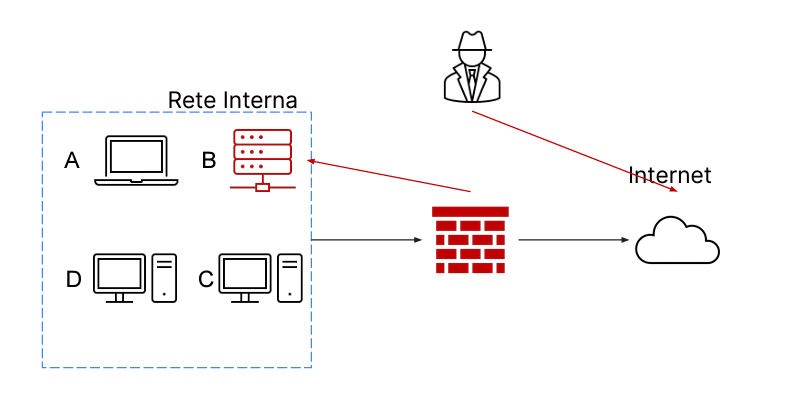
**Traccia:**

Con riferimento alla figura, 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:

1. *Isolamento*;
2. *Rimozione del sistema B infetto*;
3. Spiegate la differenza tra *Purge* e *Destroy* per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



**CSIRT** è l'acronimo di *Computer Security Incident Response Team*, che in italiano significa "Squadra di Risposta agli Incidenti di Sicurezza Informatica".

Un CSIRT è un gruppo di professionisti esperti nel campo della sicurezza informatica, incaricato di *gestire e rispondere agli incidenti di sicurezza informatica* all'interno di un'organizzazione o di una comunità.

Quando si presenta un caso come quello in oggetto, per rispondere efficacemente, prima di tutto si deve attuare un piano di **Isolamento** del sistema.

L’isolamento consiste nella completa disconnessione del sistema infetto (B in questo caso) dalla rete, per restringere l’accesso alla rete interna da parte dell’attaccante.

C’è da specificare che, prima dell’isolamento, si può preventivamente **Segmentare** la rete per contenere un incidente in corso. La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN, permettendo di separare il sistema infetto dagli altri dispositivi della stessa rete, creando una rete ad hoc, detta **rete di quarantena.** Solo quando questo non è sufficiente si passa alla fase di isolamento di cui sopra.

Ci sono casi in cui l’isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa **Rimozione del sistema** dalla rete. Prima di procedere alla rimozione del sistema compromesso, si esegue un backup dei dati critici presenti nel sistema B per garantire la loro integrità e disponibilità; dopodiché si da il via alla fase di formattazione completa per eliminare eventuali tracce dell'attacco e dei malware.

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la fase di **recupero**. Essa consiste nel *ristabilire la normale operatività* delle applicazioni e dei servizi. Include ad esempio il recupero dei dati e delle informazioni perse, l’applicazione delle patch dove disponibili per eventuali sistemi obsoleti, la revisione delle politiche dei firewall, IPS e IDS oppure l’aggiornamento delle firme degli antivirus.

Infatti, lo scopo della fase di recupero è anche quello di evitare che lo stesso attacco possa capitare nuovamente in futuro; attuando anche una monitorizzazione delle attività per individuare eventuali tentativi di reinfezione o attività sospette.

Durante la fase di recupero, ci si trova spesso a dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso.

Tale scelta dipenderà in gran parte dalle politiche di sicurezza dell'organizzazione e dalla sensibilità dei dati archiviati sul supporto.

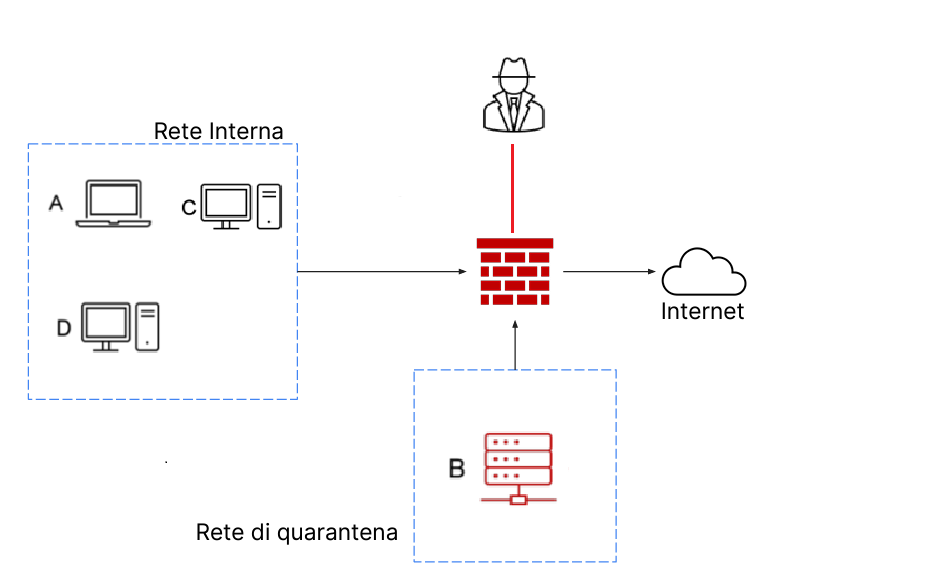
Generalmente si ricorre a tre opzioni in particolare:

* **CLEAR:** attraverso questo processo il dispositivo viene completamente ripulito avvalendosi di tecniche *logiche*, come ad esempio la sovrascrizione del contenuto più e più volte; o riportandolo allo stato iniziale con la tecnica del *factory reset*;
* **PURGE**: un processo di eliminazione sicura dei dati sensibili dal sistema di archiviazione, rendendoli irrecuperabili. Esso può coinvolgere l'uso di strumenti software specializzati per sovrascrivere i dati sensibili più volte con dati casuali o nulli, al fine di rendere impossibile il loro recupero, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;
* **DESTROY**: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili; si utilizzano tecniche di laboratorio come disintegrazione e polverizzazione dei media ad alte temperature, rendendo fisicamente impossibile il recupero dei dati.

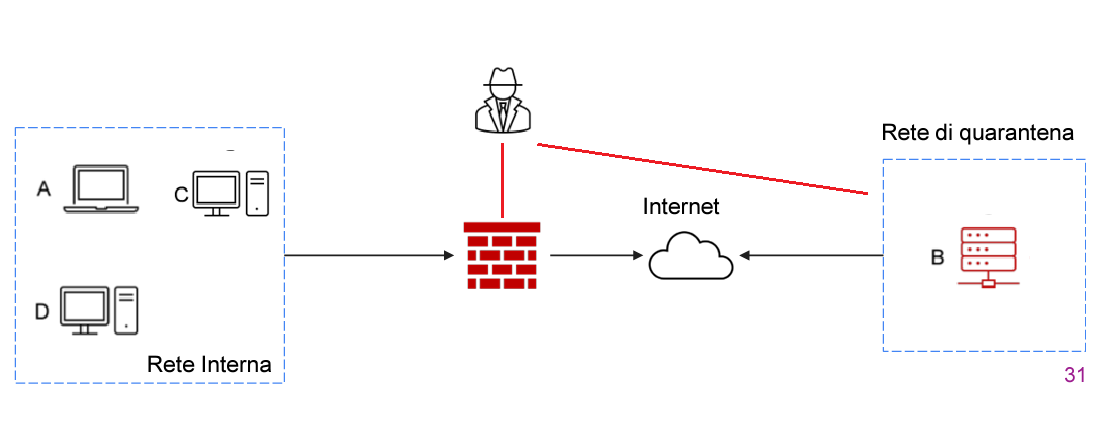
Quindi mentre Purge si concentra sulla *cancellazione sicura dei dati sensibili* senza danneggiare fisicamente il supporto di archiviazione, Destroy prevede la *distruzione fisica del supporto stesso* per garantire che i dati non siano più accessibili in alcun modo

**Rappresentazioni grafiche:**

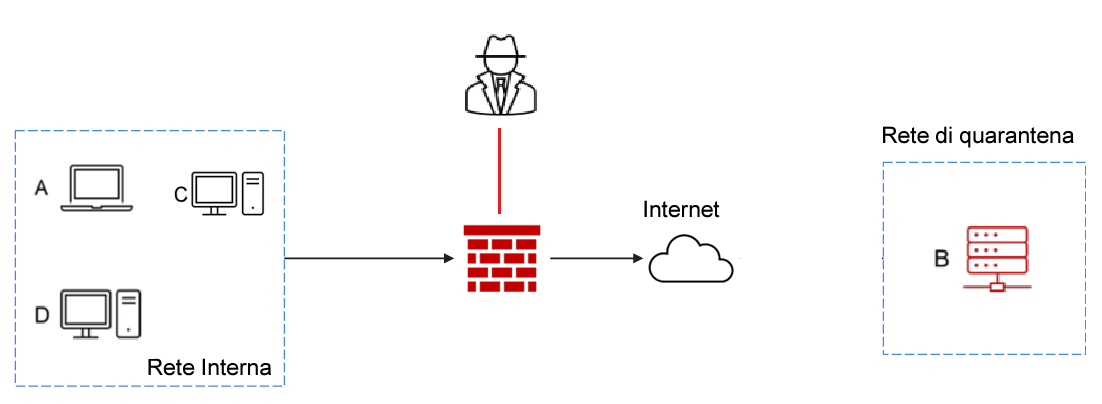
**Segmentazione:**

****

**Isolamento:**

****

**Rimozione:**

****