EGI CSIRT, keeping the infrastructure secure

Sven Gabriel sveng@nikhef.nl, **Nikhef, EGI-CSIRT**

The evolution of Security for distributed e-Infrastructures and Research Infrastructures

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

Introduction

Introduction

How to keep a reasonably secured infrastructure a safe place for our users?

- What is a reasonably secured infrastructure?
- What EGI CSIRT does to keep it a safe place.
- Is this complete?
- How to address the challenge of security in evolving Infras

What is a reasonably secured infrastructure?

Secured Infrastructure?

- **Reasonably** secured.
  - different requirements on security (for example: .mil, .gov, .com, .edu)
  - different requirements on user experience
- Example for .edu: Grid Infrastructure
  - 'Grid started as a 'new technology", security matured/improved over the years.
  - Cloud: AWS, Azure, . . . FedCloud

Reasonably Secured Infrastructure, Grid

- Start from a well described Usage model ✓
- Develop a Policy Framework a CSIRT can operate in ✓
- Typical components: Access Control to the infra ✓
- Traceability of user activities. ✓
- Require Incident Response Capabilities on all levels (Project, Resource Centers, VOs)✓
- Communication channels to the major players in security ✓
- Does such an secure grid security exist? Well, we are reasonably close

Keep the Grid a secure place

- Incident Prevention, for example
  - Address challenges of a evolving Infrastructure (VO WMSes)
  - Software: Critical vulnerabilities found.
  - End-of-Life, no updates for Software.
- Incident Handling
  - Containment,be able to stop the incident from spreading out.
  - Resolve Incident, find and remove the vulnerability used by the attacker to gain control.
  - Cleanup the infrastructure, monitor for re-occurrences.

Cloud Security

Does the same approach work for the cloud, . . . lets see

Reasonably Secured Infrastructure, FedCloud

- Start from a well described Usage model ✗
- Develop a Policy Framework a CSIRT can operate in ✗
- Typical components: Access Control to the infra **incomplete**
- Traceability of user activities. ✗
- Require Incident Response Capabilities on all levels (Project, Resource Centers, VOs) **with every incident we learnt to know new players**
- Communication channels to the major players in security ✗

Reasonably Secured Infrastructure, FedCloud

Lets try another tack . . .

Reasonably Secured Infrastructure, FedCloud

- Incident Prevention, for example
  - Make sure all contributing RCs have a common understanding on security. (RC Certification procedure PROC09).
  - Provide the users with a secure point to start from, i.e. trustworthy VMs (VM-Endorsement policy)
  - did this help?

Reasonably Secured Infrastructure, FedCloud

- Incident Prevention, for example
  - Make sure all contributing RCs have a common understanding on security. (RC Certification procedure PROC09).
  - Provide the users with a secure point to start from, i.e. trustworthy VMs (VM-Endorsement policy)
  - did this help? **No!**
- Incident Handling
  - Traceability? Depends, problems with robot certificates.
  - Incident Response at the sites, varies a lot! From incident detection, forensics investigation, incident report to *"we have shut down the VM"*
  - same incidents happened multiple times, known problems were not addressed.

Make the Cloud an a little more secure place, Summary

- Start from usage model, based on that, have an agreed set of policies.
- Users trust EGI/INDIGO that ”their” services do not expose users to high risk environment. Clearly indicate which services are approved/certified and which not.
- Have a procedure to integrate new services/technologies, make sure security is not degraded

Make the Cloud a secure place, Todo:

Resource Centers:

- Review the RC certification procedure
- Aim at Understanding the IR Procedures, incl expected response times at RC needed
- Make sure the technical set-up, local expertise is available to do useful IR

Make the Cloud a secure place, Services

Make clear what are EGI trusted services, i.e. which have gone through a service integration/certification process: provider should have documented, demonstrated

- What is the purpose? configure a single host, or a grid infra in the cloud?
- Are end-user credentials processed? If yes, how are they protected?
- Access to the service? Access control?
- to be able to trace all user activities undeniably to a user?
- To be able to suspend access in an emergency.
- adhere to the security policies, follow IR procedure

Make the Cloud a secure place

- in short, adhere to EGI's *Service operations Security Policy*[1]

[1] https://documents.egi.eu/public/ShowDocument?docid=1475

Make the Cloud a secure place

We are not there yet …
A procedure to integrate new technologies would help a lot.

Thank you for your attention!

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142