M5 D7

ESERCIZIO 1

GIORNO 2 – INCIDENT RESPONSE

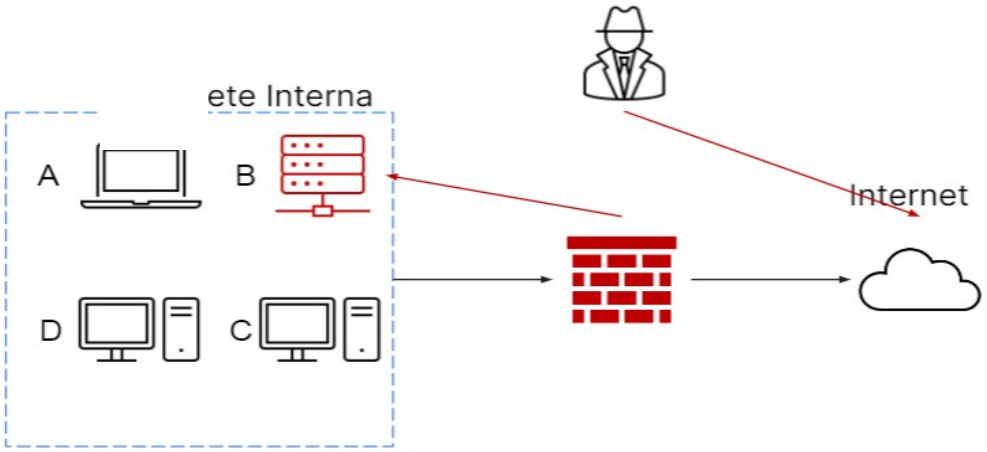
Il sistema B è stato compromesso interamente da un attaccante che è riuscito a bucare la rete e accedere al sistema tramite internet.

Team CSIRT varie azioni possibili di "remediation" tra cui fasi di contenimento, eliminazione e recupero:

1) **Contenimento ---> per ridurre gli impatti causati dall' incidente**

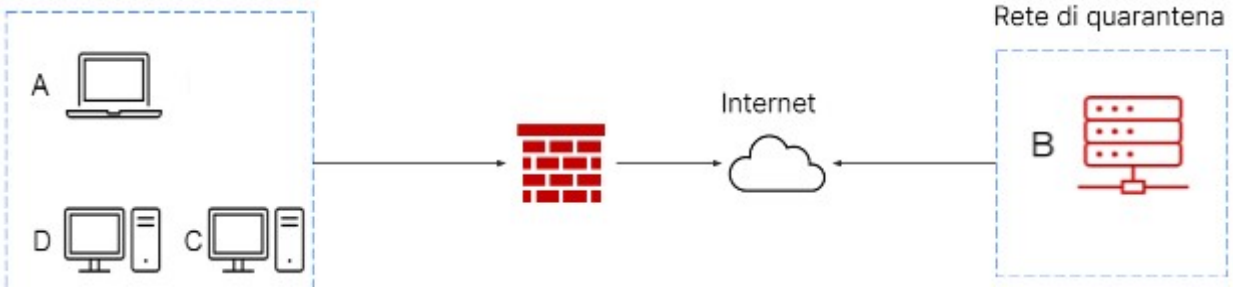
Scopo primario è isolare l' incidente in modo che non crei ulteriori danni a reti e sistemi.

Si deve isolare il sistema rispetto al resto della rete, in modo che il malware non si riproduca.



Isolamento:

Una tecnica valida per la gestione degli incidenti di sicurezza sulla rete è la segmentazione, utile anche nella fase di contenimento di un incidente in corso. La segmentazione include tutte le attività che permettono di dividere una rete in diverse LAN o VLAN. Ci permette così di separare il sistema B infetto dagli altri dispositivi sulla rete, creando una rete chiamata rete di quarantena.L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere l' accesso alla rete interna all' attaccante.

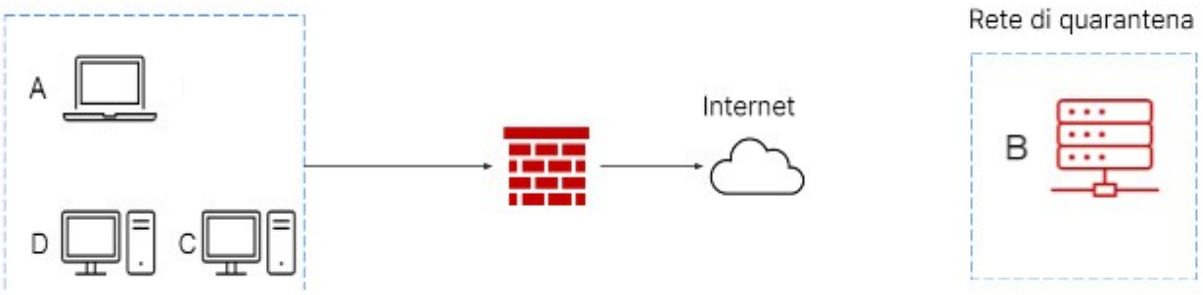


Ci sono casi in cui non è sufficiente l' isolamento.

In questo caso si pratica la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema infetto.

Rimozione:

In questo modo l' attaccante non avrà né accesso alla rete interna né alla macchina infetta.



A valle delle attività di contenimento, lo CSIRT passa alla rimozione dell' incidente.
Lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell' incidente all' interno della rete o sui sistemi. Può includere la rimozione di eventuali backdoor installate da un malware o ripulire dischi e chiavette USB compromesse.
La fase di rimozione dipende molto dal tipo di incidente di sicurezza, consultando la lista da seguire presente nei palybooks.

Fase di recupero (dati):

In questa fase sono molto delicate le attività di gestione dei media contenenti info sensibili:

- **Purge: è un approccio usato per la rimozione dei contenuti sensibili, prima di procedere allo smaltimento dei dischi compromessi, utilizza tecniche di rimozione fisica come l' utilizzo di forti magneti per rendere le info non più accessibili su certi dispositivi.**

- **Destroy: rispetto al precedente è un approccio più netto e definitivo per lo smaltimento di dispositivi contenenti dati sensibili. Si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature e trapanazione.**
  E' il metodo più efficace per rendere le info inaccessibili, tale che comporta un effort in termini economici maggiore.

- **Clear: questa tecnica è sicuramente meno invasiva rispetto alle prime due, il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche. Si utilizza un approccio di tipo read and write dove il contenuto viene sovrascritto più volte o si utilizza la funzione di factory reset (ripristino alle impostazioni di fabbrica) per riportare il dispositivo nello stato iniziale.**