Introduzione al Workshop sulla Sicurezza Informatica

Alessandro Brunengo

Security INFN oggi (I/III)

Gruppo Security CCR

- R&D, spesso in collaborazione col netgroup
- coordinamento attività security: scansioni, MM AGiD, policy (gestione passowrd, filtri perimetrali, ...), piattaforme per l'end point protection
- CSIRT INFN: segnalazione vulnerabilità, gestione incidenti
- task force di emergenza

Attivita' nelle strutture (servizi calcolo locali)

- configurazioni per la protezione locale (MM, GDPR, antivirus, antispam, filtri)
- gestione incidenti

Formazione

- Corsi locali e nazionali
- Costante mantenimento del livello di attenzione degli utenti (avvisi)

Security INFN oggi (II/III)

SIT INFN Cloud

- Attivita' dedicata alla INFN Cloud
- Sviluppata in modo indipendente, ma grande sovrapposizione di persone con il gruppo Security di CCR

Datacloud WP4

- Derivato dal WP4 di INFN Cloud, include alcune persone del gruppo Security CCR
- Per impostazione iniziale, e' il gruppo security della CCR (cioe' dell'INFN) che si occupa di attivita' specifiche di Datacloud

Audit

- audit interno per strutture e infrastrutture (SSNN, DSI)
- cadenza annuale
- dal 2/2/2023 sotto il coordinamento dell'RTD

Security INFN oggi (III/III)

Policy e compliance: gruppo Harmony

- gruppo che include esperti di security, DPO, legali
- disciplinare di utilizzo delle risorse informatiche
- analisi di use case specifici

GDPR: il DPO

- organismo di riferimento per l'INFN sul GDPR
- attivita' anche propositiva

Datacloud WP7: Sistemi integrati di gestione e Legal Compliance

- Data Protection, risk assessment, legal and ethical requirement, ...
- Misura della conformita', certificazioni ISO, ...

In stretta collaborazione con INFN Security e WP4
Sovrapposizione di temi e persone con Harmony

Sfide da affrontare

- Criticita’
  - rispetto delle norme
  - protezione dei dati
  - funzionalita’ delle infrastrutture e dei servizi
- Standardizzazione
  - policy, strumenti, procedure
- Strumenti
  - collezione e normalizzazione informazioni
  - analisi e correlazione eventi, analisi e gestione minacce
  - integrazione con End Point Protection
- Monitoraggio ed allarmistica
  - Monitoraggio incidenti, vulnerablity alert, preallarmi
  - Gestione degli incidenti, analisi dei rischi
- Interazione verso terzi
  - Condivisione di informazioni di threat intelligence
  - Interazione con CERT/CSIRT in Italia ed in Europa
- Formazione
  - Campagne awareness e self-assessment
  - Formazione interna ed esterna

Una nuova organizzazione

- La sicurezza informatica dell'INFN deve essere una sola
  - Servizi Nazionali, strutture, centri di calcolo, laboratori, INFN Cloud/Datacloud, DSI

- CCR Security e WP4 di Datacloud: una sola attivita'
  - il WP4 nasce come gruppo costituito dalle persone attive sia in INFN Clooud che nel gruppo Security di CCR
  - quasi totale sinergia di attivita' e di persone
  - e' l'attivita' del gruppo security su questioni specifiche di Datacloud

- Policy e compliance: una sola attivita'
  - il WP7 di Datacloud integra le attivita' di analisi di policy e compliance di Harmony e della CCR
  - anche qui ci sono importanti sinergie di contenuti e persone

Centralizzazione: cosa

Molte attivita' devono necessariamente essere sviluppate e gestite a livello centrale

- Policy
- Strumenti di verifica della compliance
- Strumenti e infrastrutture di collezione dati
- Strumenti e procedure di analisi, threat intelligence
- Interazione ed integrazione con altre realta'
- Organizzazione delle attivita' di formazione
- Coordinamento della attivita' di R&D

Centralizzazione: perche’

- Visibilita’ e reattivita’ globale ad eventi di sicurezza
- Strumenti migliori e piu’ efficaci (SOC, monitoring)
- Ottimizzazione del man power
- Aumento delle competenze
- Maggiore efficacia nella gestione degli incidenti

Migliore postura verso la CyberSecurity

Migliore efficacia del lavoro delle persone

La fondamentale attivita' locale

- Attivita' sono necessariamente di pertinenza delle strutture
  - asset management, risk assessment
  - data protection, implementazione delle misure (GDPR, AgID)
  - ...

  ma attraverso processi e strumenti definiti e coordinati

- Attivita' centralizzate non significa persone centralizzate
  - indispensabile la collaborazione alle attivita' centrali del personale delle strutture
  - garanzia di mantemimento e potenziamento del know how a livello locale

Il team di Cyber Security INFN siete voi

Il progetto

Progetto di una struttura di gestione della sicurezza informatica dell'INFN

- Presentato in CCR ad aprile 2022
- Adottato nel PTI-PA in accordo con l'RTD
- Presentato in CD in gennaio 2023

Basato sulla adozione di un cybersecurity framework

- Protect: configurazioni di sistemi e servizi, scansioni, formazione, ...
- Monitor: creazione di un SOC (collect, threat intelligence, vulnerability mgmt ...)
- Respond: sviluppo CSIRT INFN
  - unificazione di CSIRT INFN e CSIRT INFN Cloud
- Govern: interazione con CCR (policy, finanziamenti), coordinamento strutture, ...

INFN Cyber Security Team

Struttura di gestione della Cybersecurity dell'INFN

- adozione di un security framework (pianificazione, controlli, misure, correzione)
- definizione e adozione di policy e strumenti comuni e coordinati
- struttura operativa centrale per coordinare le funzioni di protezione, controllo e risposta
- creazione di una infrastruttura centralizzata per la raccolta degli indicatori dalle strutture, la loro analisi e la threat intelligence
- adozione di tool di risk assessment e monitoring omogenei
- standardizzazione della valutazione e gestione del rischio
- definizione di un programma di formazione interna (team) ed esterna (utenti)
- coordinamento con CERT/CSIRT nazionali ed internazionali

Risorse

L’azione di gestione e di coordinamento di queste attivita’ richiede un impegno importante e garantito

- il best effort non e’ sufficiente
- percentuali piccole sono inefficaci

Il management deve supportare questa attivita’ con

- riconoscimento del lavoro del personale delle strutture
  - e’ un lavoro che va a beneficio della struttura, oltre che dell’Ente nel suo complesso
- (nuovo) personale dedicato a supporto
  - posizioni dai concorsi per il PNRR

Ma non possiamo aspettare.

Il workshop

- Con questo workshop iniziamo l'attivtia' lavorativa
  - identificazione di azioni
  - definizione ed avvio di progetti specifici

- Il programma:
  - Presentazione del progetto (Luca)
  - CSIRT (Gianluca, Luca, Vincenzo)
  - Strumenti OSINT (Gianluca, Luca, Patrizia)
  - SOC (Alessandro, Gianluca, Luca, Vincenzo)
  - Strumenti per le strutture (Roberto, Gianluca, Luca)
  - La nuova disciplina europea sulla cyber security: aspetti tecnico-giuridici a confronto (Barbara, Nadina)
  - Discussione piano formativo (Silvia)
  - Discussione finale