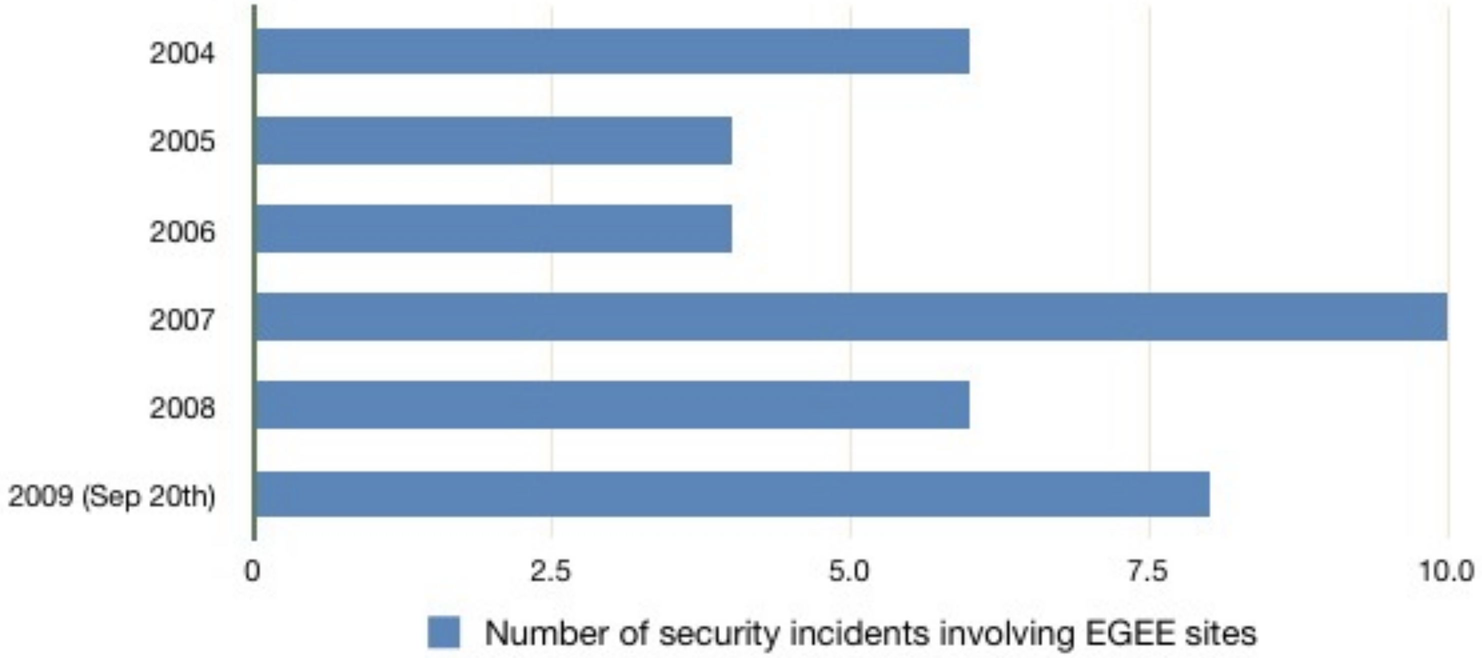
Incident response

Romain Wartel
CERN, IT Department
EGEE Operational Security Coordination Team

EGEE'09, Barcelona, Spain, 21-25 September 2009

OSCT - incident response

- **EGEE statistics on security incidents**



- **Common attack:**
  - Stolen SSH account(s), or Web application (known) vulnerability
  - Escalate as root (CVE-2009-2692, CVE-2009-2698, etc.)
  - Deploy rootkit or further malware
- **Several incidents avoidable if sites were up-to-date with security patches**

OSCT - incident response

- **Updated incident response procedure**
  - Redesigned to include feedback and metrics from SSC
  - Specific details and contact points added
    - User suspension (exposed, compromised certificate)
    - Contact with the VOs, CAs and external organisations added
    - What information is expected from the sites
    - Where to find the information usually needed
    - Unique incident identifier usage
  - Templates for initial reporting and final report
  - Coordination process within the OSCT described

https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf

http://cern.ch/osct/incident-reporting.html

Incident response

- **Main issues**
  - Lack of expertise at the sites
    - *Mitigated by increased collaboration with/trust in the OSCT?*
  - Lack of understanding of the incident response procedure at the sites
    - *Mitigated by the new procedures/templates?*
  - Lack of understanding of incident implications in some ROCs/NGIs
    - *How can we improve internal communication (and/or with NRENs)?*
  - No feedback from most sites when alerts are sent
    - *Assume the best/worst? Pakiti(CVE-2009-2698) is quite worrying!*
    - *Should we have a more fine-grained structure, closer to the sites?*
  - Increasing number of cross-grid security incidents
    - *Huge information flow + complex coordination*
    - *Probably more cross-grid incidents to come - how to be more prepared? (especially as NGIs may be a bit more independent/isolated?)*
  - External collaboration is an essential aspect

OSCT - external collaboration

- Collaboration with the NRENs
  - Significant progress since last year
  - Many more contacts established between the ROCs and their NRENs
  - BoF at TERENA 09
  - Collaboration plan agreed, implementation in progress
  - As far as we can go, the rest is in the hands of each ROC/NREN
- Collaboration with peer grids
  - Creation of GRID-SEC
    - "A coordinated response to cross-grid security incidents"
    - http://cern.ch/grid-sec/
  - Framework to share incident-related information
  - Rather extensive coverage of the academic community
  - Already been handling 2 cross-grid security incidents
    - Incidents affecting sites belonging to different grids