# Handling security incidents in e-infrastructures: Balancing prevention and response

Daniel Kouril

WISE, 27.9.2016

# EGI CSIRT

- EGI is federated environment
  - Infrastructure (EGI)
  - NGI
  - Site (resource provider)
- (Site responsibilities affected by clouds)
- Mission of EGI CSIRT - maintain secure EGI
  - Incident handling
  - Prevention

# Dealing with incidents

- Focusing on response
  - So far mainly coordination and “consultations” - not always sufficient/efficient
  - Possibility to take action at sites (by policies)?
  - A big dedicated incident response team needed
- Focusing on prevention
  - Involvement of sites necessary
  - Transfer responsibilities to take actions
    - Communications needed from CSIRT ( vulnerability assessment, threats, monitoring definitions, trainings)
  - Implemented centrally – site autonomy affected

# Discussion

- What is the right balance between prevention and response?
  - Just follow patterns of commercial providers?
- How can we rely on (EGI) federation?
  - What is realistic?
  - How sites could/should be involved (in prevention)?
  - Inter-federations
- (What is actually changed by clouds?)