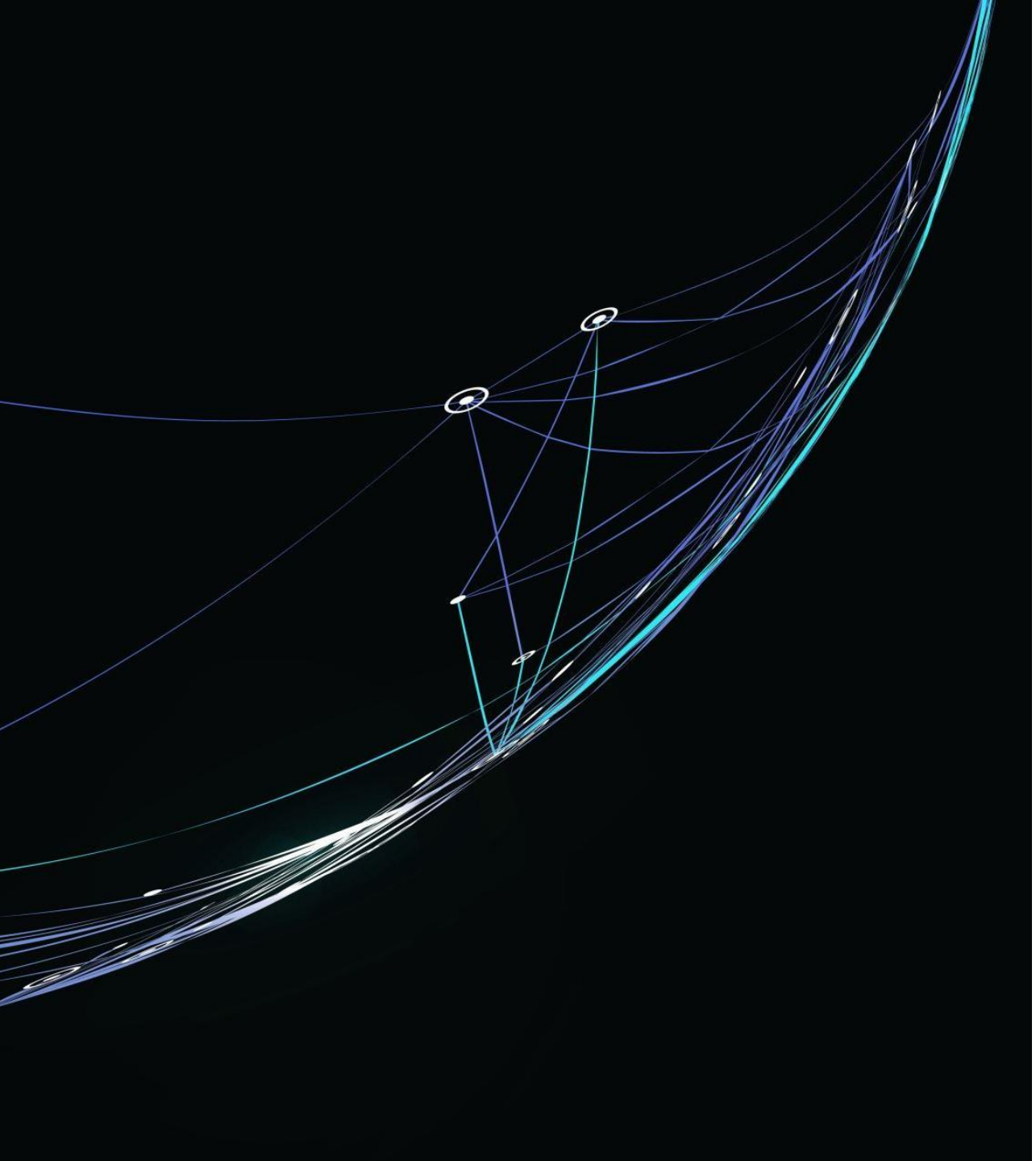


Incident response

Pablo Andres Balbuena Rios

Esercizio 4 Settimana 9

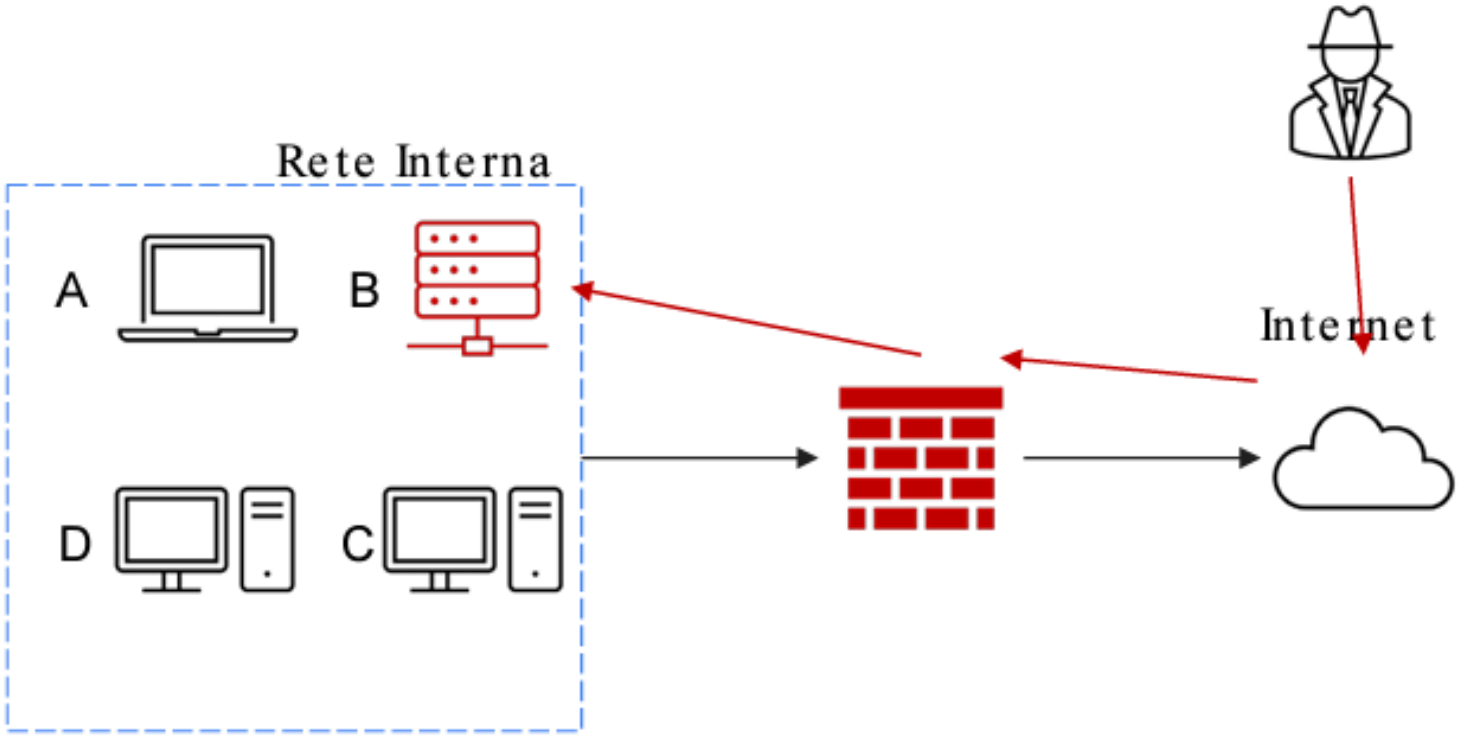
Con riferimento al modello, il Database è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

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

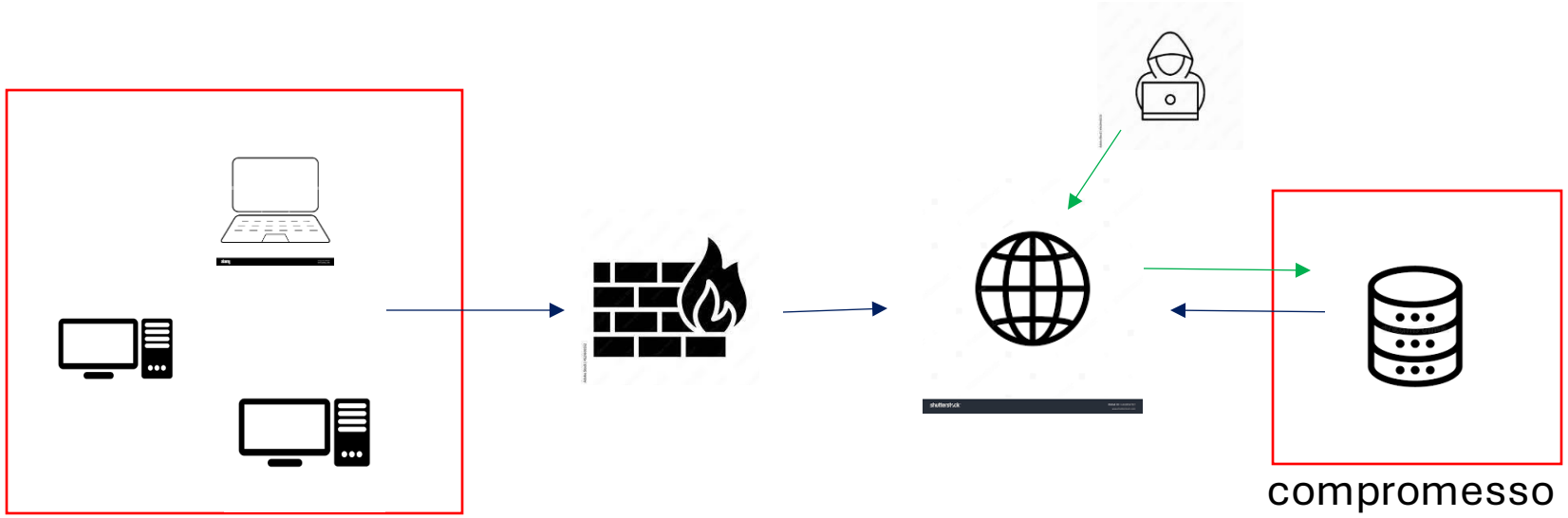
Modello



Tecniche di Isolamento-Rimozione

Tecnica di Isolamento:

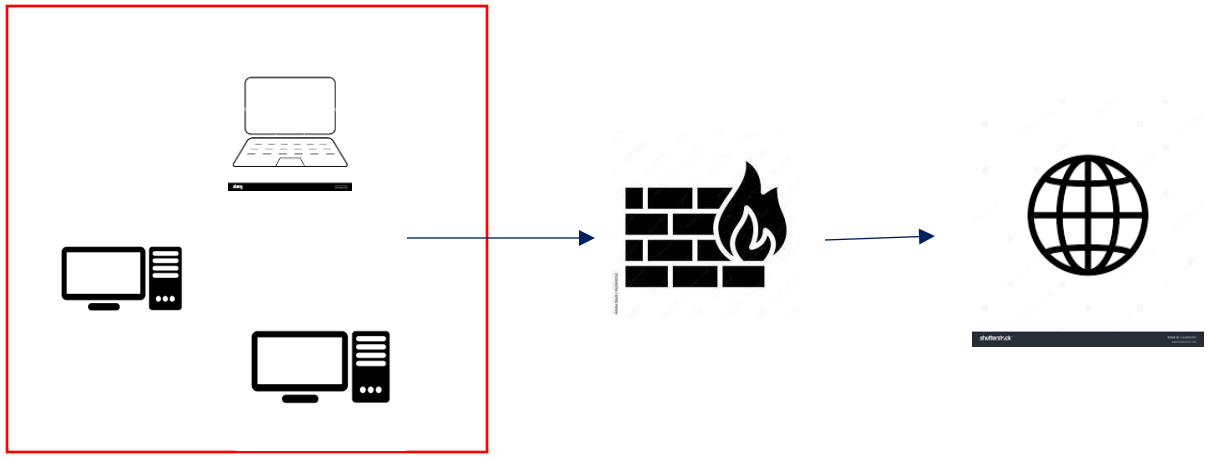
- La tecnica di isolamento consiste nel separare o limitare l'accesso a determinati elementi o sistemi, riducendo la diffusione di rischi o danni non desiderati. Disconnettendo il sistema infetto dalla rete ma non dalla connessione internet.



Tecniche di Isolamento-Rimozione

Tecnica di Rimozione:

- Questo approccio può essere utilizzato per garantire la sicurezza, la privacy o la gestione di rischi, a differenza dell'isolamento che mira a separare senza necessariamente togliere completamente la connessione ad internet.



compromesso

Gestione dei media contenenti informazioni sensibili

Il termine "Clear": si riferisce alla cancellazione di informazioni da un dispositivo o sistema. Indica solitamente la rimozione di dati o file, senza implicare necessariamente la distruzione irreversibile come nel caso di "Destroy".

"Clear" può comprendere procedure che liberano spazio o ripristinano un dispositivo alle impostazioni predefinite senza garantire la completa irrecuperabilità delle informazioni.

Gestione dei media contenenti informazioni sensibili

L'approccio Purge: non solo gestisce emotivamente contenuti sensibili, come nel caso di Clear, ma include anche tecniche fisiche, come l'uso di forti campi magnetici, per rendere inaccessibili le informazioni su determinati dispositivi. In breve, combina aspetti logici ed emotivi con azioni fisiche per garantire la sicurezza e la privacy delle informazioni.

Gestione dei media contenenti informazioni sensibili

Il termine "Destroy": implica un'azione più radicale rispetto a "Purge".

Mentre "Purge" potrebbe indicare la rimozione o la cancellazione di informazioni, "Destroy" suggerisce una distruzione completa o irreversibile. Questo può includere l'eliminazione fisica di dispositivi o supporti di archiviazione, l'uso di procedure avanzate di sovrascrittura per rendere i dati irrecuperabili o l'adozione di altre misure drastiche per garantire la completa eliminazione delle informazioni.

In termini di sicurezza delle informazioni, "destroy" evidenzia un'azione più estrema e definitiva nel prevenire il recupero delle informazioni distrutte.