Proposta di istituzione del INFN-CERT

Vincenzo Ciaschini

Riccardo Veraldi

Gruppo Security INFN

- Sottogruppo CCR che si occupa di:
  - topologia LAN: configurazioni ottimali delle LAN e monitoraggio, ai fini della minimizzazione dei rischi e danni in caso di intrusione;
  - auditing: verifica della sicurezza delle LAN e dei server critici;
  - token USB: token hardware per la conservazione e gestione dei certificati X.509;
  - virtualizzazione servizi: Configurazioni standard per alcuni servizi strategici, per fornire, e mantenere, distribuzioni di macchine virtuali;
  - aspetti legali (Harmony): gestione documentazione accompagnatoria al Regolamento d'uso delle risorse informatiche e altri problemi legali-informatici.
  - **INFN-CERT**

CSIRT

- Istituzione incaricata di raccogliere le segnalazioni di incidenti informatici e potenziali vulnerabilità nei sistemi operativi e software utilizzati dalla comunità dei propri utenti
- Sinonimi di uso comune (e non)
  - CERT (Computer Emergency Response Team)
  - IRT (Incident Response Team)
  - CIRT (Computer Incident Response Team)
  - SERT (Security Emergency Response Team)

Modello CSIRT NREN

- Lo CSIRT della NREN (GARR-CERT) coordina/armonizza i vari CSIRT facenti capo ai singoli enti in un unico punto di contatto nazionale e provvede ai servizi core e alla distribuzione delle informazioni riguardanti gli incidenti verso i CSIRT locali
- L'INFN deve dotarsi di un proprio CSIRT

Costituzione di INFN-CERT

- Obiettivo
  - servizi per la gestione della sicurezza informatica relativi alla rete INFN
- Costituenti
  - Fanno parte dello STAFF INFN
- Punti di contatto con le sezioni INFN
  - APM sedi INFN ?
  - Responsabili servizi calcolo ?

INFN-CERT: servizi erogati ?

- **Alerts e warning**
- Gestione incidenti
  - Analisi incidenti
  - **Risposta agli incidenti, supporto e coordinamento**
  - Risposta agli incidenti con supporto on-site
  - **E' auspicabile una stretta collaborazione con il gruppo Harmony INFN e soprattutto con l'ufficio Legale INFN in caso di incidenti con possibile rilevanza penale**
- Gestione Vulnerabilità
- Security audit/assestment (su richiesta)
- Configurazioni, mantenimento della sicurezza informatica
- Sviluppo di security tools
- Servizi di intrusion detection
- Analisi forense dei dati relativi a incidenti informatici (chiavi di registro, file, log, timestamp ecc
- Analisi del rischio
- Business continuity-disaster recovery
- **Security consulting**
- **Awareness building**
- **Corsi di formazione**
- Valutazione dei prodotti

Struttura organizzativa INFN-CERT

- Descrivere le funzioni di base
- Organizzazione strutturale
  - Staff/team leader
    - Chi fa parte dello staff e chi coordina ?
  - Team operativo
    - Chi operativamente risponde agli incidenti ?
  - Esperti esterni
    - A livello tecnico
    - A livello legale

Staff: linee guida

- Per fornire 2 servizi principali (fra quelli elencati) almeno 4 persone ad es:
  - Distribuzione delle security advisory
  - Gestione incidenti
- Per organizzare uno CSIRT FULL SERVICE che risponde in orari di ufficio: da 6 a 8 FTE
- CSIRT FULL SERVICE 24/7: 12 FTE

Risorse infrastrutturali e informatiche

- Canali di comunicazione
  - **Sito INFN-CERT**
  - **Web form per riportare un incidente**
  - **Email (PGP/GPG S/MIME support)**
  - **Mailing list**
  - Social Network
- **Utilizzo di sistemi informatici intrinsecamente più sicuri**
- **Sistema per la gestione degli incidenti**
- Sistema di comunicazione out of band (in caso di attacco informatico)
- Ridondanza nella connessione a Internet
- Controllo di accesso agli uffici/building
  - Non realmente implementabile in caso di struttura distribuita
- Telefono/FAX numeri SMS dedicati
  - Non implementabile se non con un numero considerevole di FTE

Politiche di sicurezza e procedure

- Descrivere le procedure operative e amministrative
- Deve essere in linea con la legislazione vigente e gli standard in particolare relativa a
  - Protezione dei dati e privacy
  - Leggi sulla data retention
- Come viene gestita la divulgazione di informazioni in particolari ad altri CSIRT riguardo a incidenti ?

Codice di condotta

- Tutti i membri del INFN-CERT devono rispettare le regole su cosa sia consentito e non consentito o non etico fare:
  - Per es. come gestire dati confidenziali affidati allo CSIRT stesso ?
- E’ importante stabilire un codice di condotta ridiscusso quando necessario

Cooperazione con gli altri CSIRT

- In particolare collaborazione stretta con il GARR-CERT e utilizzo degli strumenti che gia' sono in essere forniti da GARR-CERT ad es:
  - Alert automatici agli APM (via email)
  - Elenco aggiornato vulnerabilita' piu' gravi e rilevanti

Gestione incidenti

- Ricezione di una segnalazione di incidente
  - Identificazione della sorgente
  - Rilevanza
  - Classificazione
- Valutazione della segnalazione riportata e sua successiva gestione
- Azioni
  - Aprire un ticket per l'incidente riportato
  - Gestire il ciclo di vita dell'incidente (con l'aiuto di tool opportuni)
  - Report finale sulla gestione dell'incidente stesso
  - Archiviazione incidente
- Fare riferimento alle pratiche di gestione ENISA

Classificazione incidenti

- **Denial of service**
- **Forensics**: any forensic work to be done by CSIRT.
- **Compromised Information**: Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
- **Compromised Asset**: Compromised host (root account, Trojan, rootkit), network device, application, user account
- **Unlawful activity**: Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature,likely involving law enforcement, Global Investigations, or Loss Prevention.
- **Internal Hacking**: Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
- **External Hacking**: Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
- **Malware**: A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan.
- **Email**: Spoofed email, SPAM, and other email security-related events.
- **Consulting**: Security consulting unrelated to any confirmed incident.
- **Policy Violations**: Sharing offensive material, sharing/possession of copyright material., Deliberate violation of Infosec policy, Inappropriate use of corporate asset such as computer, network, or application, Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

Possibili tool da utilizzare

- Gestione degli incidenti
  - The Hive Project, **RTIR**, OTRS
- Gestione indirizzi email istituzionali (RFC2142):
  - security@, infn-cert@, csirt@
- E-mail encryption
- Raccolta di informazioni relative a security threat, vulnerabilita', malware
  - MISP: Malware Information Sharing Platform
  - Threatcrowd

Cosa non fa il INFN-CERT

- Attivita’ di controllo sulle strutture.
- Gestione di violazioni del copyright.
- Consulenza legale diretta.

Collaborazione con il GARR-CERT

- Durante le fase iniziale di costituzione del INFN-CERT utilizzeremo alcuni servizi erogati da GARR-CERT:
  - Accesso alla lista degli APM
  - Alert inviati via email
- Stretta collaborazione in caso di incidenti o rischi diffusi ad elevata criticità

Man Power

- Costituenti di INFN-CERT
  - Fanno parte dello STAFF INFN

- Chi ha voglia di collaborare attivamente a questo nuovo progetto ?
  - Progettazione
  - Implementazione
  - gestione