PRACE security incident handling

Jules Wolfrat, SURFsara, The Netherlands

EGI-EUDAT-PRACE security workshop, Linkoping, Sweden, 9 October 2013

CAPACITIES

e-infrastructure

PRACE Security Forum

Coordinates security activities

1. Defines Policies and Procedures - to build “A trust model that allows smooth interoperation of the distributed PRACE services”;

2. Risk reviews - to define and maintain “An agreed list of software and protocols that are considered robust and secure enough to implement the minimal security requirements”;

3. Operational security

Operational Security – PRACE CSIRT

- All sites must be represented in the CSIRT
- Site CSIRT information maintained on the wiki (names, phone numbers, e-mail addresses, incident information)
- Site with information about an incident (or thinks something is wrong) is responsible to take action, e.g. the organization of a video/phone conference
- Site must inform other partners if they think that incident may have impact on the infrastructure. How do they decide? Should there be a core team of persons that can be consulted? E.g. 2-5 experienced security officers of partners, so no false alarms and wrong information given. Partners also may be reluctant to contact the whole list

Operational Security – PRACE CSIRT (2)

- Actions and results of actions are discussed, however no rules defined about response times etc.
- The EGI rules are adopted for the distribution of security related information (Amber, White, etc.).
- Also subscribers from EGI CSIRT on our internal list (Leif, Romain).
- No external abuse list yet.

Operational Security

- High level of trust between sites that they behave well, e.g. patch policy, firewall set-up, local CSIRT, etc.
- Requirements must be better documented with increasing number of sites
- Implementation of audits?
- Security Challenges?

Collaboration

- Share information about policies and Procedures – SCI activity
- Risk reviews: work together if there is common interest
- Incident handling: further develop and test procedure