

EGI – Round table discussion

Romain Wartel

EGEE08 Conference, Istanbul, 24th September 2008

- **Current OSCT model is working very well**
- **Do not expect any dramatic change**
- **UKI ROC will maintain the same level of commitment to OSCT**
- **UKI ROC might also have a ROC level security team**
- **Current UK NGS will likely be NGI in the model of EGI;**
- **Not clear the relationship between NGS and GridPP in NGI**

- Very similar to the situation in EGEE-III:
 - Central coordination (EGI.org)
 - NGI security contact supplied by gNOC (ROC equivalent in EGI)
 - Formalized information channels between security officers of participating organisations inside the NGI and the NGI security contact
 - Continuing use of JSPG documents

- Main difference would be to have a dedicated person for the NGI security contact

- Question:
 - What will happen to MWSG and GSVG/RAT?

- **OSCT must exist but focused on**
 - Policies
 - Coordination
 - Training
 - Trusting structures
- **EGI should push NGI to use the security infrastructure already in place, i.e. NREN CERTs**
- **Involving them into GRID environment**

- Security operations will fall mainly under the responsibility of each region without, with its own NGI-CERT group for:
 - Support for incident response
 - Monitoring, training etc.
- Nevertheless a top “EGI-CERT (OSCT)” contact point is needed:
 - Discussion
 - Common activities planning
 - Escalation of problems
 - Inter-regional incident response coordination (EGI-CERT)
- At NGI level:
 - Each NGI has a group (NGI-CERT) of security experts for incident response (possibly in collaboration with the “regional COD”)
 - The “regional COD” should in any case be informed about incident reports and follow up (ex. via a common EGI security dashboard in addition to the usual “csirts” and “support” channels)
- At EGI level (for incidents involving multiple NGIs), EGI-CERT group replaces OSCT-DC
 - Coordinates the incident when multiple regions are involved
 - Coordinates the incident when VOs are involved
 - Keeps contacts with other grids

- **Multiple MW stacks foreseen for EGI**
 - More extensive expertise needed to get familiar with potential security weaknesses, etc.
- **Increased number of NGIs**
 - CE is composed of eight countries, some of them are expected to form independent NGI
 - ROCs may not exist in their current form
 - All NGIs security contact should have proper expertise - “certification” and periodic training necessary
- **Analogy to OSCT in terms of global incident response coordination**
 - Maintains channels to/from NGI's CSIRTs
- **Providing services to NGI/ROC that want to outsource security tasks**
 - Requires intimate knowledge of NGI
- **A 'security challenge' mechanism needed as part of training & channels establishment**
- **Basic security monitoring should be also performed at the EGI level**
- **Training/Introduction of NGI security contacts**
 - Together with TERENA's CSIRT activities?
- **Applications expected to be more active (?)**
- **Must be able to deal with security issues/incidents**
- **EGI.org/NGIs need to have proper channels to VO security contacts**
- **Security training of VO mgmt necessary - EGI.org could help**

- **Better coordination with local CSIRTs**
- **Work on raising awareness**
 - Produce documentation and guides
 - Run frequently security Service Challenges
- **Further develop current security monitoring services**
- **Moving to EGI will security coordination remain at the regional level or move to the NGI?**

- **Current OSCT model is working very well**
- **Do not expect any dramatic change**
- **UKI ROC will maintain the same level of commitment to OSCT**
- **UKI ROC might also have a ROC level security team**
- **Current UK NGS will likely be NGI in the model of EGI;**
- **Not clear the relationship between NGS and GridPP in NGI**

- **Improvements within EGEE sites are still necessary**
 - many sites have not much practical experience yet with incident response procedures
- **Collaboration between EGEE- and D-Grid in the field of security should be improved (OSCT (IR) and GSVG, JSPG)**
- **Special incident reporting channels for Grid incidents are not established in D-Grid (National German Grid Initiative) yet. Discussion to put in place such channels or to use the 'normal' DFN-CERT-service should be resumed.**
- **Now with GOC-DB and roles of security officers for regions and sites a good status is achieved within EGEE. This could be used as a model for NGI's**

- **Devolution of tasks to NGIs as foreseen in EGI supports the already existing OSCT structure**
 - **i.e. light central coordination, security tasks shifted to NGIs**
- **Given the variety of national legislations involved dealing with IT-privacy/security a more centralized Security Infrastructure will be very difficult to put in place**
- **It might be useful to offer support for security training**
 - **installation/configuration/usage of the various security monitoring tools available**
- **Moving closer and closer to the existing NREN CERTS, so that in the future grid security becomes part of 'regular' CSIRT**

- **EGI should gradually adopt best practices from EGEE, particularly from OSCT – no need to break existing things: assimilate them.**
- **Collaboration between current Grid-wide and local security groups should be improved.**
- **Discussion channels between local CERT teams and Grid-wide security entities should be improved – both**
- **The number of sites in each ROC (will be called NGI?) will grow and many small sites can emerge – most of them will need security training and best practices guidance → EGI (or NGIs) will need to support this activity.**
- **All members of all security-related activities should start to discuss the new roadmap “just now” – perhaps some working group or mailing list will be useful.**

- **Need to keep a structured team**
- **Also need to scale up with the number of NGIs**
- **If possible, several activities distributed in the NGIs (SSC software, etc.)**
- **Needs to be merge with NREN CERTs as much as possible**
- **Needs to scale-up our incident response operations (including peer grids)**

Discussion