INFN CSIRT: gestione di incidenti di sicurezza in lockdown

Riccardo Veraldi

INFN

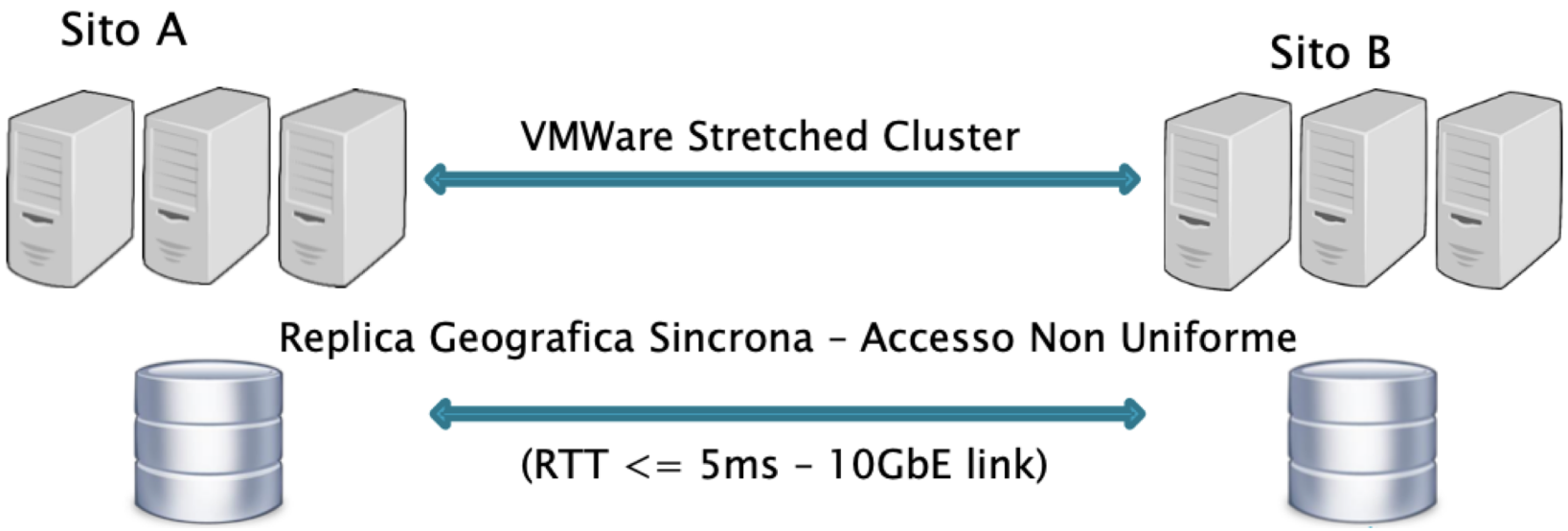
WORKSHOP GARR 2020

NET MAKERS

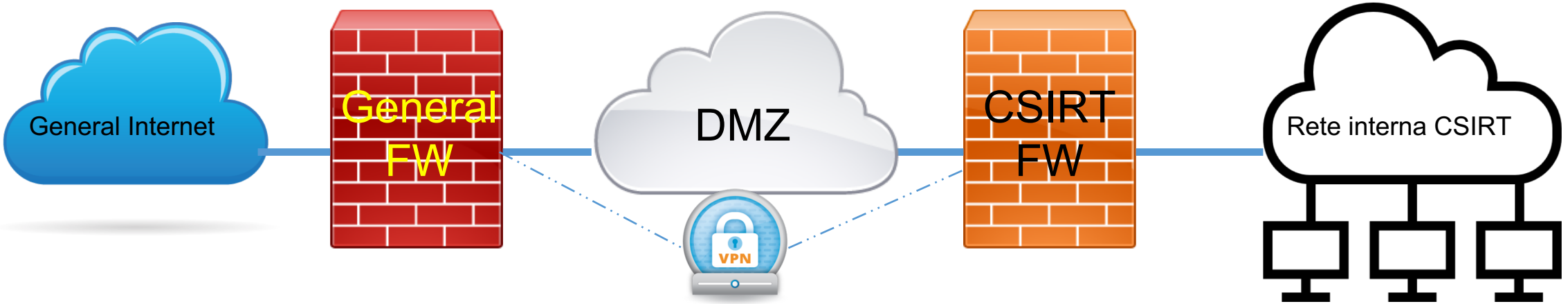
INFN CSIRT

- Gestione incidenti di cyber security INFN
- Operativo da Dicembre 2019
  - https://www.csirt.infn.it/
- Quattro membri dei quali un coordinatore:
  - Vincenzo Ciaschini
  - Stefano Dal Pra
  - Gian Piero Siroli
  - Riccardo Veraldi

INFN CSIRT: architettura BC

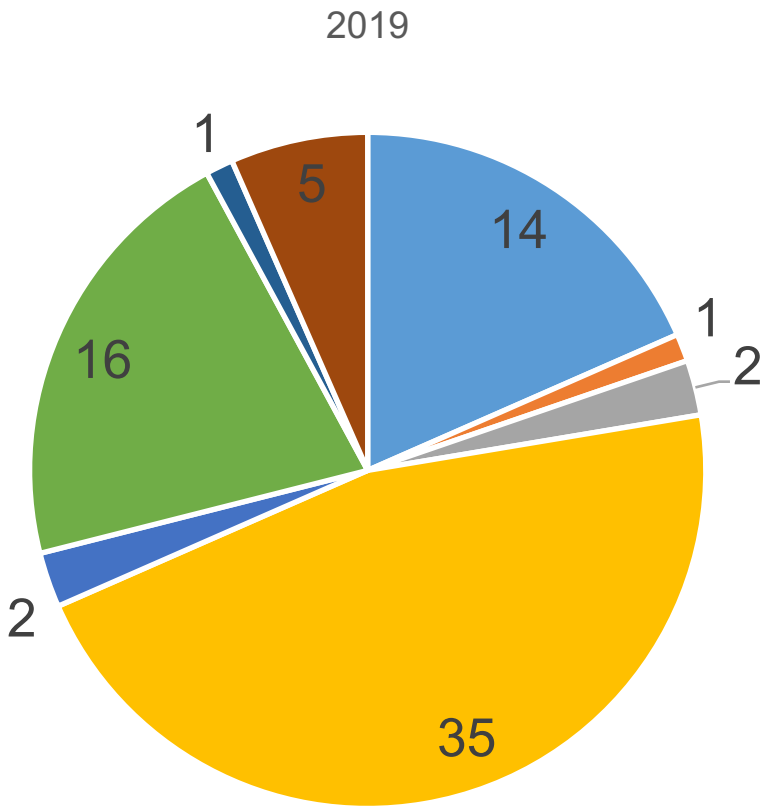


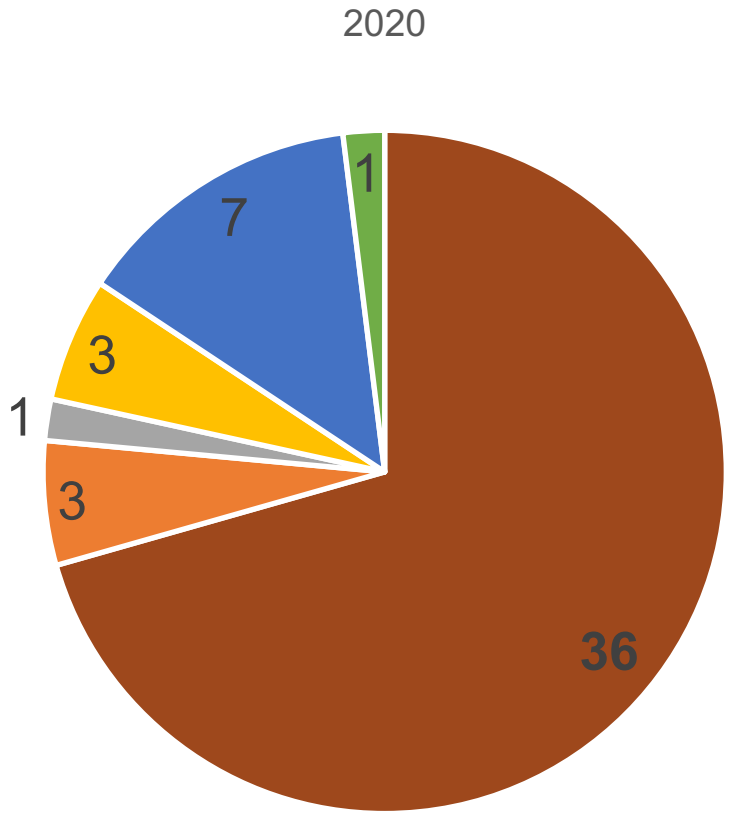
INFN CSIRT: schema di implementazione



- Servizi interni implementati su storage criptato
- Le email a INFN CSIRT vengono ulteriormente cifrate «a caldo» una seconda volta

Report 2019 (GARR CERT) vs Report 2020 (INFN CSIRT)





Azioni intraprese durante il lockdown

- Personale INFN CSIRT on duty tramite VPN dedicata
- Utenti INFN sensibilizzati tramite corso cyber security online OBBLIGATORIO
- Dipendenti INFN in lavoro da remoto (lavoro agile)
  - Laptop con AV e VPN client configurato dai serv. Calcolo
  - Si e' cercato di limitare l'utilizzo di dispositivi personali

Considerazioni

INFN CSIRT

- I dati relativi agli incidenti sono compatibili con i dati di GARR CERT e non denotano un aumento significativo del numero di incidenti totali
- Si nota un incremento degli incidenti di tipo Vulnerable Host
  - Vulnerabilita' segnalate da piattaforme OSINT
    - Vulnerabilita' legate a SSL
    - XSS
    - Altri tipi di vulnerabilita'
    - Data breach dovuti a phishing