Esercizio W20D1 - Incident Response

RICHIESTA

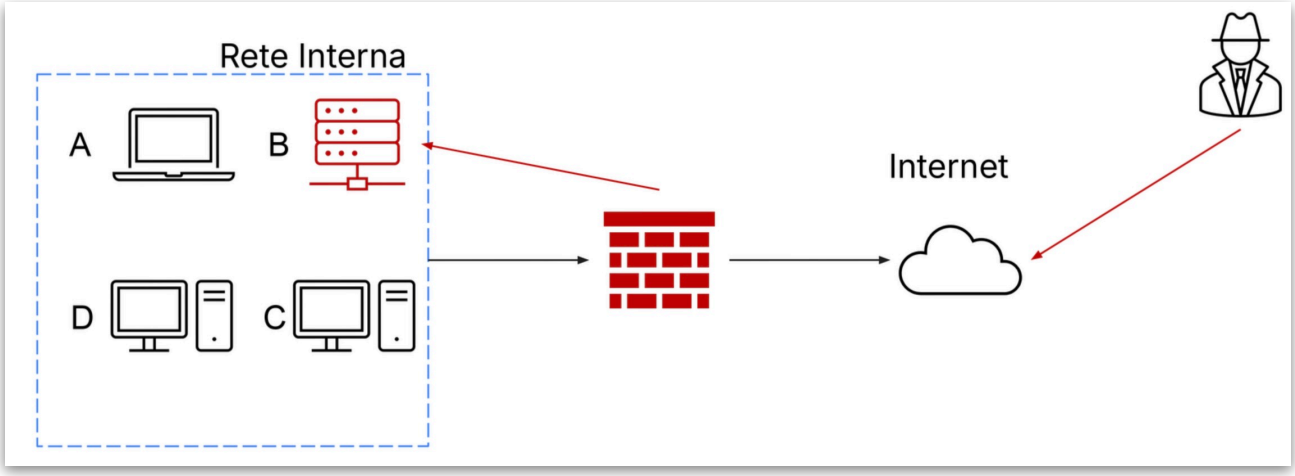
L'esercizio W20D1 ipotizza che, nella rete interna di un'azienda, un vecchio sistema con funzione di database e diversi dischi per lo storage sia stato compromesso da un attaccante. L'attacco è avvenuto via Internet, e ha colpito il sistema nella sua interezza.

L'allievo, che nella simulazione fa parte del team CSIRT, dovrà illustrare le necessarie tecniche di isolamento e rimozione del sistema infetto dalla rete. Successivamente dovrà illustrare le diverse tecniche di eliminazione e recupero delle periferiche infette.

~~~

SOLUZIONE

Nell'ambito dell'Incident Response, la prima fase è quella del **contenimento**. Questo vuol dire fermare la diffusione dell'attacco e limitare i danni. Il primo passo in tal senso è quello di disconnettere completamente il sistema infetto, sia dalla rete interna dell'azienda che da Internet.

Nel caso in oggetto, opterei per porre il sistema infetto in una **rete di quarantena**, cioè un ambiente altamente controllato e monitorato. In questo modo è possibile contenere l'attacco e, nello stesso tempo, analizzare il sistema per la successiva fase di ripristino dell'operatività.

La fase successiva prevede **l'eradicazione completa della minaccia**, cancellando completamente i dati presenti sui diversi dischi o, nella peggiore delle ipotesi, rendendo i dischi inutilizzabili. Fa parte di questa fase anche la ricostruzione del sistema, con il riutilizzo o la sostituzione dei dischi, l'installazione di sistema operativo e app e l'eventuale ripristino dei dati tramite backup.

A chiudere la fase di Incident Response c'è poi **la fase post-incident**, in cui il team CSIRT analizza tutte le dinamiche relative all'incidente di sicurezza e studia come migliorare le politiche di sicurezza in previsione di un possibile futuro attacco.

~~~

RAPPRESENTAZIONE GRAFICA

Nell'immagine successiva, la rappresentazione grafica della rete interna dell'azienda al momento dell'attacco



DETTAGLI TECNICI

Come anticipato all'interno del capitolo "Soluzione", il primo passo che il team CSIRT dovrebbe intraprendere, in questa situazione, è quella dell'**isolamento completo del sistema compromesso**. Sostanzialmente, sono tre le opzioni percorribili:

- La disconnessione fisica, tramite distacco del cavo di rete o disabilitazione della rete Wi-Fi del sistema infetto
- L'isolamento logico, tramite posizionamento della macchina in una rete di quarantena strettamente sorvegliata
- L'isolamento tramite firewall, tramite regole del firewall che blocchino completamente il traffico della macchina compromessa, sia in entrata e in uscita

Nella situazione ipotizzata dall'esercizio, avrei scelto il posizionamento della macchina in una rete di quarantena. Rispetto alla disconnessione fisica della macchina, infatti, l'utilizzo di una rete di quarantena strettamente controllata permette ai tecnici del CSIRT di accedere al sistema compromesso in remoto e attuare le necessarie operazioni per il ripristino.

La seconda fase è quella dell'**eradicazione completa della minaccia**. La tecnica più comune e consigliata per l'eliminazione completa della minaccia è quella del **Rebuilding**, che prevede l'intera ricostruzione di un sistema compromesso. La tecnica garantisce che qualsiasi malware, backdoor o alterazione fatta dall'attaccante sia completamente rimossa.

Prima di partire con il Rebuilding - che cancellerà completamente i dati presenti sui diversi dischi o, nella peggiore delle ipotesi, renderà gli stessi inutilizzabili - è fondamentale creare **un'immagine forense** dei vari dischi del sistema. Questo agevola l'analisi forense, la conservazione delle prove e altre eventuali analisi.

Un aspetto cruciale del Rebuilding è la **sanificazione dei dati.** Si parla di quel processo che assicura la completa e irrecuperabile eliminazione delle informazioni dai supporti di memorizzazione, sia in fase di dismissione che in risposta, come nel nostro caso, a un incidente di sicurezza.

Sono tre i differenti approcci per la sanificazione dei dati, che illustrerò in maniera più dettagliata nel capitolo "Differenze fra Clear, Purge e Destroy". Ecco una panoramica:

- L'approccio **Clear** prevede la sovrascrittura dei dati del disco con un pattern specifico, così da rendere i dati originali irrecuperabili. Il disco può essere riutilizzato
- L'approccio **Purge** è più robusto rispetto al Clear, e rende i dati originali irrecuperabili anche con tecniche di laboratorio. Fra le varie tecniche abbiamo la sovrascrittura avanzata e la **smagnetizzazione**, che consiste nell'esporre il supporto a un forte campo magnetico per azzerare la polarità magnetica di tutti i settori
- L'approccio Destroy è quello più radicale, e prevede la distruzione irreversibile del supporto di memorizzazione stesso. Fra le varie tecniche, le più utilizzate sono la frantumazione e la perforazione

Una volta conclusa la fase di sanificazione dei dati, e indipendentemente dal fatto che i dischi siano riutilizzabili o da sostituire, la procedura di Rebuilding prevede **l'installazione del sistema operativo**. Le procedure di sicurezza prevedono che il SO sia scaricato direttamente dal sito ufficiale del produttore su un PC pulito, e poi installato tramite supporto di memorizzazione sul sistema precedentemente infetto.

Una volta installato il sistema operativo, si passa alla fase di **ripristino da backup dei dati.** È necessario però controllare che i dati di backup non siano stati, a loro volta, compromessi dall'attaccante. Esistono varie tecniche o accortezze per essere sicuri che i dati non siano compromessi. Fra queste cito:

- L'utilizzo di un backup creato prima dell'inizio dell'attacco (Punto Pulito)
- La scansione del backup dei dati con un antivirus e un antimalware
- La verifica dell'hash crittografico del backup in modo da garantire l'integrità dei dati
- La verifica della dimensione e del conteggio dei file compresi nel backup

Giunti a questo punto, l'operatività del sistema è stata ristabilita. A chiudere la fase di gestione dell'incidente c'è la fase di **post-incident**: il team CSIRT deve eseguire infatti un'analisi approfondita di tutte le dinamiche dell'incidente, dal rilevamento all'eradicazione. Lo scopo è quello di ricostruire l'incidente, identificare le aree di miglioramento e rafforzando le politiche di sicurezza al fine di prevenire futuri attacchi simili.

~~~

DIFFERENZE FRA CLEAR, PURGE E DESTROY

Come visto in precedenza, nell'ambito della sanificazione dei dati sono tre gli approcci: Clear, Purge e Destroy. Prima di illustrare le differenze fra i tre diversi metodi, giova ricordare però che, specialmente per le aziende che trattano dati sensibili o che operano in settori regolamentati, la scelta del tipo di approccio non è libera ma è **vincolata a stringenti normative o leggi** (ad esempio il GDPR dell'Unione Europea).

Andando a guardare i tre approcci nello specifico, il Clear è quello meno radicale. Prevede **la cancellazione logica dei dati**, attraverso la sovrascrittura di quest'ultimi con un pattern prestabilito (solitamente tutti 0). I dati originali sono irrecuperabili tramite strumenti software o comuni strumenti hardware. Potrebbero essere recuperati, però, tramite tecniche di laboratorio. Un hard disk sanificato con metodo Clear può essere tranquillamente riutilizzato.

L'approccio Purge è più robusto del Clear. Esistono diverse tecniche di Purge: le più utilizzate sono la sovrascrittura avanzata (molteplici passaggi di sovrascrittura con pattern complessi) e **la smagnetizzazione**, che prevede l'esposizione del supporto a un forte campo magnetico così da azzerare la polarità magnetica di tutti i settori e cancellare totalmente i dati. A differenza del Clear, i dati di un hard disk sottoposto a sanificazione con Purge non sono più recuperabili, nemmeno in laboratorio. L'hard disk non può però essere riutilizzato, e va sostituito.

L'approccio più radicale alla sanificazione dei dati è il Destroy che, come lascia intendere il nome, prevede **la distruzione fisica** del supporto di memoria. I metodi di distruzione di un hard disk sono molteplici, e fra questi abbiamo la **frantumazione** (riduce l'hard disk in piccoli frammenti), la **perforazione** (buca ogni piatto dell'hard disk con un apposito strumento), l'incenerimento e la polverizzazione. L'approccio Destroy offre l'assoluta certezza che i dati originali non siano più recuperabili ma, chiaramente, il vecchio hard disk non può più essere riutilizzato.
~~~