ISGC 2017 Security Workshop

Sven Gabriel

Security Incident handling in Federated Clouds

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

Introduction

EGI-ENGAGE

Introduction

Security in Distributed Infrastructures

- Incident Prevention
- Incident/Intrusion Detection

Incident Response (IR)

- IR Communications
- Containment
- Forensics

Security in Distributed Infrastructures

Security and Business Models

Why bother about Security, another business model
Cyberbunker: *Mind Your Own Business policy*

Security in Distributed Infrastructures

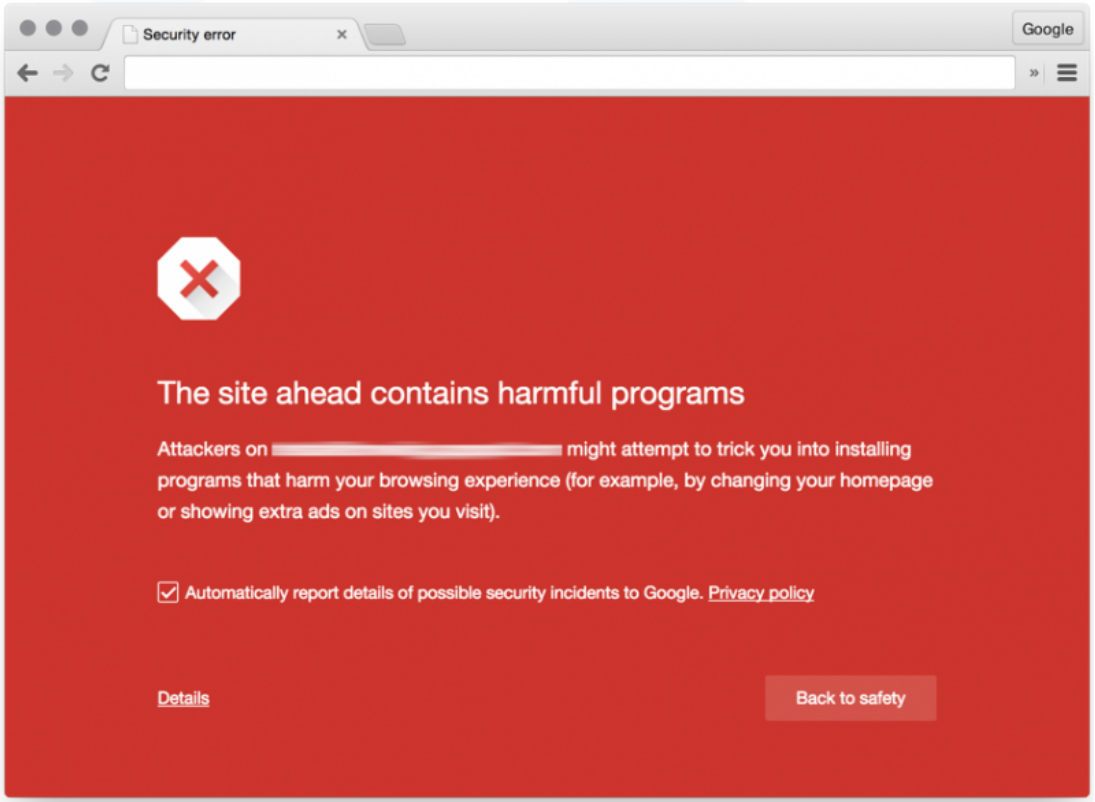
Why bother about Security
Security always has in impact how users experience services. How much you want to care about security is dependent on your business model. This has a serious impact and is a management decision, see for example:

http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html?_r=1

Security and Users/Customers

How to sell security to the users/customers

Some sociology:



https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43265.pdf

http://www.nature.com/news/how-to-hack-the-hackers-the-human-side-of-cybercrime-1.19872

Security and Users/Customers

Examples from our Infra

- Request to patch, . . .
- You use our service from an unknown location, . . .
- no, we can't give you root on the compute cluster
- no, we will not install your preferred editor on our supercomputer

Goal: keep Users/Customers happy

Ingredients

- Have a clear set of agreed policies (ex. AUP)
- Be transparent on why certain actions are requested (Advisories)
- Use the proper ’language’ for the intended recipient (Admin/User)
- Be prepared to deal with frustrated / swamped users.

Security Incidents

Incidents, finally . . .

Security Incidents in Distributed Infrastructures

Definition[1]: A security incident is the act of violating an explicit or implied security policy (ex: local security policy, EGI Acceptable Use Policy) (https://documents.egi.eu/public/ShowDocument?docid=47)

- Who violates policies?
- Criminals: Automated Attacks, compromised systems rented out for illegal activities (Botnet, used for ddos, spam, distribute malware etc).
- Hacktivism, Creative young people
- Insiders, Users

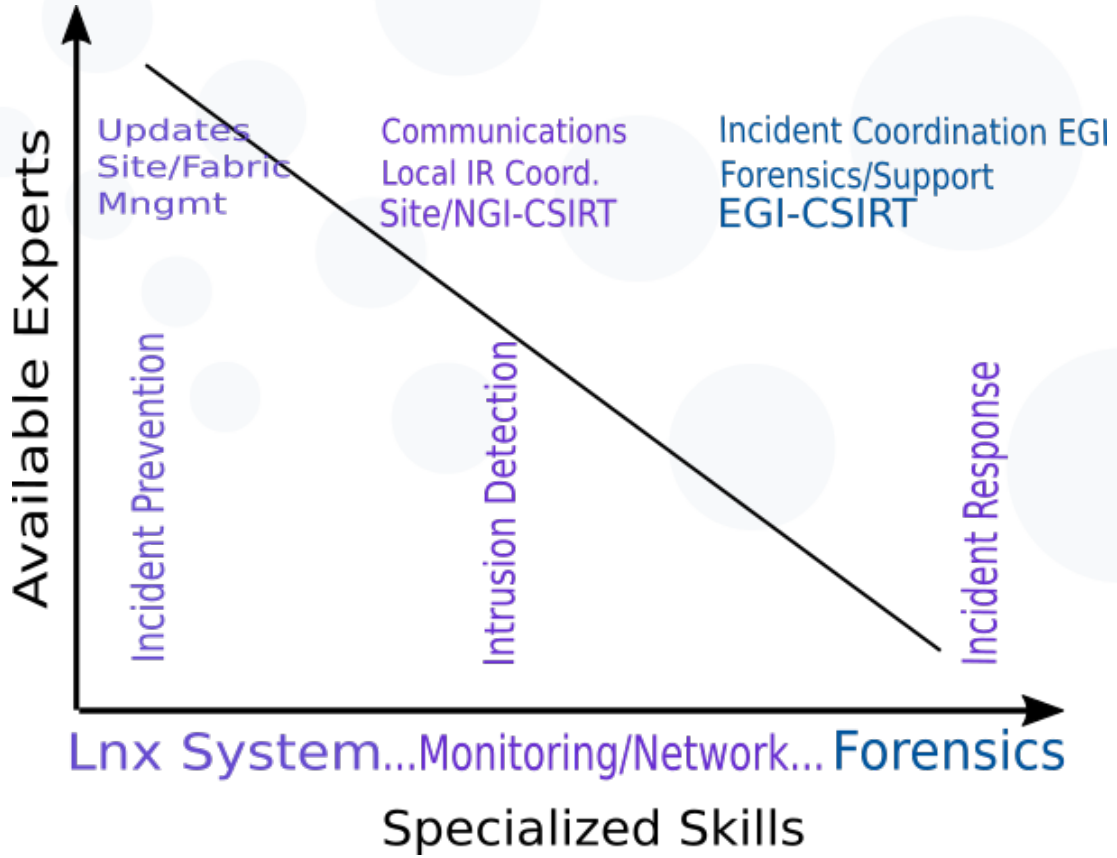
How attackers access the infra

- **External, unauthenticated** Most serious, needs to be prevented
- **External, authenticated** Ex: stolen Credentials
- **Local, authenticated** Also: Impersonation Vulnerabilities

Security in Distributed Infrastructures

- Incident Prevention
- Incident/Intrusion Detection (also Tue. 16:00, Fyodor, Watz)
- Incident Response (Vincent)

Who can Work on Security ...



Incident Prevention

Infrastructure Housekeeping

Vulnerability Handling Process:

- Vulnerability Detection (often external sources)
- Assessment (SVG/RAT) $\rightarrow$ Criticality
- If Critical, develop: HeadsUp/Advisory, Security Monitoring
- All Sites need to take action (patch/mitigate)
- Follow up (Ticketing)
- Monitor the Infrastructure

Infrastructure Housekeeping

Why:

- Prevent being victim of standard attacks (check your logs, a lot background noise)
- Clean-Up of an incident is expensive!
- Provide an environment where users are ”protected” from each other.
- If the infra is not usable/working (for whatever reason) will result in funding issues.

Goal: Reducing Security Incidents

Number of incidents using grid technology

Goal: Reducing Security Incidents

Number of incidents using grid technology 1

Grid/Cloud differences

- Admin / User role separated in Grid
- Grid Admins are Linux Systems experts
- Grid Software is verified against EGI's current Quality Criteria (UMD)
- FedCloud RCs (up to Hypervisor, Network) are managed by Admins
- VMs are managed by the Users

Some Cloud Security

Non System Experts (Users) are admins of their Infrastructure they deploy in the cloud.

- To mitigate this risk VM Endorsement Policy was developed.
- Distinguish between VM Operators/Users
- Provide the users with endorsed secure VMs

Incident/Intrusion Detection

Incident/Intrusion Detection

Tue 16:00 Identifying Suspicious Network Activities in Grid Netw

Tue 16:30 Modern Monitoring Systems (Watz)

Incident Response (IR)

IR Requirements

- Know your perimeter: Security Policies
  https://wiki.egi.eu/wiki/Security_Policy_Group
- Know your Infrastructure, who has which role, what are the communication endpoints.
- Have an Incident Response Procedure
  (https://wiki.egi.eu/wiki/SEC01)

Actors and Roles

- Site Security Contact
- EGI-CSIRT Security Officer on Duty
- User
- VO-Security Contact
- External party

IR Communications

IR Communications

Questions:

- You know now the actors, where do you get the contacts?

IR Communications

Questions:

- You know now the actors, where do you get the contacts?
- You know that the contacts are in http://goc.egi.eu/ and https://operations-portal.egi.eu/vo/security

IR Communications

Questions:

- You know now the actors, where do you get the contacts?
- You know that the contacts are in `http://goc.egi.eu/` and `https://operations-portal.egi.eu/vo/security`
- So, . . . what will you ask? . . . report?

IR Communications

Questions:

- You know now the actors, where do you get the contacts?
- You know that the contacts are in http://goc.egi.eu/ and https://operations-portal.egi.eu/vo/security
- So, . . . what will you ask? . . . report?
- , see https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
- Or

IR Communications

Questions:

- You know now the actors, where do you get the contacts?
- You know that the contacts are in http://goc.egi.eu/ and https://operations-portal.egi.eu/vo/security
- So, . . . what will you ask? . . . report?
- , see https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
- Or just contact abuse .at. egi.eu

Containment

Containment

- Stop the incident! How?

Containment

- Stop the incident! How?
- Stop a DN submitting new jobs/starting VMs

Containment

- Stop the incident! How?
- Stop a DN submitting new jobs/starting VMs
- Central Argus system

Containment

- Stop the incident! How?
- Stop a DN submitting new jobs/starting VMs
- Central Argus system
- For the forensics see Vincents talk

Forensics

Forensics

Talk: Computer Forensics Analysis (FyodorVincent)

- What went wrong
- How to detect it
- How to react to it . . .