Esercizio 4 settimana 9 Daniele D'Esposito

In caso di incidente di sicurezza, il CSIRT(Computer Security Incident Response Team) incaricato di rispondere all'incidente mettera' in atto il processo di Incident Response che si articola in 4 fasi:

1-Preparazione

Questa fase si effettua prima di qualsiasi possibile attacco e consiste nella **foundation** e nella creazione del team CSIRT.
La sottofase foundation e' la preparazione delle policy e delle procedure di incident response, la stesura di tutti i playbook necessari ad istruire tutti i componenti del team di gestione dell'incidente.

2-Rilevamento ed analisi

Questa fase avviene quando ci si accorge di essere sotto attacco e si cercano le evidenze dell'attacco, i vettori di attacco e gli asset compromessi attraverso i tool di monitoraggio della rete.

3-Contenimento, eliminazione e recupero

Questa e' la fase pratica di difesa contro l'attacco e si occupa di ridurre il piu' possibile i danni. Per fare cio' bisogna isolare l'incidente dal resto del sistema che e' ancora sano.
Una tecnica preventiva agli attacchi e' la **segmentazione** delle reti, cioe' dividere una rete in diverse LAN o VLAN, in modo tale che in fase di attacco risulta facile isolare una specifica porzione creando cosi' una rete di quarantena.
Se non dovesse bastare questa pratica, si passa all'**isolamento**, la completa disconnessione del sistema infetto dalle rete ma permettendogli ancora di connettersi a internet.
La misura piu' drastica e' invece la **rimozione** del sistema, impedendogli anche di connettersi ad internet.
Il recupero consiste nel ristabilire la normale operativita', l'applicazione di patch, la revisione delle politiche firewall, l'aggiornamento antivirus e il recupero dei sistemi compromessi.
Le tre tecniche principali per lo smaltimento o il recupero dei dispositivi sono:
-**Clear**: ripetuta sovrascrizione dei dati in modo da renderli illegibili
-**Purge**: in aggiunta al clear si usano tecniche di smagnetizzazione ma che non danneggiano fisicamente l'hardware
-**Destroy**: si distrugge fisicamente il componente

4-Attivita' post incidente

Si fanno delle considerazioni sull'accaduto e si analizza cosa si puo' migliorare per evitare che l'evento si possa ripetere in futuro.

Le fasi 2 e 3 si ripetono in loop fino a quando la minaccia non e' stata debellata e si puo' quindi passare alla fase 4.