IGI CSIRT

R. Brunetti
INFN - Torino

Contenuti

- Cosa e' uno CSIRT
- Gestione della sicurezza in EGI/IGI e IGI-CSIRT
- Servizi ed attivita' previste
- Collaborazione con il GARR-CERT
- Conclusioni

Definizione di CSIRT

- CSIRT (Computer Security Incident Response Team) e' sinonimo di CERT (termine coniato e registrato negli USA)

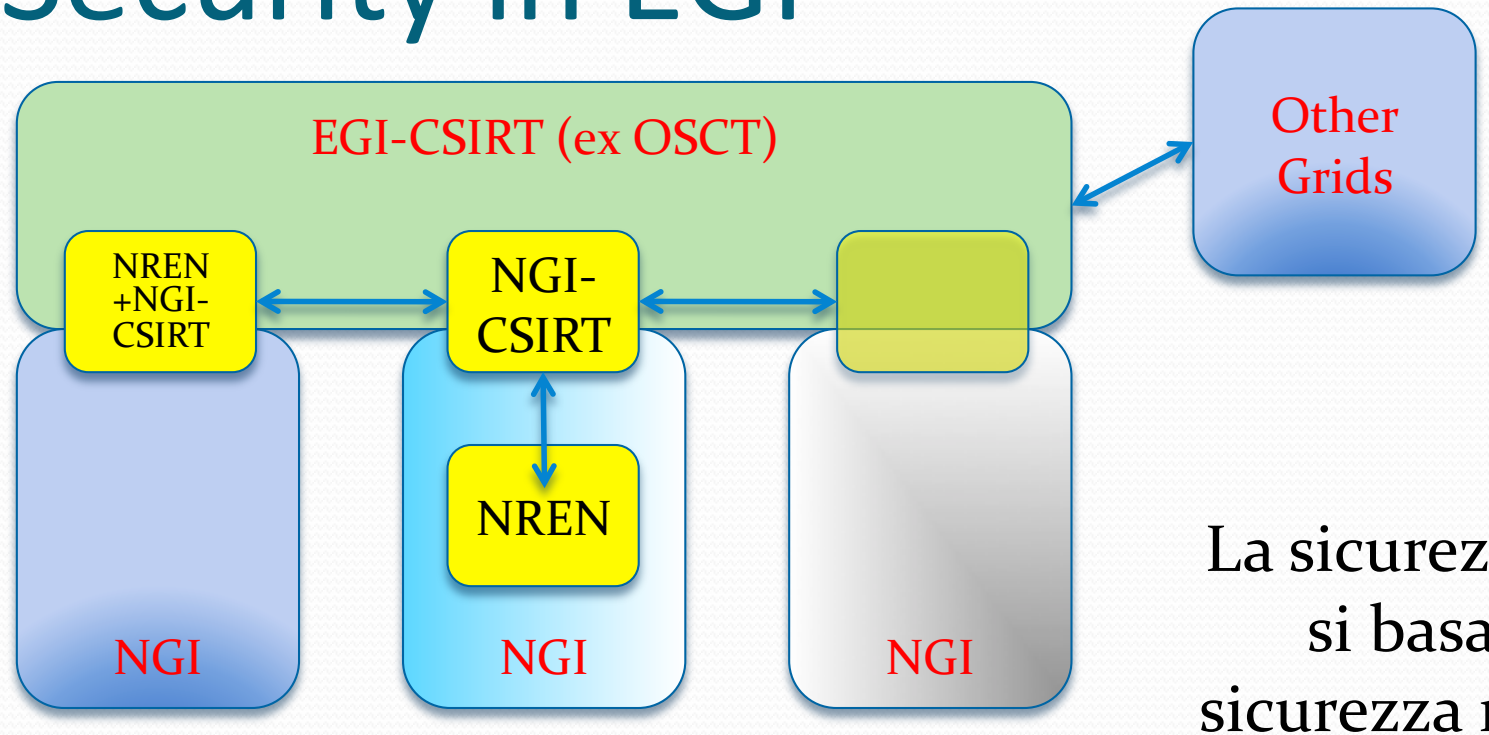
Gruppo di esperti di sicurezza IT che ha come compito quello di reagire in caso di incidente di sicurezza, al fine di limitarne le conseguenze e assistere gli utenti nel recupero delle funzionalita' e gli amministratori nel ripristino dei sistemi

Non solo Emergenze….

- Col tempo, gli CSIRT hanno progressivamente assunto connotati di *Security Service Providers*, includendo attivita' come:
  - Security Advisory
  - Sviluppo/divulgazione di tools di sicurezza
  - Training
  - Monitoring/Auditing
  - Analisi del rischio
  - …..

Sicurezza in EGI/IGI

Security in EGI



La sicurezza di EGI si basa sulla sicurezza nelle NGI

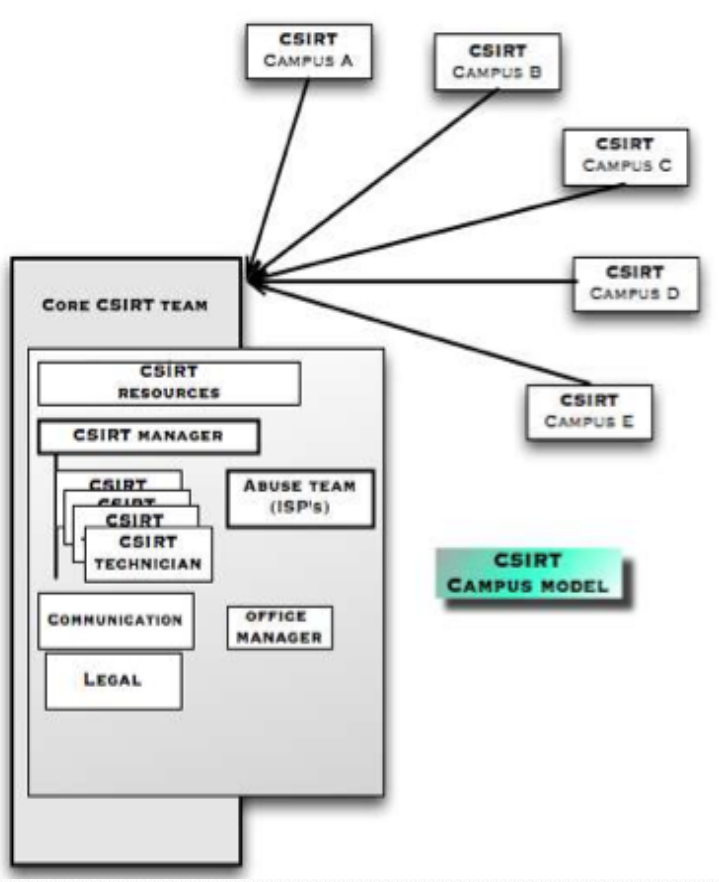
- Coordina le attivita' sulla sicurezza in EGI
- Gestisce le procedure in uso e mantiene i contatti con gli CSIRT
- Fornisce il framework generale per la collaborazione tra gli CSIRT

Esigenze di IGI

- Sulla base dell'esperienza maturata in EGEE:
  - Le problematiche di sicurezza sono (o possono rapidamente diventare) GLOBALI
  - Molti siti di dimensione piccola/medio piccola → gestione piu' onerosa
  - Esperienza, effort e sensibilita' alle questioni di sicurezza molto variabile tra i siti
  - Molto utile (necessaria) un'attivita' di monitoring
  - Molto utile (necessaria) un'attivita' di auditing (challenges)
  - Cruciale la comunicazione, la divulgazione delle procedure di IR e l'interazione con il GARR-CERT

Modello di IGI-CSIRT

- I siti hanno gia' (o dovrebbero avere gia') uno CSIRT ed un responsabile della sicurezza.
- IGI-CSIRT deve:
  - Coordinare le attivita' di IR e fornire supporto ai siti
  - Gestire eventuali strumenti centralizzati
  - Interagire con l'operation management di IGI
  - Interagire con EGI-CSIRT e contribuire alle sue attivita'



Attivita'

Security Advisory

- Segnalare le vulnerabilita' a livello di
  - Sistema operativo
  - Middleware
  - Applicativi
- Fonti:
  - Vendors
  - GSVG
  - EGI-CSIRT
  - Siti
- Sottile distinzione tra vulnerabilita' locali e remote.
- Atteggiamento attivo: non solo segnalazioni
  - Follow up sui siti nei casi piu' importanti

... Senza esagerazioni ed inutili allarmismi

Incident Response

- Coordinamento delle azioni e verifica che le procedure di IR vengano seguite
- Punto di contatto con EGI-CSIRT, con le altre NGI, con le VO e con il GARR
- Supporto per:
  - Contenere i problemi
  - Analizzare gli incidenti
  - Ripristinare i servizi

Monitoring/Auditing

- L'esperienza ha mostrato che e' fondamentale avere uno strumento che:
  - Informi sullo stato di aggiornamento dei sistemi (Pakiti)
  - Permetta di realizzare un monitoraggio centrale dei siti (Nagios)
- Il tipo e livello di monitoraggio sara' concordato con i siti (salvi i requirements di EGI)
- SSC (Security Service Challenges) e campagne di auditing per verificare le procedure, i canali di comunicazione e la prontezza di risposta dei siti
  - Modi, tempi e finalita' dei challenges saranno definiti ufficialmente.

Training

- Mantenimento di pagine web sul portale IGI
- Prevediamo di organizzare almeno un training/tutorial all'anno
  - Best practices
  - Tools utili
  - Forensic
  - Middleware security
  - Cosa fare per aumentare la sicurezza e….

… cosa NON fare per preservarla

Collaborazione con GARR-CERT

IGI-CSIRT e GARR-CERT

Gli obiettivi di IGI-CSIRT e GARR-CERT sono leggermente diversi e complementari.
I due gruppi potranno essere autonomi, ma collaborare strettamente per alcune attivita'

Obiettivo di GARR-CERT

- Mantenere l'integrita' dell'infrastruttura di rete

Obiettivo di IGI-CSIRT

- Mantenere la sicurezza dei servizi Grid, preservare gli utilizzatori (utenti e VO) e l'integrita' dei dati

Collaborazione con GARR-CERT

Security Advisory

- GARR-CERT: lo fa gia' (organizzazione, fonti ecc..)
- IGI-CSIRT: Contatti verso EGI, GSVG.

Training

- GARR-CERT: Know-how sulle "tendenze" in materia di sicurezza
- IGI-CSIRT: Approccio Grid-oriented

Incident Response

- Le rispettive procedure di IR devono "intersecarsi"
- GARR-CERT(NOC) riconosca IGI-CSIRT come "autoritativo" nel caso di problemi con attori Grid

Conclusioni

- La sicurezza e' un'attivita' necessaria in IGI e deve essere parte integrante delle operation.
- E' importante che IGI possegga un gruppo dedicato per la sicurezza con un mandato (ed un'autorita') ben preciso
- IGI-CSIRT dovrebbe essere autonomo ma puo' e deve collaborare strettamente con GARR-CERT
- IGI-CSIRT potrebbe essere un punto di aggregazione anche per le attivita' di INFN Sec.group

Obiettivo da conseguire:

Dotarci degli opportuni strumenti per mantenere la sicurezza e l'integrita' dell'infrastruttura Grid

Gruppo di lavoro

- Riccardo Brunetti (Torino)
- Giuseppe Misurelli (CNAF)

- Luciano Gaido, Tiziana Ferrari
- Roberto Cecchini