Incident Response in the EGI Federated Cloud

Boris Parák, CESNET

Preventing an Incident

- Only trusted & endorsed images
- Periodical scans of active VMs for know vulnerabilities (user agreement)
- Educate users & VM operators
- Periodic (deeper) analysis of available appliances (EGI CSIRT?)

Detecting an Incident

- Abuse report from "outside" (too late)
- Advanced network monitoring & profiling capabilities locally at sites (netflow probes? real-time network analyzers?)
- Logging all traffic crossing site boundaries, optionally even local traffic

Suspending User DN

- Argus for grid, with polling usable for cloud (scalability?)
- Acceptable polling frequency (once a day, once every hour?)
- How should this affect resources?
  - Running virtual machines (suspend?)
  - Storage blocks (nothing)
  - Network reservations/allocations (release? keep?)
- Per-user sub-proxies? How will we know "who" to ban?
- Banning a gateway (a sub-proxy issuer) must affect resources owned by its users (identified by sub-proxies)!

Disabling Vulnerable Images

- Detecting a vulnerable image (How?)
- Blocking this image in AppDB (EGI CSIRT)
- Propagation to all sites, image no longer available
- But
  - What about appliances in image lists?
  - What about VMs already running from these images?
  - How fast should this be?

Detecting Similar VMs

- What is a "similar" VM?
  - Same user?
  - Same image?
  - Same start time?
  - Same network profile?
- Notifying owners of potentially vulnerable VMs
- Should we interfere with only "potentially" vulnerable VMs?

Disabling Vulnerable VMs?

- What does "vulnerable" mean? How sure are we?
- User notification might be better than outright suspension (user-oriented responsibility model)
- VM launched from a vulnerable image != Vulnerable VM

Network Traceability

- Complex issue tied to site-specific hardware, software & configuration
- Logging
  - Ownership of public IP addresses (CMF)
  - Ownership of private IP addresses (CMF)
  - In NAT'd environments (port -> private IP address)
  - MAC addresses for local diagnostics (L2 issues)
- **How to expose this information to EGI CSIRT?**

– Discussion –

Final Slide

– That's All Folks! –