve the tools and collaboration framework of GÉANT2 security teams
    • “The Toolset”
    • The GÉANT2 co-ordination infrastructure
  – Explore the possibility to offer centrally provided services to GÉANT2 security teams
    • Traffic blackhole service of GÉANT2
What’s new in 2006?

• (JRA Meeting, Cambridge, January 2006)
• Tools:
  – from “what’s there?” to “what’s missing?” & “make it!”
• Co-ordination:
  – from “design” to “implementation”
  – covering training, BCP statements and policy requirements
• Central services: From “design” to “implementation”
• Risks (unchanged):
  – Major incidents may dramatically shift priorities and interests within the security community
Looking at Risks

GÉANT

- GÉANT is (was) connected with NREN networks
- Securing GÉANT means protecting against customer network influence

GÉANT2

- GÉANT2 is in parts based on NREN network services (e.g. lightpath provisioning)
- Securing GÉANT2 implies securing the partner networks: requiring minimum security standards

->> Insecure partner networks pose a threat to GÉANT2
->> This risk needs to be managed by GÉANT2
Proposed new focus

“Increase GÉANT2 overall security!”

• Challenges:
  – Help security-challenged NRENs to improve security
  – Security-challenged NRENs underrepresented in security activities (thus, try to get them on-board)
Success factors

• Management commitment
  – Defining minimum security standards for all partners
• Separating applied research and operations (JRA vs. SA)
  – Deploying JRA2 results and offering training -> SA
• Involving the affected
  – JRA2 members likely to fulfil minimum standards
  – We need the involvement of partners below standard
• Community spirit
  – Experts to train the ones below standard