Consegna S9-L4

Incident response

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.

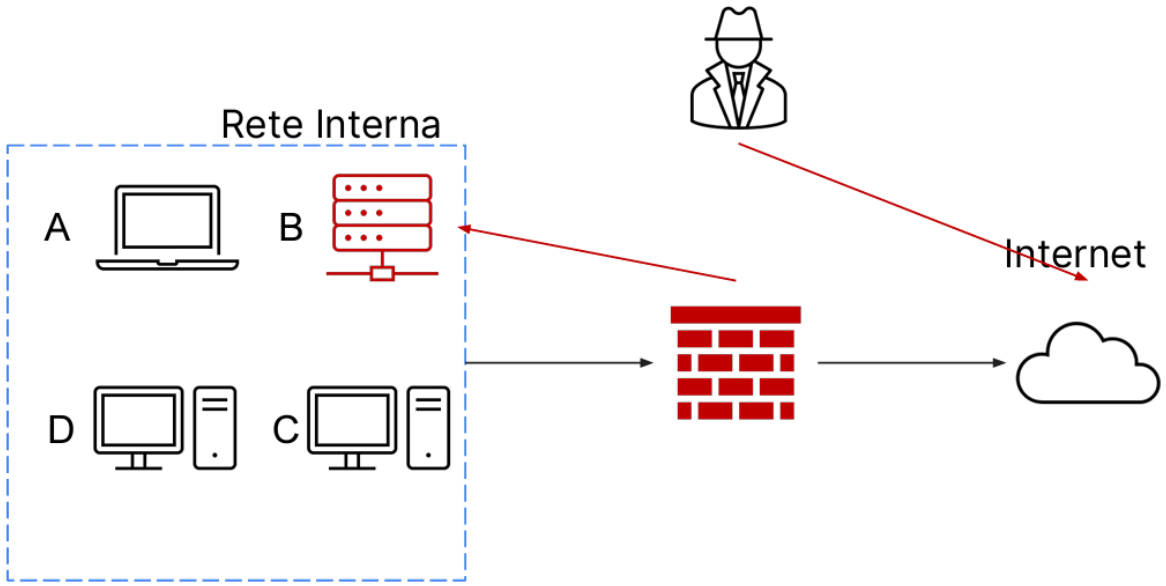
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

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

Traccia



Isolamento

Quando una parte della rete aziendale viene compromessa da un attacco esterno, è essenziale isolare immediatamente quella parte dal resto della rete. Questa azione mira a limitare la diffusione dell'attacco, proteggendo le altre parti della rete da eventuali danni. Pur mantenendo un collegamento con l'esterno, è possibile monitorare l'attività nell'area compromessa per identificare la fonte dell'attacco e adottare le misure necessarie per contrastarlo. In questo modo, si limita il rischio di compromettere ulteriormente la sicurezza dell'intera rete aziendale.

Rimozione

Quando una parte della rete aziendale è stata compromessa da un attacco esterno e la situazione richiede misure drastiche, si può optare per la rimozione completa del sistema dalla rete. Questo implica che il sistema compromesso venga completamente disconnesso dalla rete, rendendolo incapace di comunicare sia con l'esterno che con l'interno dell'azienda. Questa procedura estrema assicura in modo definitivo che il sistema compromesso non possa essere utilizzato come via d'accesso per ulteriori attacchi e garantisce la protezione dell'integrità della rete nel suo complesso.

Differenza tra Purge e Destroy

La distinzione tra "Purge" e "Destroy" è fondamentale quando si tratta di eliminare informazioni sensibili prima di disfarsi dei dischi compromessi. Il "Purge" implica una procedura di cancellazione sicura dei dati, dove le informazioni vengono sovrascritte con dati casuali o con zeri multiple volte. Questo processo mira a rendere le informazioni precedenti irrecuperabili, proteggendo così la riservatezza dei dati.

D'altra parte, "Destroy" comporta la distruzione fisica del disco, rendendolo completamente inutilizzabile. Questo può avvenire attraverso la demolizione del disco o attraverso metodi come la triturazione o la perforazione fisica. Questa azione garantisce che le informazioni non possano essere recuperate in alcun modo, offrendo un livello più elevato di sicurezza nella gestione dei dati sensibili.

Fine della presentazione

Amedeo Natalizi