Planning for emergencies

Grid security, just another case for emergency preparation?

Pål S. Anderssen
CERN - IT

Motivation

- The LHC Computing Grid (LCG) will be an important element for the processing of the data from the detectors of the LHC accelerator
- The agreement between the collaborating institutes and CERN are laid down in a Memorandum of Understanding (MoU)
- During LHC data taking, the MoU requires 99% uptime for the links which connect CERN to 12 Grid sites
- Security is perceived as one significant risk factor
- Provoked a discussion in the Joint Security Policy Group (JSPG)

The layman's availability sheet

Availability is a component of the service level agreement

yearly availability		up-time	down-time	down-time	down-time
lingo	[%]	[hour]	[hour]	[min]	[day]
	100	8760	-	-	-
5 x 9	99.999	8759.9	-	5	-
4 x 9	99.99	8759.1	1	52	-
3 x 9	99.9	8751.2	8.76	525	0.4
2 x 9	99	8672.4	87.6	5256	3.7
1 x 9	90	7884	876	52560	36.5

LHC T1

Redundant self–healing infrastructure

Reliance on human intervention possible

Do we have the means to match the requirements with our service model in case of possible types of incidents?

Grid information assets are at risk

Overview of possible types incidents:

- Outages of supporting services
  - Supply of electricity
  - Environmental control
- Destruction
  - Physical force
  - Heat, fire
  - Chemicals
  - Water
- Abuse
  - Broken confidentiality
  - Compromised integrity
  - Denial of access
  - Unauthorized use of resources

Outages of supporting services

- Many sites have been hit
- Can be caused by off-site events
- Can be mitigated by redundant supply lines and redundant on-site installations
- Impact on reputation and budget -
  - Downtime
  - Call for contingency services
  - Extra cost for restoration of service
  - Extra cost for transition back to normal service

Destruction

- Rare, mostly unpredictable
- Catches the operation utterly unprepared
- Effects can be disastrous when several factors are combined
- Injury to people
- Permanent damage to infrastructure
- Access to premises may be restricted

Abuse

- Management controls include safeguards and countermeasures to protect –
  - Integrity
  - Confidentiality
  - Availability

  - of the information assets
- Are the controls effective on the Grid today?
- Breaches of security may go un-noticed
- Confusing motivation of intruding party –
  - Hamper operation, denial of service
  - Enrichment, theft of information
  - Unauthorized use of infrastructure
- Can controls be automated in order to enhance availability?
- Perhaps security vulnerabilities are of a different, more complex nature
- Severe security breaches reinforce the call for an emergency strategy to be prepared in advance

Impact of disasters

Scale of impact from incidents in a publicly funded research establishment

LCG/EGEE Planning for emergency

Brief from the September 2005 meeting of the Joint Security Policy Group (JSPG)

When are emergency procedures required?

- Emergency procedures are required to cover the following cases:
  - Incident response plans cannot be followed: critical parts of the infrastructure are unavailable (e.g. mailing lists)
  - Incident response plans are inappropriate: E.g. need to rapidly inform large parts of the community, beyond the security contacts, and incident communication channels are compromised

- Examples
  - Major power cut at Site A lasted several days
  - Cable cut network access to Site B
  - Major worm disrupted network access at Site C
  - Security incident blocks user access to accounts at Site D
  - Wide area exploit of the (homogeneous) security fabric

What is needed in an emergency?

- *Out-of-band* communication channels
  - Alternative service providers (Internet, telephony)
  - Alternative contact details (e-mail, chat, …)
  - Alternative technology
- Clear decision-making roles
  - There is no time for consensus during a crisis
  - Usual decision making process needs to be bypassed
- Clear information flow and roles
  - For at least management, users, the press
  - Reduce the risk of mis-communication
- Disaster Recovery Plan
  - Definition of critical infrastructure to be kept running or repaired quickly
  - Dependencies and sequence must be clear for restoring services
  - Mailing lists (at CERN) are key to restoring communication

Some ideas to stimulate discussion

- Define an emergency advisory committee?
  - Members, mandate
  - Goal is to ensure rapid and appropriate decisions
- Assure information flow
  - E.g. update DNS servers to point to temporary (web) servers
  - Pre-record messages on telephone help services
- Prepare alternative communication channels
  - E.g. commercial conference call facilities
  - Alternative Internet providers (e-mail addresses, chat, phone,…)
- When/do we return to normal Incident Response?

Incidents will occur

- Over time, responses to re-occurring incidents find their way into operational procedures
- This is also the case for **security breaches**
  - Sites have in place procedures to handle minor, local cases of abuse
- LCG/EGEE Grid security problems, above a certain level of severity, call for the formal **Incident Response Handling** (IRH)
  - The incident may have impact beyond the local site
  - Reporting channels are prepared in advance
  - The IRH relies on a minimum of the infrastructure being operational
- In the event of a disaster, the operational procedures and the predefined response handling may not work
- In extreme cases they may even be counterproductive

Some specific suggestions

- Prepare for disaster recovery
  - Assemble a knowledge team
  - Look for common elements of disasters
  - Identify services and their criticality
  - Review impact of service disruptions
  - Analyze vulnerabilities
  - Analyze dependencies of services
  - Review contingency options
- Develop a plan
  - Analyze requirements for an alternate service location
  - Identify resources required for service restoration
  - Identify people who are likely to contribute to the restoration
  - Identify people/functions/roles that will constitute the emergency management team
  - Define the extent of authority of the management team

I thank you for the attention…