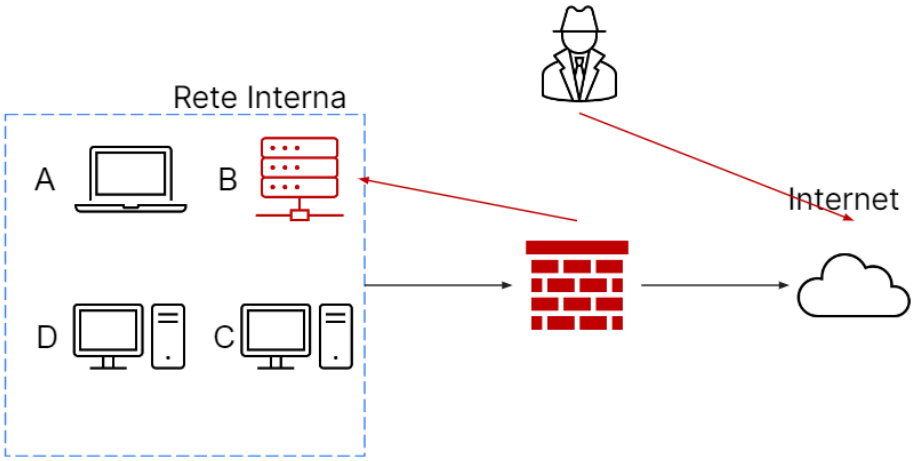
Gabriele Di giampietro **Esercitazione 22/12/2022**

Obiettivo: Abbiamo come riferimento una rete che è stata attaccata compromettendo il sistema B risultante essere un Database.

L'attacco è attualmente in corso e noi facciamo parte del team CSIRT (Computer Security Incident Response Teams), dobbiamo risolvere i seguenti quesiti:

- **Mostrare le tecniche di Isolamento e Rimozione del sistema infettato B**
- **Spiegare la differenza tra Purge, Destroy e Clear per l'eliminazione dei dati sensibili prima di procedere allo smaltimento dei dischi compromessi.**

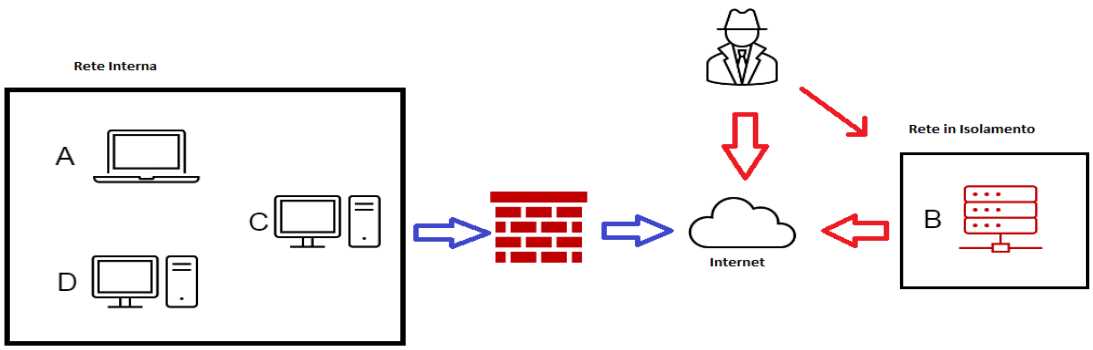


Tecnica di isolamento

Sapendo che un attacco è in corso e che un sistema è stato infettato, dobbiamo procedere nella fase di contenimento, eliminazione e recupero.

Partiamo infatti dal contenimento della minaccia, per ridurre gli impatti causati dall'incidente, nel nostro caso il sistema B che è un Database contente informazioni sensibili.

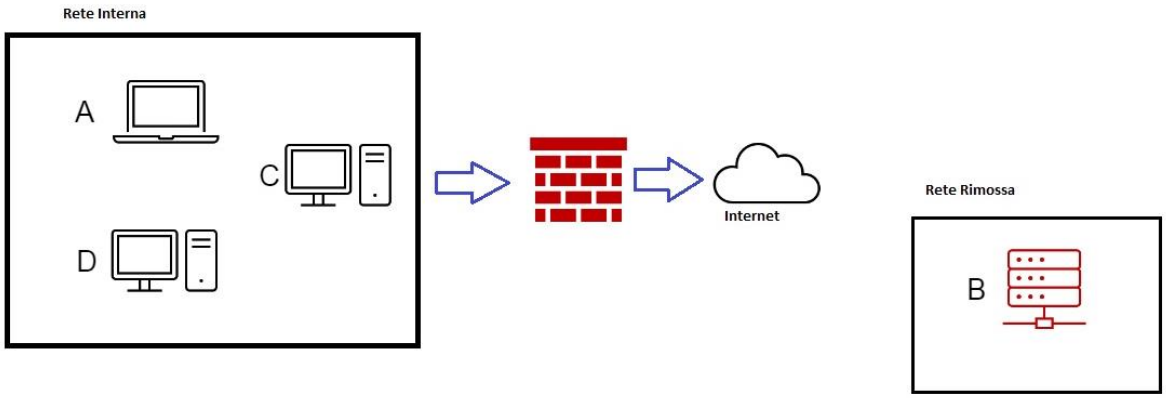
Una delle tecniche preventive per proteggere il sistema è la **segmentazione della rete** in varie sotto reti LAN o VLAN. Quando però questa non risulta efficace bisogna procedere all'**Isolamento** del sistema infettato. Nell'immagine che segue possiamo vedere la nostra soluzione per isolare il Database, sistema B.



Possiamo notare però che comunque l'attaccante continua ad avere accesso attraverso il collegamento ad Internet al sistema B, dove si trovano dati sensibili essendo un Database, anche se fondamentalmente non può accedere alla rete interna.

Tecnica della rimozione

Se l'isolamento non risulta quindi efficace, si può applicare un a tecnica più drastica e cioè quella della rimozione del sistema infetto sia della rete che da internet. Possiamo vedere nell'immagine la soluzione proposta per la rimozione del sistema B.



In questo caso neanche più l'attaccante è in grado di accedere al Database.

Smaltimento Dischi Compromessi

Dopo aver proceduto all'eliminazione dei sistemi compromessi, si procede alla fase di recupero dei dati eventualmente persi e del ripristino del servizio di rete. Nel nostro caso essendo stato compromesso un Database dobbiamo gestire il riutilizzo dei dischi o il loro smaltimento.

Per prima cosa bisogna verificare che i dati presenti sui dischi siano completamente inaccessibili o compromessi irrimediabilmente per poter procedere a loro smaltimento.

Possiamo scegliere di intraprendere tre percorsi per la gestione di dati sensibili del Database ormai compromesso:

- **1 Clear:** Il dispositivo viene completamente ripulito dai suoi dati all'interno con tecniche logiche, procedendo cioè con un Read and Write e cioè sovrascrivendo più volte i dati in esse contenuti; Oppure si procede ad un reset all'impostazioni di fabbrica (Factory reset). Questa opzione permette il riutilizzo del disco dopo essere stato in un certo senso pulito.

- **2 Purge:** In questo caso oltre alla rimozione dei dati all'interno del disco, vengo utilizzate anche tecniche di rimozione fisiche come l'utilizzo di forti magneti e lo smantellamento del disco che rende i dati al suo interno completamente inaccessibili. Questa opzione non permette però un completo non riutilizzo dei dischi che potrebbe portare ad un suo ripristino, se utilizzati strumenti e laboratori adatti.

- **3 Destroy:** Questo è l'approccio più drastico, in quanto anche dopo la rimozione logica e fisica dei dati dal disco, si procede alla sua completa distruzione e polverizzazione. Questo percorso rende definitivamente i dati inaccessibili e irrecuperabili, anche se può risultare il

più efficace ha comunque un costo economico elevato in quanto si dovrà sostituire il sistema con un nuovo disco.