

# Grid Security Developments

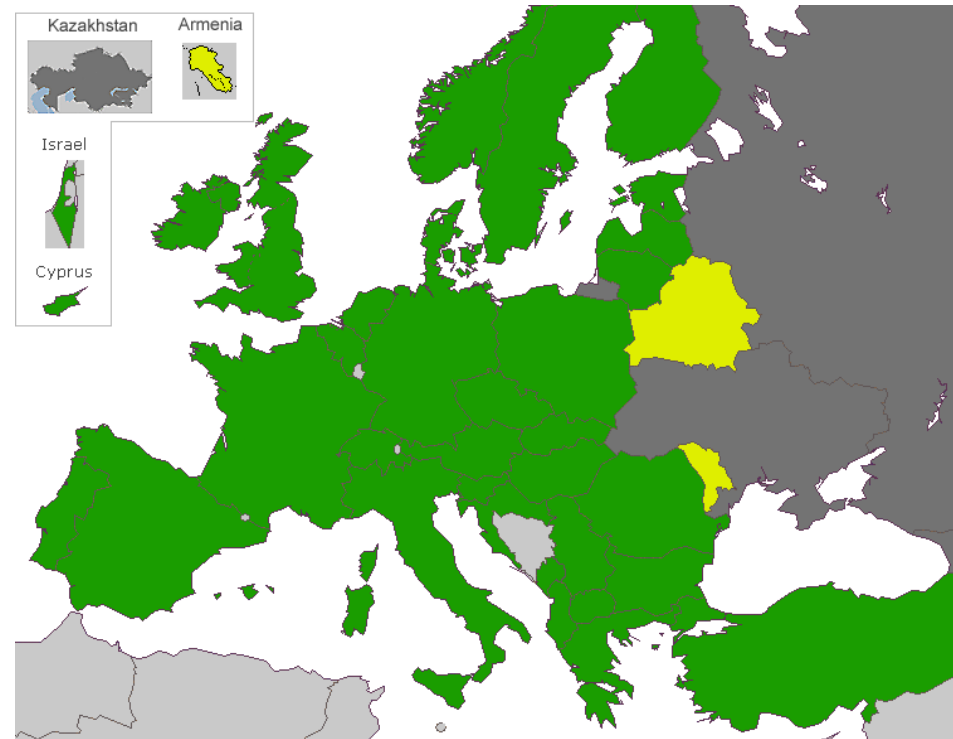
Daniel Kouřil, CESNET

# European Grid

- EGEE
  - Regular daily production
    - 250 sites, 150,000 CPUs, 30 Petabytes of storage
    - Tens of hundreds jobs per day
- Site autonomy as a key corner-stone
  - Sites are independent and fully responsible for their resources
  - Grid participants bound by access policies
    - e.g. to properly handle incident and communicate information
- Project-based funding, finishing in April 2010

# EGI

- Believed to start in May 2010
- Long-term activity, eventually funded by the NGIs
- Each participating country represented by a single NGI
- Coordination provided by EGI.eu



# Operational Security in EGEE

- EGEE CSIRT
  - EGEE Operational Security Coordination Team (OSCT)
  - Listed in TI
- Incident handling & coordination
- Proactive services (monitoring, training, drills)
- Several parties involved
  - EGEE (grid provider)
  - Sites (Resource providers)
  - Virtual organizations (Users)
- Binding policies

# Incident Response Procedure

- Inform your local security team/ROC Security Contact
- Announce the incident to site CSIRTs (4 h)
- Perform appropriate forensics and take necessary corrective actions
  - Identify and kill suspicious process(es) ... but aim at preserving info
  - Suspend the relevant accounts
  - Check the VO has been contacted (if the credentials have been abused)
  - Check the CA has been contacted (if the credentials are compromised)
- Send additional reports if needed, and final report (30d)
  - Templates are available
- Restore service and re-activate suspended account(s)
- [https://edms.cern.ch/file/867454/2/EGEE\\_Incident\\_Response\\_Procedure.pdf](https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf)
- <http://cern.ch/osct/incident-reporting.html>

# Information Needed

- Essential to identify the source, to prevent re-occurrence
- Usually involves
  - Logging information (IP addresses, timestamps, identities) from services
- Sites are expected to provide the following information
  - Host(s) affected (compromised hosts, hosts running suspicious code)
  - Host(s) used as a local entry point to the site (ex: UI or WMS IP address)
  - Remote IP address(es) of the attacker
  - Evidence of the compromise (suspicious files or log entry)
  - What was lost, details of the attack (compromised credentials/hosts)
  - If available and relevant, the list of other sites possibly affected
  - If available and relevant, possible vulnerabilities exploited by the attacker
  - The actions taken to resolve the incident

# Real Life Example

- Dec 4
  - OSCT receives a report about an incident at a Swiss site
- Dec 5
  - Incident confirmed, alert sent to EGEE site security contacts
  - Ssh logs show connections from Germany, Netherland, Poland
- Dec 6-10
  - Rootkit found on the „first“ host
  - Received information from sites involved
- .....
- Jan 21
  - An update from a Netherland site confirming root compromise; traces found from Sep.
  - An updated list of suspicious IP address produced

# Lessons Learnt

- Collaboration essential to stop spreading incident
- Non-Grid CSIRTs should be involved
  - Including their communication channels and relationships
- Different CSIRTs can deliver different information
  - Netflow from NREN
  - Local arrangements from site
  - .....

# Transition to EGI

- NGIs and NGI CSIRTs being established
- Different skills/manpower for operational security
- Procedures and best practices available
  - But must be turned into life!
  - A lot of (NGI) „CSIRTs“ to emerge
- Close collaboration with NREN CSIRTs highly welcome

# Grid & NREN CSIRTs

- Incidents don't respect grid boundaries
- Coordination is time and resource consuming – effort can be shared

