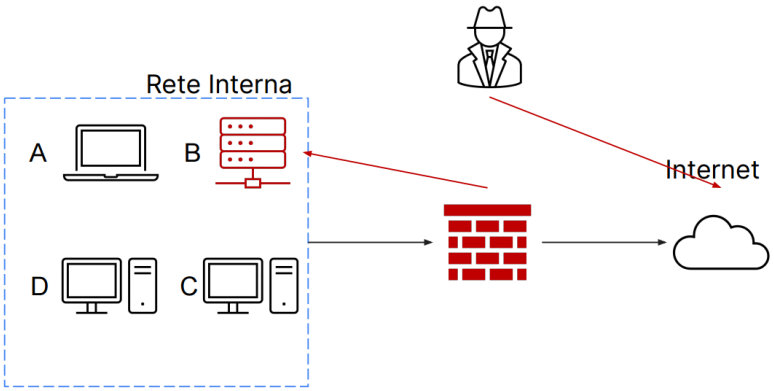
Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.



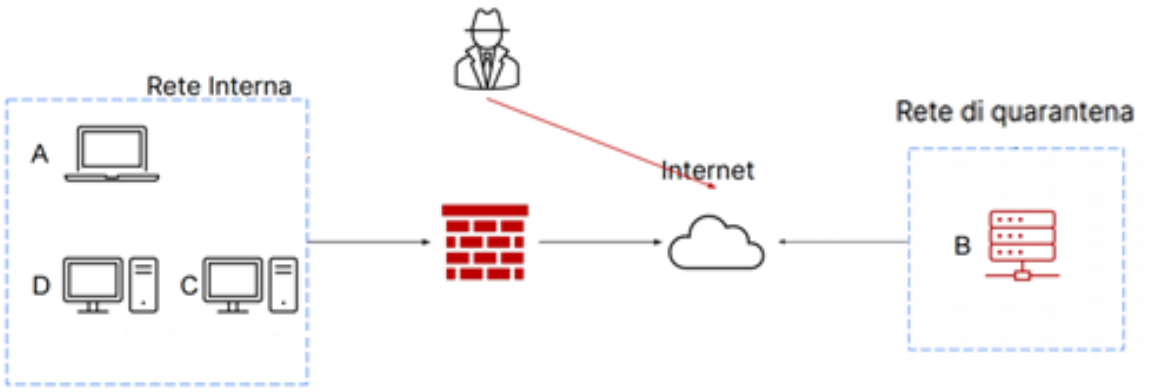
- **Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto**

Dopo che il team CSIRT ha avviato le procedure per determinare l'origine dell'incidente, i sistemi coinvolti e individuato potenziali ulteriori rischi, deve trovare rapidamente soluzioni per minimizzare le conseguenze dell'incidente. Questa fase si chiama **contenimento**, ed ha lo scopo circoscrivere l'incidente per prevenire ulteriori danni a reti e sistemi.

Una tecnica preventiva e strategica per gestire gli incidenti di sicurezza nella rete è la **"segmentazione"**. Questo implica isolare il sistema compromesso dagli altri dispositivi nella rete, creando una rete dedicata, spesso denominata **"rete di quarantena"**. Questa strategia è particolarmente preziosa anche durante la fase di contenimento di un incidente in corso.

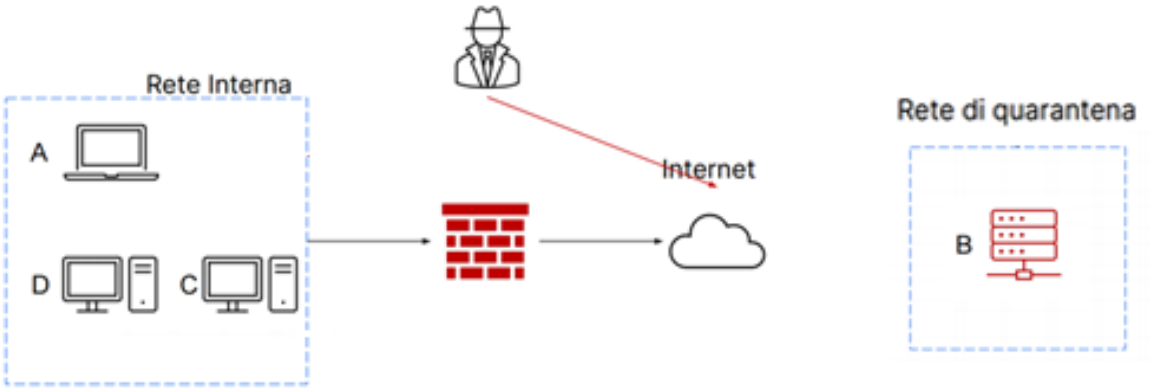
I. ISOLAMENTO

Anche se la segmentazione può contenere la propagazione del malware e limitare l'accesso dell'attaccante alla rete, spesso non basta per concludere la fase di contenimento. Quando è necessario un intervento più incisivo, si ricorre alla tecnica dell'**isolamento**, illustrata nell'immagine seguente. L'isolamento prevede la totale disconnessione del sistema compromesso dalla rete, per ridurre ulteriormente la possibilità che l'attaccante acceda alla rete interna.



II. RIMOZIONE

In alcune situazioni, l'isolamento potrebbe non essere sufficiente. Quando ciò accade, si adotta una misura di contenimento ancora più drastica: la **rimozione**. Si scollega completamente il sistema sia dalla rete interna sia da internet. In questa condizione, l'attaccante non potrà accedere né alla rete interna né al sistema compromesso.



- **Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear**

Dopo le operazioni di contenimento, il team CSIRT entra nella **fase di rimozione** dell'incidente. In questo stadio, l'obiettivo è cancellare ogni traccia, componente o processo legato all'incidente presenti nella rete o sui dispositivi. Successivmente si entra nella **fase di recupero**. Questa fase ha come obiettivo il ripristino della funzionalità normale delle applicazioni e dei servizi. I sistemi, server e host violati durante un attacco non dovrebbero più essere considerati sicuri. Pertanto, è essenziale pulirli accuratamente prima di rimetterli in uso. Durante il recupero può emergere la necessità di gestire lo smaltimento o il riutilizzo di un disco o un dispositivo di storage precedentemente compromesso. In tale circostanza, è fondamentale assicurarsi che tutte le informazioni su tale dispositivo siano totalmente inaccessibili prima di decidere se scartarlo o riutilizzarlo.

Di solito, esistono tre alternative per la gestione di dispositivi che conservano dati sensibili:

- **Clear**
- **Purge**
- **Destroy**

DIFFERENZA TRA PURGE E DESTROY

Con la tecnica **purge** si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come nel caso di **clear,** ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili. **Destroy** rappresenta invece la strategia più drastica per l'eliminazione di dispositivi che conservano informazioni sensibili. Al di là dei metodi logici e fisici precedentemente descritti, vengono applicate tecniche avanzate come la disintegrazione, la riduzione in polvere dei dispositivi attraverso alte temperature e la perforazione. Sebbene questa sia indubbiamente la soluzione più affidabile per assicurare l'inaccessibilità dei dati, è anche la più onerosa dal punto di vista economico.

In sintesi, il metodo **purge** non è mirato a distruggere il dispositivo danneggiato, ma solo le informazioni in esso contenute. Il metodo **destroy**, invece, comporta la distruzione fisica del dispositivo, rendendolodel tutto inutilizzabile.