S9 LEZIONE 4

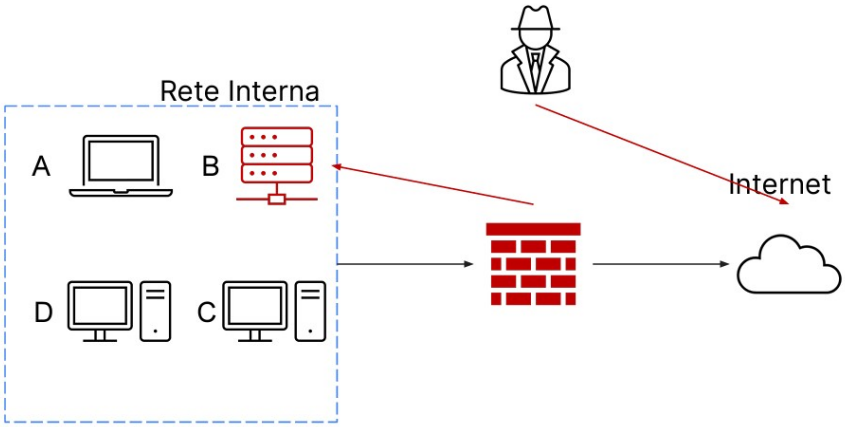
Traccia:

Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.
Mostrate le tecniche di:

I) Isolamento

II) Rimozione del sistema B infetto

III)Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



Il primo step di risposta agli incidenti è il contenimento del danno causato dall'incidente di sicurezza.
Le attività di contenimento hanno lo scopo di **isolare l'incidente** in modo tale che non possa creare ulteriori danni a reti e sistemi dell'azienda.
Una tecnica per la gestione di questo tipo di incidenti è la segmentazione:
include tutte le attività che permettono di dividere una rete in diverse LAN o VLAN, permettendo di separare il sistema, in questo caso il B, dagli altri dispositivi sulla rete, creando una rete ad hoc chiamata **rete di quarantena**.
Durante un attacco i sistemi che sono stati compromessi dovrebbero essere considerati non più affidabili e dovrebbero essere di conseguenza ripuliti prima di essere utilizzati nuovamente utilizzando le tecniche di **reconstrucion** e **rebuilding,** quindi tecniche per recuperare parti ancora affidabili e tecniche per ricostruire il sistema impattato.

Purge: utilizza tecniche di rimozione fisica (es: magneti:) per rendere le informazioni inaccessibili sui dispositivi compromessi

Destroy: è l’approccio più netto per lo smaltimento dei dispositivi impattati, in poche parole si utilizzano tecniche di disintegrazione e polverizzazione. Questo metodo è quello che comporta uno sforzo economico maggiore in quanto i dispositivi andranno distrutti per sempre.