Course: clusters, Grids, Clouds

Lecture 7: Cluster & Cloud security

- Information threats
- Some methods to neutralize the threats

Shevel.Andrey@gmail.com

Information Security Threats

- **Illegal access to the data in computing system.**
- **Unplanned change the data**
  - Data changing
  - Data loss
- **Illegal use of computing resources**
- **Viruses**
- **Botnets**
- **Deny Of Service**

Illegal access to the data

- **Outside attempts to access to the cluster**
  - Separate persons (hacker)
  - Group of persons (network hackers)
  - Large laboratory (large group of network experts)
- **Inside attempts to access to the cluster**
- **Counter actions must be adequate the threads and potential loss**

Data loss

- **Possible causes for data loss:**
  - Illegal access to the data;
  - Human errors;
  - Malfunctions.
- **Counter actions:**
  - Passwords, two factor authentication, etc.
  - Education/Training
  - Backup copy.

Technology problems

- **Part of equipment is out of order due to:**
  - Electricity problems;
  - overheating;
  - Bugs in software.
- **Counter actions:**
  - Make stable elecricity;
  - Make cooling system and keep the temperature in recommended limits;
  - Update software requlary.

Standarts/Recomentations

- International standard ISO 27002
  - http://en.wikipedia.org/wiki/ISO/IEC_27002
- The ITIL (Information Technology Infrastructure Library) framework is designed to standardize the selection, planning, delivery and support of IT services to a business. The goal is to improve efficiency and achieve predictable service levels. The ITIL framework enables IT to be a business service partner, rather than just back-end support. ITIL guidelines and best practices align IT actions and expenses to business needs and change them as the business grows or shifts direction. - http://searchdatacenter.techtarget.com/definition/ITIL

Standard ISO 27002

- Risk assessment
- Security policy
- Management of information security
- Inventory and estimation of information sources;
- Management of employee
- Physical security
- Network security
- Access control

Standard ISO 27002 - 2

- Communications and operations management – management of technical security controls in systems and networks
- Information security incident management – anticipating and responding appropriately to information security breaches
- Business continuity management – protecting, maintaining and recovering business-critical processes and systems
- Compliance – ensuring conformance with information security policies, standards, laws and regulations

Basic recommendations on the security

- Hardware and software **have to be up to date**.
- Passwords (must be complicated) never possible to inform about password from one person to another one (even collegues).
- Cluster room has to be guaranteed from any entering by any creatures (including people, mouses, insects, etc).
- All logs with records who and when uses the cluster must be kept long time (may be one year or more).

Basic recomendations on the security - 2

- The procedures to restore the cluster software from scratch are the MUST.
- After any accident the investigation has to be performed to avoid the same in future.

Basic administrative steps

- At least special security officer.
- Regular training for all staff.

Additional info

- http://www.nist.gov/cyberframework/ - National Institute of Standards and Technologies (NIST) – CyberSecurity Framework

End of Lecture