ISTITUTO NAZIONALE DI FISICA NUCLEARE

CNAF

INFN-19-19/CNAF
12 novembre 2019

PROPOSTA PER LA DEFINIZIONE DI INFN CSIRT

Riccardo Veraldi e Vincenzo Ciaschini[1]

[1)]INFN-CNAF, Viale Carlo Berti Pichat, 6, 40127 Bologna, Italy

Abstract

Il seguente documento definisce l'implementazione generale di INFN CSIRT e le funzioni principali erogate per la propria *constituency*.

CCR-57/2019/P

Published by
Laboratori Nazionali di Frascati

Indice

1 CSIRT: significato, considerazioni e definizioni generali

1.1 Premessa

Riguardo al nome ufficiale da attribuire al CERT dell'INFN è stato scelto l'utilizzo dell'acronimo CSIRT quale Computer Security Incident Response Team, in quanto la parola CERT (Computer Emergency Response Team) non è più un acronimo ma è diventato, a partire dal 1997, un termine coperto da Copyright ©. Il proprietario è la Carnegie Mellon University (Pittsburgh, PA).

1.2 Definizione di CSIRT

Il significato di CSIRT è comunemente associato ad un gruppo di professionisti dedicato alla gestione degli incidenti di sicurezza informatica, in grado di cooperare e coordinare gli interventi necessari per contenere il loro impatto e ripristinare le normali o accettabili condizioni operative nell'erogazione dei servizi. Al fine di attenuare gli impatti e ridurre al minimo il numero di interventi richiesti, la maggior parte degli CSIRT fornisce anche servizi di prevenzione e di formazione e sensibilizzazione per la propria comunità di riferimento. Il funzionamento di uno CSIRT si basa sulla gestione integrata dei flussi informativi provenienti dalla propria *constituency* e dal mondo esterno, in qualità di unica interfaccia operativa per le attività di Information Sharing. Gli CSIRT capaci di raccogliere, oltre alle segnalazioni di incidenti informatici, le vulnerabilità e le potenziali minacce, analizzano gli impatti che si potrebbero verificare sulle infrastrutture informatiche della propria *constituency* (o sull'organizzazione stessa) così da identificare i rischi e dunque le più adeguate contromisure. Nel contesto attuale, secondo le linee guida ENISA e AGID, lo scopo e la missione di uno CSIRT sono stati estesi, e oltre a parlare di "Response" (risposta) si pone l'accento sulla nozione di "Readiness" (prontezza/preparazione). In particolare, a fronte dell'evoluzione dei servizi informatici, della crescente sofisticazione delle minacce e della rilevanza strategica dei target cui le stesse si rivolgono, ogni organizzazione, di fronte ad un incidente di sicurezza informatica, deve prepararsi per tempo, sviluppando la propria cultura sulla cybersecurity e mettendo in campo azioni proattive e procedure tese a ridurre la probabilità ma anche l'impatto degli incidenti. "Readiness" in tema di sicurezza informatica vuol dire dunque sviluppare quella capacità di adattare i propri sistemi di difesa (non solo tecnologici, ma anche di processo e procedurali) sulla base dell'evoluzione delle minacce, della scoperta di nuove vulnerabilità e degli incidenti avvenuti sia internamente che subiti da altre organizzazioni.
Elementi fondamentali per assicurare la Readiness sono in particolare:

- capacità di rilevazione e risposta agli incidenti;
- capacità di comprendere ciò che sta avvenendo sulle proprie infrastrutture e sui sistemi, attraverso una conoscenza approfondita dei propri asset, incluse le configurazioni dei sistemi e le vulnerabilità;

- capacità di individuare le minacce esterne e le modalità con cui potrebbero essere colpiti i propri sistemi e servizi informatici;
- capacità di condividere informazioni, in modo efficiente, per consentire all'interno della propria organizzazione e tra altri CSIRT di condividere la conoscenza al fine di anticipare eventuali attacchi, innalzando in questo modo il proprio livello di protezione.

1.3 Missione di uno CSIRT

Le attività critiche di uno CSIRT si possono sintetizzare nei seguenti punti principali:

- fornire supporto ed assistenza specialistica alla *constituency* nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
- agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori;
- incentivare l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite;
- collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security;
- accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale.

1.4 Identificazione della *constituency*

Nell'ambito del proprio funzionamento, ogni CSIRT interagisce con una vasta gamma di entità e soggetti. La più importante comunità tra queste è quella per cui lo CSIRT stesso è stato fondato e a cui rivolgerà i propri servizi, ovvero la sua *constituency*, cioè la comunità di utenti ed entità interne o esterne all'organizzazione cui lo CSIRT appartiene e verso cui lo CSIRT eroga istituzionalmente i propri servizi. Lo CSIRT, oltre che con la propria *constituency*, potrà comunque intrattenere rapporti con ulteriori entità non ricomprese in quest'ultima, organizzate all'interno di una o più "community" informali, più o meno strutturate (si pensi ad esempio ad attività di scambio di informazioni tra le parti regolate da specifici accordi o a regolamenti generali definiti dalle community stesse). L'identificazione della propria *constituency* è un'operazione estremamente critica per l'efficacia di uno CSIRT. Infatti, a seconda della gamma di servizi offerti dallo CSIRT e della natura di tali servizi, lo CSIRT

potrebbe anche avere la necessità di definire più di una *constituency*. È altresì possibile che uno o più CSIRT offrano un determinato servizio a *constituency* che si sovrappongono, con il rischio di avere uno scarso coordinamento in termini di ruoli e responsabilità, nonché una potenziale duplicazione degli sforzi e servizi inefficaci e/o in reciproco contrasto. Una volta individuata e definita la *constituency*, lo CSIRT dovrebbe promuovere sé stesso e i suoi servizi sia all'interno della propria *constituency* che al di fuori della stessa nel modo più ampio possibile per garantire una chiara comprensione del suo ruolo e dei servizi offerti ed ottenere un riconoscimento all'interno della più ampia comunità degli CSIRT (Ad esempio CSIRT a livello italiano ed europeo). Le informazioni sulla propria esistenza e i servizi erogati dovrebbero essere diffuse attraverso il maggior numero possibile di canali di comunicazione, inclusi quelli istituzionali (sito web, ecc.), organizzazione di workshop e in generale attività di sensibilizzazione, nonché l'ottenimento di certificazioni riconosciute a livello internazionale quali, ad esempio, *Trusted Introducer*. Quest'ultima entità forma il backbone dell'infrastruttura di servizi CSIRT ufficialmente riconosciuti come tali, accredita e riconosce i vari team di cybersecurity secondo il livello di maturità dimostrato nell'erogare i servizi compresi all'interno dello CSIRT candidato.

2 INFN CSIRT

2.1 Perchè un CSIRT dedicato?

Con il documento "Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali" del 14 Maggio 2019, AGID fornisce le linee guida per la costituzione di CSIRT regionali e locali, in riferimento esplicito alla Pubblica Amministrazione Italiana. In particolare si cita:

"*In accordo con gli indirizzi strategici nazionali, devono quindi essere create le condizioni per sviluppare un'azione integrata che metta a fattor comune le diverse attribuzioni istituzionali delineate, anche al fine di avere un maggior presidio ed assicurare una maggiore efficacia delle azioni sul territorio e nel rispetto delle esigenze delle relative* constituency*. In quest'ottica si inserisce l'esigenza di definire un modello organizzativo ed operativo per la costituzione e l'avvio di CERT regionali nell'ambito della Pubblica Amministrazione italiana, che possa delineare uno standard nazionale rispetto al quale basare ogni implementazione degli stessi su base locale, tenendo in considerazione ed indirizzando al meglio le esigenze dei singoli settori, dell'industria ed i vincoli specifici delle singole amministrazioni*".

Inoltre l'INFN si è da sempre avvalsa del servizio GARR-CERT per la gestione, analisi e risoluzione degli incidenti di cybersecurity. La struttura GARR-CERT non è più gestita da personale INFN, pertanto si auspica in tempi brevi la realizzazione da parte dell'INFN di una propria struttura interna in tal senso, nella quale i membri di INFN CSIRT siano individuati all'interno del personale dipendente INFN.

2.1.1 I vantaggi di avere uno CSIRT

Avere un gruppo di sicurezza IT dedicato in particolar modo alla gestione degli incidenti di cybersecurity aiuta un'organizzazione ad attenuare e prevenire gli incidenti gravi, nonché a proteggere i suoi beni di valore. Altri possibili vantaggi sono:

- avere un coordinamento centralizzato per le questioni di sicurezza IT all'interno dell'INFN;
- gestione e risposta centralizzata e specializzata agli incidenti di sicurezza informatica;
- avere a portata di mano le competenze per sostenere e aiutare gli utenti a riprendersi rapidamente dagli incidenti di sicurezza informatica. Per questo però è anche necessaria una continua formazione del personale staff INFN, che dedica una parte del proprio tempo allo CSIRT;
- tenersi al corrente degli sviluppi nel campo della sicurezza;
- stimolare la cooperazione all'interno dell'INFN in merito alla sicurezza IT (sensibilizzazione);

2.2 Constituency

La *constituency* è la comunità di riferimento ovvero l'insieme dei "clienti" dello CSIRT. Nel caso di INFN CSIRT è l'INFN stesso inteso globalmente come Ente, con i suoi utenti e infrastrutture di calcolo scientifico ed ICT. In tal senso quindi INFN CSIRT si può considerare e definire come entità all'interno della categoria degli CSIRT di tipo *interno*, ovvero fornisce servizi soltanto all'organizzazione che lo ospita.

2.3 Mission

Lo scopo principale di INFN CSIRT è di fornire informazioni e assistenza ai propri utenti di riferimento ovvero le sezioni e i laboratori dell'INFN nell'attuazione di misure proattive volte a ridurre i rischi di incidenti di sicurezza informatica e nella risposta a tali incidenti quando questi si verificano. Offrire sostegno alla propria *constituency* sulla prevenzione e risposta agli incidenti di sicurezza informatica. In particolare:

- Gestire gli incidenti di cybersecurity che possono presentarsi all'interno della rete e sistemi informatici dell'INFN;
- aiutare ed indirizzare i sistemisti e gli utenti dell'INFN condividendo informazioni relative all sicurezza informatica, avvalendosi anche di strumenti di formazione;

2.4 Modello di attività

INFN CSIRT si caratterizza operativamente all'interno del modello (ENISA) *incorporato*, dal momento che lo CSIRT opera all'interno di un'organizzazione IT preesistente che comprende i Servizi Calcolo e i centri di calcolo scientifico dell'INFN, nonché la Commissione Calcolo e Reti (CCR) con le proprie strutture dedicate ai temi della sicurezza (gruppi Security e Harmony). INFN CSIRT é guidato da un responsabile di gruppo che risponde delle attivitá alla CCR, nell'ambito del gruppo Security. Il responsabile riunisce e coordina il personale con capacità tecniche necessarie per risolvere gli incidenti e lavorare alle altre attività dello CSIRT. Puó inoltre chiedere assistenza all'interno delle organizzazioni già esistenti (ad esempio il Gruppo Security della CCR) per ricevere un sostegno specialistico.

2.5 Servizi forniti da INFN CSIRT

- Gestione incidenti di cybersecurity.

  INFN CSIRT si occupa di tutti i tipi di incidenti di sicurezza informatica che possono presentarsi all'interno della propria *constituency*. Il livello di supporto dato da INFN CSIRT varierà a seconda del tipo e della severità degli incidenti e nei casi più gravi verrà fornita una risposta all'interno di una giornata lavorativa. Come riferimento i seguenti incidenti saranno quelli gestiti da INFN CSIRT, con priorità in ordine decrescente:

  1. attacco diretto con root/privileged escalation verso qualsiasi server o sistema informatico facente parte della rete INFN;
  2. qualsiasi altro tipo di attacco diretto senza root escalation, che possa peró dare accesso diretto non autorizzato a qualsiasi server o sistema informatico facente parte della rete INFN;
  3. attacco diretto DoS e DDoS verso server, apparati di rete che fanno parte della rete dell'INFN;
  4. qualsiasi tipo di azione malevola riconducibile alle già sopra citate che originino internamente alla *constituency* e abbiano come target sistemi esterni alla rete INFN;
  5. qualsiasi tipo di azione malevola riconducibile alle già sopra citate che originino internamente alla *constituency* e abbiano come target altri sistemi all'interno della rete INFN;
  6. attacchi di ogni altro tipo su larga scala in cui siano coinvolti sistemi informatici INFN come vittima o causa dell'attacco;
  7. uso abusivo delle infrastrutture informatiche dell'Ente, dovute ad un'attacco di qualsiasi tipo (ad es: web site defacement, divulgazione di informazioni offensive o diffusione di informazioni implicanti un crimine, mining di criptovalute, ecc);
  8. scansioni di porte TCP/UDP aperte (host e port scan) che non abbiano carattere di attacco DoS;

9. accessi errati da parte di utenti che, pur comportando il lock di una singola utenza, non denotano una particolare attività illecita mirata al DoS, o all'accesso non autorizzato ai sistemi informatici dell'INFN;
10. fingerprinting su sistema operativo e applicativi di sistemi informatici INFN;
11. allarmi di tipo Policy Violations, determinati dalla presenza di software non autorizzato sui sistemi client (Instant Messaging, File Sharing, P2P, ecc.)

Ogni altro tipo di incidente verrà prioritizzato a seconda del grado di severità che verrà assegnato a discrezione di INFN CSIRT.

- Gestione delle relazioni con altri CSIRT e gruppi di lavoro anche internazionali su questioni relative alla cybersecurity quali GARR-CERT, EGI-CSIRT, WLCG Security Operation Centres (SOC), CERN SOC, ecc.;
- Distribuzione delle security advisory:
  - raccolta di informazioni;
  - valutazione della pertinenza e della fonte delle informazioni;
  - valutazione del rischio sulla base delle informazioni raccolte;
  - distribuzione delle informazioni;
- security consulting nei confronti della propria *constituency*;
- corsi di formazione rivolti al personale INFN relativamente a tematiche di cybersecurity a diversi livelli:
  - corsi per utenti generici volti a prevenire gli incidenti più comuni e banali (ad es: phishing);
  - corsi per utenti che amministrano i dispositivi "Tecnico-Scientifici" ad uso personale [rif. implementazione Misure Minime AgID];
  - corsi per amministratori di sistema;
- security audit/assessment: da effettuare in collaborazione con gli Auditor INFN per la cybersecurity;
- scansione vulnerabilità dei sistemi: da effettuare con la collaborazione del gruppo Auditing/Security della CCR;

2.5.1 Procedure di gestione incidenti di sicurezza informatica

INFN CSIRT assiste la propria *constituency* negli aspetti di gestione tecnica degli incidenti di cybersecurity definendo le seguenti procedure:

- Triage:

  - assessment riguardo all'incidente di cybersecurity per verificare che in effetti l'incidente stesso sia accaduto e non sia un falso positivo;
  - determinare l'entità e definire la gravità dell'incidente;

- Incident Response.

  INFN CSIRT eroga il servizio di gestione e risoluzione degli incidenti di cybersecurity limitatamente ai sistemi informatici dell'INFN, in particolare dando consulenza ai propri utenti sui seguenti argomenti:

  - rimozione delle vulnerabilità che sono state causa di un incidente;
  - mettere i sistemi compromessi in sicurezza relativamente all'incidente in corso;
  - collezione dell'evidenza dei fatti relativi a un incidente, log di sistema, osservazione sull'evoluzione dell'incidente in corso ove possibile ed eventualmente predisporre "trappole" in caso di accessi non autorizzati ai sistemi;

  INFN CSIRT normalmente non agisce direttamente sui sistemi compromessi e non applica direttamente le azioni risolutive sui sitemi stessi. Tale attività è compito dei Servizi Calcolo locali delle strutture o dei centri di calcolo scientifico dove si sia verificato un incidente.

- Incident Response Coordination

  - ove possibile si cerca di determinare la causa iniziale dell'incidente (vulnerabilità sfruttate);
  - tenere i contatti con altri siti non INFN che possono essere coinvolti in un incidente;
  - contattare l'Ufficio Legale INFN nel caso di incidenti di sicurezza ove vi sia il sospetto di un illecito penale, o nei casi più gravi dove sia richiesta l'interazione con le Forze dell'Ordine;
  - quando richiesto riportare l'incidente ad altri CSIRT (ad esempio GARR-CERT, EGI-CSIRT, ecc.);
  - se e quando richiesto da incidenti su larga scala, diffondere bollettini straordinari agli APM;

2.5.2 Gestione degli artefatti

Si tratta di gestire la raccolta e l'analisi di qualsiasi elemento o evidenza (file, codici malevoli, script di exploit, root kits, tracce in memoria) che sono impiegati o in generale sono coinvolti nella realizzazione di azioni malevole.
INFN CSIRT è disponibile a realizzare un'analisi tecnica limitata degli artefatti reperiti in un sistema compromesso o artefatti segnalati dalla propria *constituency*. Le azioni che possono essere eseguite sono:

- identificazione del tipo di file;

- comparazione con artefatti già in possesso;
- eventuale comparazione con artefatti già gestiti da GARR-CERT;
- ricerca online su data base di artefatti;

2.6 Risorse infrastrutturali e informatiche

INFN CSIRT utilizza i seguenti canali di comunicazione:

- sito web INFN CSIRT (http://csirt.infn.it)
  - Web form per riportare un incidente di sicurezza (http://csirt.infn.it/report)
- Email(PGP/GPG) csirt@infn.it
- Telefono

INFN CSIRT utilizza al suo interno per implementare i servizi critici, sistemi operativi intrinsecamente più sicuri, non utilizzati di norma per i servizi informatici o servizi di calcolo dell'Ente. Il servizio di gestione incidenti informatici/ticketing ed il servizio di posta elettronica utilizzano tecnologie di cifratura dello storage a livello di block device e dove possibile anche a livello applicativo.

2.7 Staff INFN CSIRT

Lo staff di INFN CSIRT, secondo il modello di gestione *incorporato* deve avvalersi di personale INFN, ovvero interno, costituito da almeno 5 persone provenienti dalle strutture dell'INFN che dedichino parte del loro tempo, non meno del 20%, alle attività dello CSIRT per complessivi 2 FTE effettivi. Una tra queste persone svolge l'attività di coordinamento dello CSIRT stesso, oltre alle normali attività tecniche relativamente ai servizi offerti, per un totale di 0.7FTE. I servizi minimi che possono essere erogati in questo scenario sono quelli precedentemente citati, escludendo corsi di formazione rivolti al personale INFN.

2.8 Potenziali destinatari delle informazioni rilasciate da INFN CSIRT

I destinatari o punti di contatto preferenziali di INFN CSIRT sono principalmente i seguenti:

- Contatti per la cybersecurity nelle varie strutture dell'INFN:
  - In questo caso il punto di contatto per INFN CSIRT sono gli APM della rete GARR relativi alla specifica sede INFN. Questi verranno contattati sia nella distribuzione delle security advisories, ma soprattutto saranno il punto di contatto principale in caso di incidenti di sicurezza di una specifica sede dell'INFN;
- gli utenti delle risorse di calcolo e rete dell'INFN;

  - gli utenti INFN dovrebbero in generale avere la minore interazione possibile con INFN CSIRT e l'APM GARR deve essere il punto di contatto preferenziale in virtù delle proprie responsabilità a trattare informazioni confidenziali relative a incidenti di sicurezza. In caso di sospetto incidente o allarme l'utente INFN deve contattare il proprio APM che provvederà a notificare INFN CSIRT;

- altre entità CSIRT;

  - altri CSIRT, quando dovessero essere partner in una investigazione riguardante un incidente di sicurezza, possono essere eventualmente considerati entità "trusted" per alcuni tipi di informazione confidenziale. Le informazioni condivise saranno limitate allo stretto necessario per arrivare alla risoluzione dell'incidente;
  - viene instaurata invece una stretta collaborazione con GARR-CERT in particolare riguardo agli incidenti più rilevanti per l'INFN e la condivisione di informazioni relativamente alle vulnerabilità e security threat, collaborazione sull'utilizzo di tool comuni in modo da coadiuvare ed agevolare la diffusione del know-how per entrambe le parti;

2.9 Comunicazione con INFN CSIRT

Dato il tipo di informazioni trattate da INFN CSIRT, l'utilizzo di una linea telefonica standard è ritenuta sufficientemente sicura anche senza cifratura. E-mail non cifrate non sono da considerarsi un metodo di comunicazione sufficientemente sicuro, ma saranno considerate come mezzo appropriato per inviare dati non sensibili. Indipendentemente dalla sensibilità del dato inviato a INFN CSIRT tramite E-mail, tutti i messaggi indirizzati a cert@infn.it vengono automaticamente cifrati sul server di posta dedicato allo CSIRT.

2.10 Protezione dei dati

Tutti i dati (e-mail, file, documenti ecc.) che sono ricevuti o generati da INFN CSIRT saranno catalogati nelle seguenti categorie:

- Dati pubblici:

  - tipologia di dato che non ha impatto per INFN CSIRT e la propria *constituency*. Questo tipo di dato non ha bisogno di alcun trattamento particolare e può essere memorizzato su qualsiasi dispositivo;

- Dati interni:

  - Dati interni a INFN CSIRT, ad esempio informazioni sul personale, informazioni sulle reti dell'INFN, dati riguardanti le architetture dei sitemi informatici e di rete dell'INFN;

- Dati confidenziali:
  - Tutti i dati generati o ricevuti da INFN CSIRT utilizzando specifici servizi, come ad esempio sistemi per la gestione degli incidenti di sicurezza, sono considerati dati confidenziali, ovvero dati che hanno un impatto rilevante per l'INFN, la rete ed i propri sistemi informatici. Accesso a questi dati viene concesso soltanto a membri staff di INFN CSIRT e vengono memorizzati all'interno dell'infrastruttura dedicata per la gestione degli incidenti. Questo tipo di dato è cifrato su dispositivo a blocchi e non disponibile se non a filesystem montato allo staff di INFN CSIRT.

    Se lo CSIRT dell'INFN si avvarrá di risorse informatiche dei Servizi Nazionali (SSNN) della CCR dell'INFN, Il personale responsabile della gestione dell'infrastruttura dei SSNN è da considerarsi come membro dello CSIRT.

2.11 Gestione dei dati relativi a incidenti di cybersecurity

Indipendentemente dalla categoria dei dati, questi devono essere trattati secondo le seguenti regole:

- in nessun modo i dati verranno memorizzati utilizzando servizi di cloud pubblici;
- i dati non devono essere memorizzati su dispositivi personali (PC portatili, laptop, smartphone ecc.)

Il backup dei dati sui sistemi di INFN CSIRT avverrà in modo cifrato e solo il personale autorizzato potrà avere accesso a tali dati.

3 Conclusioni

Il presente documento intende fornire una sintesi generale dei processi che coinvolgono INFN CSIRT e le attività di cui si occupa. Un numero adeguato di FTE, almeno DUE a tempo pieno per i servizi di base, deve essere dedicato allo CSIRT perché il servizio diventi operativo. Pertanto un numero di persone di staff uguale o superiore a 5 è lo stretto necessario per consentire al personale di dedicare allo CSIRT una percentuale ridotta del proprio tempo non inferiore però al 20%. I passi successivi per la creazione di INFN CSIRT sono:

- ricevere un riscontro, consigli e direttive dalla CCR per l'implementazione finale e procedere al piano attuativo vero e proprio;
- ricevere un riscontro dalla propria *constituency* per affinare i servizi forniti;
- esercitarsi in situazioni di emergenza;

- tenersi in stretto contatto con le varie comunità CSIRT in particolare con GARR-CERT, EGI-CSIRT, CERN SOC e WLCG-SOC, che guarda con molto interesse al nuovo servizio CSIRT proposto.