WP 2.3
IT Security

Vincenzo Ciaschini

Stato attuale

- La sicurezza è "reattiva."
  - C'è uno sforzo di installare i sistemi in maniera sicura
  - Ma svariati sono in genere abbandonati a se stessi
  - E altri sono tenuti aggiornati solo sporadicamente
    - Con virtuose eccezioni
  - Le macchine vengono monitorate dal punto di vista funzionale o prestazionale, ma raramente dalla sicurezza.
    - Incidenti sono spesso scoperti per tre motivi:
      - Cominciano ad incidere sulle prestazioni,
      - Vengono usati per attaccare altri centri
      - Vengono scoperti da altri e riceviamo segnalazioni da CSIRT

Stato Attuale/2

- Quando si scopre un problema è "all hands on deck" e il problema viene in genere risolto in breve tempo
  - Ma possono passare mesi tra l'incidente e la sua scoperta

Evoluzione

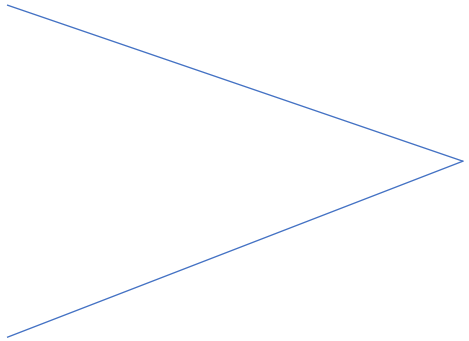
- Col passaggio al tecnopolo, il numero di macchine da tenere sotto controllo aumenterà
  - Quindi aumenterà anche il numero di quelle passate tra le maglie
  - Sarà più difficile intervenire fisicamente sulle macchine
- Occorre tenere sotto più stretto controllo i computer
  - Per rendere più difficile trovare buchi da sfruttare per un attaccante
  - Per accorgersi prima quando un buco viene trovato e un attacco ha successo.
- *NON esiste sicurezza SENZA monitoraggio*
  - Senza monitoraggio, al massimo si può dire che un sistema era sicuro in uno specifico momento.
  - Ma un sistema non è mai statico
    - Configurazioni vengono ritoccate.
    - Vengono scoperte insicurezze sul software installato

Proposta

- Creiamo un SOC (Security Operation Centre) al CNAF
  - Si tratta di un sistema di monitoraggio globale che tenga d'occhio tutti i computer del cnaf e la rete interna per scoprire anomalie che possano essere indicatori di una compromissione
  - Unito ad un sistema per intervenire direttamente sulle macchine in caso di necessità
  - Mai avuto qualcosa del genere al CNAF (o se è per quello, all'INFN) ma comune in molti centri di una certa dimensione
  - Verrà creato in maniera iterativa
    - Ingrandendolo mano a mano

Componenti:

- Monitoring dei computer
  - Software installato
  - Controllo dei log
  - Controllo della configurazione
  - Controllo dei processi
- Monitoring della rete
  - Analisi del traffico
  - IDS/IPS
- Capacità di intervento diretto sui computer
- Ricerca di indicatori di compromissione
  - Collegamenti con MISP



In tempo per la transizione

Raffinamenti successivi

Scelta dei componenti

- Preferenza a strumenti open source
- Preferenza a strumenti già conosciuti all'interno del cnaf
- Strumenti con supporto attivo e con politica di gestione delle vulnerabilità

Strategia Implementativa

- Studio di software da usare
- Implementazione di un prototipo su scala MOLTO ridotta. <- cominciamo la prossima settimana
  - Correzione dei problemi .
  - Reimplementazione di cio' che non funziona.
- Allargamento della scala
- Ripetere i passi precedenti fino a completamento

Rischi

- Non esiste nulla del genere all'INFN
  - Quindi dobbiamo imparare come crearlo
  - Prendendo inspirazione da come lo hanno costruito coloro che lo hanno già
  - Ma la possibilità di errore è sempre presente
  - Approccio iterativo con versioni successive

Rischi/2

- Personale
  - Non ci sono al CNAF persone dedicate alla sicurezza informatica
    - Tranne me
  - Ottenuto disponibilità di parte del proprio tempo da 8 persone
    - Per un totale di circa 3 FTE
    - Ma la responsabilità principale è un'altra. Se il loro responsabile toglie la disponibilità non c'è molto da fare
    - Nel caso, il progetto verrà ridotto nel suo scope
      - Ma comunque almeno la parte di monitoraggio dovrà rimanere attiva
      - Non c'è sicurezza senza monitoraggio
    - Almeno 2 FTE necessari sparsi su almeno 3 / 4 persone per tenere conto anche delle diverse specializzazioni

Rischi/3

- Personale/2
  - Non si tratta solo di costruire. Poi occorre anche tenerlo d'occhio.
  - Occorrono almeno 3, preferibilmente 4 persone (non FTE!)
    - Per tenere conto di ferie, malattie, missioni
    - Non è però necessario che sia a tempo pieno
    - Le cose ovviamente cambiano se viene rilevato un problema
      - Ma questo è già vero ora