Bezpečnostní politiky

Politiky EGEE, LCG

- JSPG
  - snaha o obecné dokumenty
- Grid Security Policy, User Registration and VO Management, Site Registration Procedure, **Agreement on Incident Response**, Grid Acceptable Use Policy, Audit Requirements, Approval of Certificate Authorities, Guide to Application, Middleware and Network Security, VO Security Policy, Grid Site Operations Policy, VO Operations Policy, Grid Service Operations Policy, Accounting and Monitoring Data Policy

EGEE procedures

- LCG/EGEE Incident Handling and Response
  - https://edms.cern.ch/file/428035/
  - Incident response procedures (guide)
- Incident Response Handbook
  - quick start guide
- Computer security incident response team coordination
  - EGEE Deliverable MSA1.4

Incident Response Scenarios

- Několik scénářů
  - The NREN reports suspicious mailing activity from the site's CE
  - A user claims his certificate has been used without his knowledge, according to accounting information
- hrubý postup řešení, nedokončeno

Best practice for Grid admins

- Grid security
  - Grid Certificates private keys
  - Containing user jobs on batch systems
- Systems monitoring
  - Central syslog server
  - Available free space
  - World-writable files or directories
  - System metrics, performance
  - System patching status
- Systems housekeeping
  - Blocking batch jobs from creating ssh back doors
  - Configuring a system-level firewall
  - Using SSH keys (not passwords)
  - Disabling root login with password
  - Applying security patches
  - Performing system backups
  - Disabling and uninstalling unneeded services

Best practice

- Systems testing
  - Backups
  - Network services
  - Remote vulnerabilities (scanning - nessus)
- Policies and documentation
  - Follow the incident response policies
  - Business continuity plan
  - System documentation
- Intrusion Detection Systems
  - Host-level IDS
  - Rootkit checkers
  - Network-level IDS
  - Centralised IDS

CESNET CSIRT

- disaster & recovery