EGI-CSIRT – Operational Security

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

Activity Update

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

EGI-CSIRT OMB 26. June 2015

Security Operations: CRITICAL CVE handling

- CVE-2014-9322/CVE-2014-6271/6277/CVE-2015-1815/CVE-2010-3081/CVE-2013-2094: 9 Sites (3 NGI-RO) / 0 site suspended
- Re-Certification: 0 Sites **in progress**.
- Re-Certification: 1 Sites **done**.
- Needs updated version of EGI-CSIRT Critical Vulnerability Operational Procedure https://documents.egi.eu/public/ShowDocument?docid=283, in preparation... still :(

EGI-CSIRT OMB 26. June 2015

Security Operations: Incidents / Alerts, Advisories 28. May 2015 – 26. June

- EGI-20150611-01 Security incident at UKI-SCOTGRID-GLASGOW
  - attack: accidentally open ElasticSearch instance
  - installed botnet malware
- Compromised EGI FedCloud virtual machine(s) at NGI CZ - CESNET-MetaCloud, ToDo: debriefing

EGI-CSIRT OMB 26. June 2015

Lisbon Conf fallout II

- Huge ToDo List, related to FedCloud security issues. Incident Response atm difficult.
- VM Endorsement as done atm useless for security.
- Enforcement of EGI-Security Policies: Incidents affecting EGI have to be reported.
- Security Policies/Procedures currently reworked to address cloud particularities. **NOTE** all currently approved policies apply for the whole infrastructure.
- SSC addressing FedCloud planned for September/October will give us more insight.