L4 Traccia

Con riferimento alla figura in slide 4, 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.

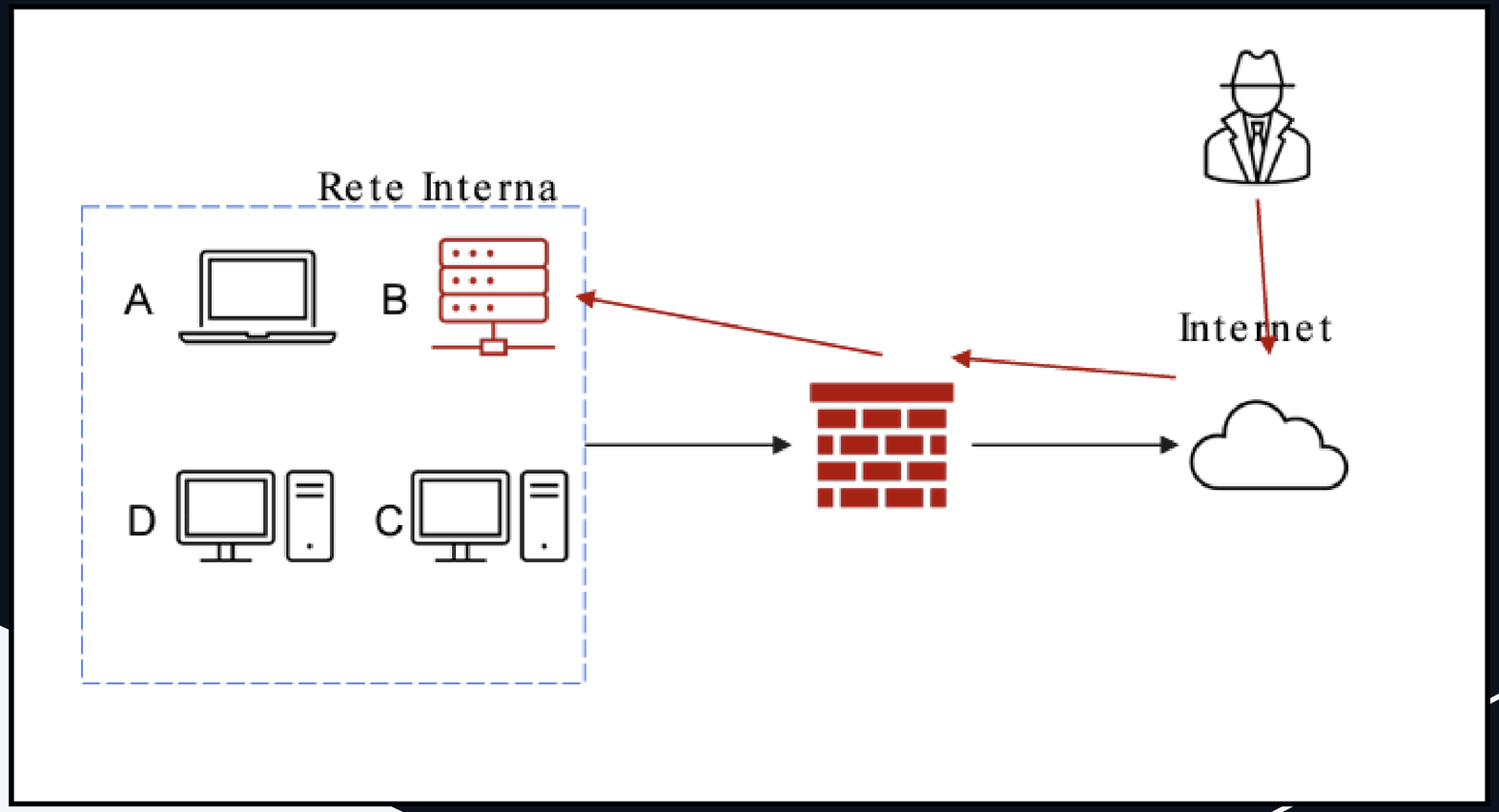
L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

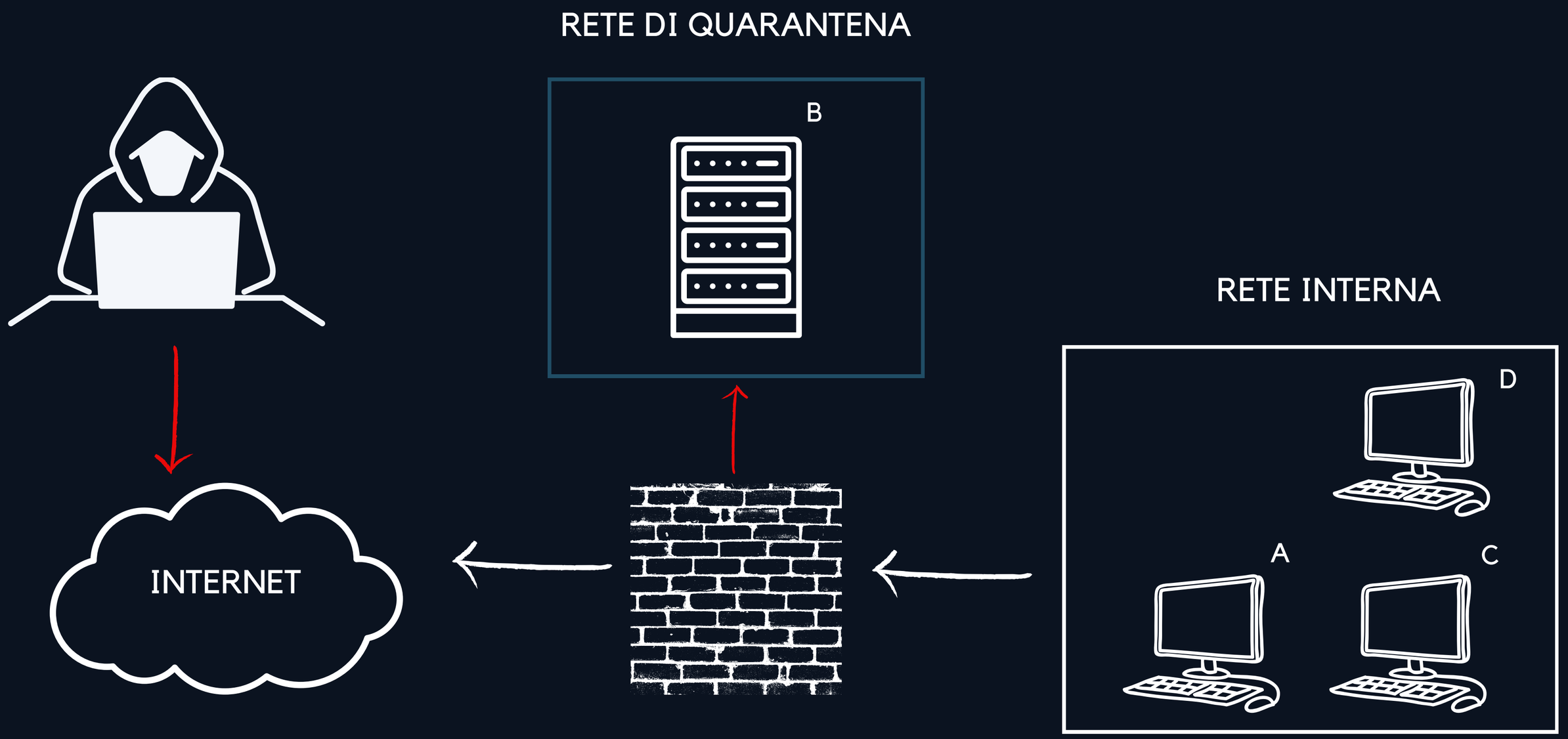
- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.

Indicare anche Clear

Immagine slide 4



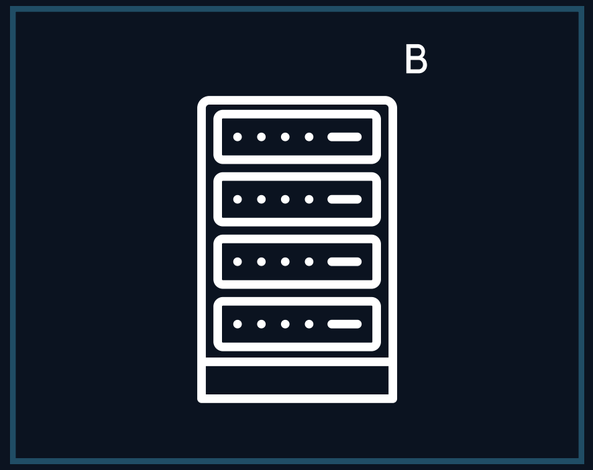
S9L1-5



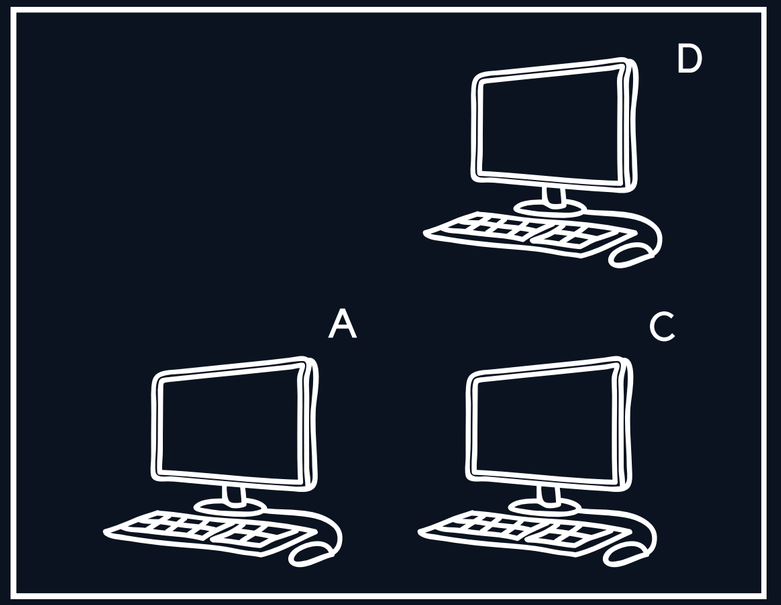
S9L1-5

ESEMPIO DI SOLAMENTO

RETE DI QUARANTENA



RETE INTERNA



S9L1-5

ESEMPIO DI RIMOZIONE

ISOLAMENTO

L'isolamento di un sistema infetto su una rete di quarantena implica scollegare il dispositivo infetto dalla rete principale e collegarlo a una rete separata per contenere la minaccia. L'attaccante in questo scenario ha comunque accesso al dispositivo infetto tramite internet. Questo processo prevede il rilevamento della minaccia, l'isolamento del dispositivo, l'analisi e la rimozione del malware, e il ripristino e reintegrazione del dispositivo nella rete principale solo quando è sicuro. L'obiettivo è prevenire la diffusione della minaccia e proteggere l'integrità dell'intera rete.

RIMOZIONE

A volte l'isolamento non basta a contenere la minaccia, e ci avvale quindi della tecnica di rimozione. Questa elimina completamente il sistema dalla rete, rendendolo inaccessibile sia da rete interna che da internet. Questo approccio fa si che l'attaccante che non abbia più accesso nemmeno al sistema infetto. Anche in questo caso si passerà poi alla rimozione del malware e ripristino del dispositivo

S9L1-5

Durante la fase di recupero di un sistema compromesso, la gestione dei media contenenti informazioni sensibili è cruciale per garantire che i dati non siano recuperabili. Le opzioni principali sono:

1. Clear:

Il dispositivo viene completamente ripulito dal suo contenuto utilizzando tecniche "logiche" attraverso la sovrascrittura ripetuta dei dati con tecniche di read and write o utilizzo della funzione di "factory reset" per riportare il dispositivo allo stato iniziale.

2. Purge:

Si tratta di una vera e propria tecnica di rimozione fisica attraverso l' utilizzo di forti magneti per rendere le informazioni inaccessibili, combinato con la sovrascrittura logica.

3. Destroy:

Si tratta di un approccio più drastico e definitivo per lo smaltimento di dispositivi con dati sensibili. che si avvale di tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature e perforazione. Questi metodi garantiscono che le informazioni siano completamente inaccessibili, ma comportano un costo economico maggiore.

Quando un attacco è in corso su una rete interna e un sistema compromesso), il team di CSIRT (Computer Security Incident Response Team) deve agire rapidamente per mitigare i danni e ripristinare la sicurezza della rete.

S9L1-5

Contenimento

Nel caso dell' esempio riportato sopra, per prima cosa, è fondamentale contenere l'attacco immediatamente. Questo comporta l'isolamento del sistema B dalla rete per impedire all'attaccante di continuare ad accedere e diffondere la minaccia. Questo può essere fatto disconnettendo fisicamente il cavo di rete o modificando le regole del firewall per bloccare l'accesso. Inoltre, è importante proteggere i sistemi A, C e D, verificando se l'attacco si è esteso a questi dispositivi e isolandoli se necessario.

Analisi incidente.

Prima di eseguire qualsiasi azione di pulizia, è essenziale raccogliere tutte le prove possibili, come log di accesso, tracce di rete e snapshot del sistema, che saranno utili per l'analisi forense.
Identificare la vulnerabilità che ha permesso all'attaccante di compromettere il sistema B è cruciale; questo può includere l'analisi delle vulnerabilità di software, configurazioni errate o l'uso di credenziali compromesse.

S9L1-5

Comunicazione e Contromisure

La comunicazione è un altro aspetto fondamentale.
È necessario informare immediatamente tutti gli stakeholder rilevanti, inclusi gli amministratori di sistema, il management e il personale della sicurezza.

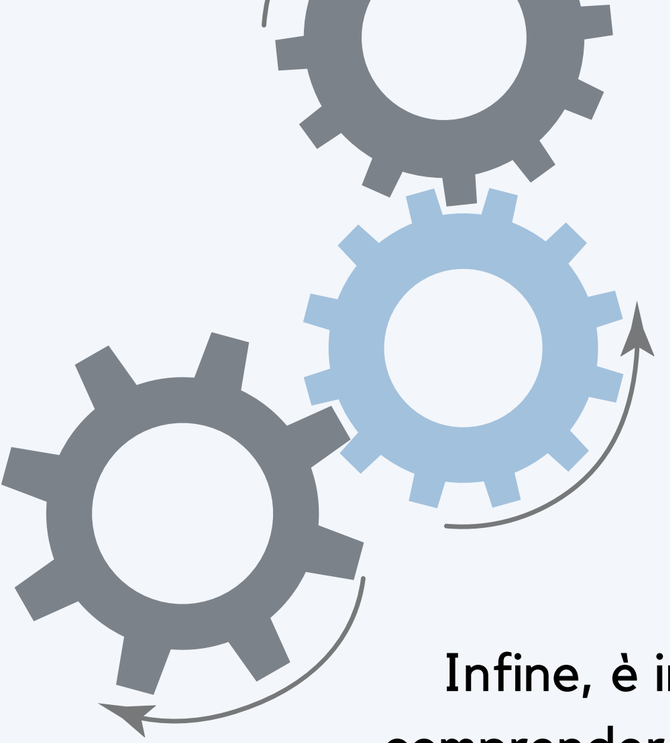
Per quanto riguarda le contromisure tecniche, è essenziale assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza e cambiare tutte le credenziali di accesso ai sistemi compromessi e a quelli potenzialmente affetti.

Rimozione

Una volta raccolte tutte le prove necessarie, si può procedere con la rimozione della minaccia. Questo implica una pulizia approfondita del sistema B, che potrebbe includere la reinstallazione del sistema operativo e del software applicativo. È anche necessario verificare l'integrità dei backup per assicurarsi che non siano stati compromessi e siano disponibili per il ripristino.

Ripristino

Il ripristino del sistema comporta la rimessa in sicurezza del sistema B e il ripristino dei dati dai backup sicuri.
Prima di rimettere il sistema in produzione, è essenziale eseguire test di penetrazione e verifiche di sicurezza per assicurarsi che il sistema sia sicuro.



Post-Incident

Infine, è importante eseguire una revisione dettagliata dell'incidente per comprendere cosa è successo, come è successo e cosa può essere migliorato. Aggiornare le procedure di sicurezza e di risposta agli incidenti in base alle lezioni apprese assicura che il team di CSIRT sia meglio preparato per affrontare futuri incidenti.