The Need for Common Security Services for Research Infrastructures

EGI CSIRT F2F 2013-12-02

Urpo Kaila
Head of Security
<kaila@csc.fi>

Current Operational Security Environment

- ‘Clouds’ (External systems and services which we cannot control) – as a consumer and as a producer
- Increasing international and cross organisational dependencies/operations
- Authentication through social media (beware!)
- Human data and privacy issues
- Case Snowden and ‘Cloud Politics’ (lobbying)
- Evolving new software and technologies
- Threat vectors becoming more complicated
- Increasing financial and legal risks
- Compliance requirements (see above)
- CSIRTs and CyberSec agencies sometimes having agendas of their own

Current Security Controls for RI

- ‘ Roll your own’ - now we have the SCI
- Much noise
- Unclear roles and responsibilities
- Incident details disclosed uncontrolled
- CSIRTs taking operative roles at sites, bypassing management, without responsibility
- Fuzzy cooperation between Sec teams
- Inefficiencies, confused reactions
- Lack of commitment by management, lack of authority
- Lack of control, inadequate risk management

‘Challenges’

- RI’s rivaling for financing
- Different stages of development
- Different technologies
- Different sites
- Different user communities
- Different types of Data

Common Denominators

- Similar security principles
- Similar security controls
- Similar risks
- Similar objectives
- Common financial sources
- Similar Security controls
- Same organisations
- Same people
- Similar constituents

Ideas for common solutions

- Agree on joint security operations for well defined areas where instant/fast gains can be obtained:
  - IRT
  - Vulnerability monittoring
  - Policies
  - Audits/Review
  - Training
  - Exercises?
- Use the extended RACI model!
  - Responsible; Accountable, Consulted,Informed,

Suggestions - a first tentative idea

- Common CSIRT for European RI’s
  - Well defined roles between CSIRT, RI, Sites/Communities
  - Not to be dominated by a single RI – but expanded EGI CSIRT?
  - CSIRT must serve the RI, Sites/Communities!
  - Well defined services
    - Vulnerability monitoring/alerting
    - Incident coordination
    - Technical security assessments
    - Development of security policies and guidelines
    - Training, Certifications
    - Site Reviews
    - CSIRT Community Liaison
- Shared board and shared Officers in Duty?