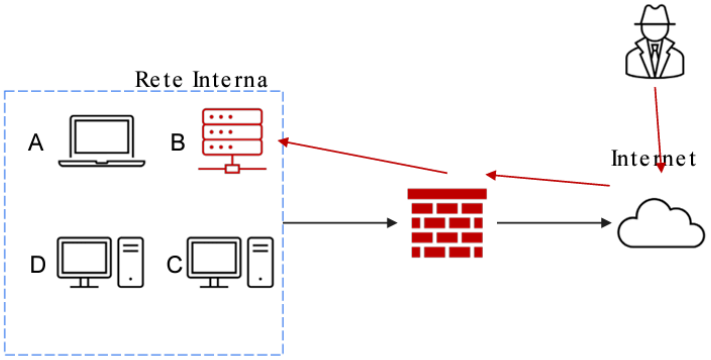
S9/L4

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.



In presenza di un incidente di sicurezza, il CSIRT deve essere in grado di rispondere in modo tempestivo. Ci troviamo nella terza fase del piano di risposta, ovvero quello del contenimento del danno. Lo scopo primario è quello di isolare l'incidente in modo tale da non creare ulteriori danni al sistema.

In questo caso l'attaccante riesce tramite internet, ad accedere ad un database aziendale collegato alla rete interna dove vi sono connessi anche tutti gli altri dispositivi in quanto non è stata attuata nessuna azione preventiva come la segmentazione di rete.
Dato che l'attacco è già in corso, la prima cosa da fare è l'isolamento, ovvero la disattivazione della connessione di rete:

- Interrompiamo la connessione di rete del Sistema B per limitare la diffusione dell'attacco ad altri sistemi. Eliminiamo così l'attaccante dalla rete aziendale, il quale però ha ancora accesso al sistema tramite internet.
- Se il database B è distribuito su più server, possiamo isolare il server o il nodo compromesso per evitare la compromissione degli altri componenti del sistema.
- Ridurre al minimo i servizi e le funzionalità attive sul database B per limitare le potenziali vie di attacco e ridurre la superficie di attacco.

Se invece vogliamo una tecnica di contenimento più restringente, possiamo optare per la rimozione completa dei sistema infetto sia dalla rete interna, sia dalla rete internet, in modo tale da negare l'accesso in modo totale all'attaccante.

Si passa poi alla fase di rimozione dell'incidente, le tecniche di rimozione dipendono molto dal tipo di attacco, infatti è buona prassi avere una lista con le attività da seguire divise per macro-casistiche chiamate playbooks.
Nella fase di rimozione e recupero, possiamo:

- isolare e pulire i dischi rigidi infetti per evitare la propagazione dell'attacco ad altri dispositivi,
- eliminare eventuali backdoor installate da un malware,
- formattare i dischi rigidi del Sistema B compromesso e reinstallare il sistema operativo,
- aggiornamenti e patching, ovvero l'applicazione di tutti gli aggiornamenti di sicurezza e le patch disponibili per mitigare le vulnerabilità che hanno permesso all'attaccante di compromettere il Sistema B.
- Verificare e aggiornare le regole di sicurezza e le politiche di accesso per garantire che il database B sia adeguatamente protetto e che solo gli utenti autorizzati possano accedervi.

Durante la fase di recupero, ci si trova spesso a dover gestire lo smaltimento o il riutilizzo di un disco. In questo caso, per prima cosa dobbiamo essere sicuri che tutte le informazioni presenti sul dispositivo siano cancellate e inaccessibili.
Possiamo individuare tre opzioni:

- Clear: il dispositivo viene ripulito tramite tecniche logiche e operazioni a livello software, indica l'azione di eliminare dati specifici/file da un sistema o da un dispositivo. Può anche riferirsi all'azione di eliminare o cancellare i log di sistema o di sicurezza, per eliminare tracce di attività o di accesso indesiderate o per liberare spazio su disco. In sintesi il dispositivo viene pulito (tramite la sovrascrittura di dati) e riportato alle impostazioni di fabbrica. Utilizzando "clear", potremmo però non arrivare ad una cancellazione irreversibile dei dati come invece avviene con "purge" e "destroy".
- Purge: è un intervento a livello fisico/hardware, l'azione di eliminare o cancellare definitivamente dati, file o risorse digitali da un sistema o da un dispositivo. Questo processo viene spesso eseguito per garantire che i dati sensibili non possano essere recuperati da terze parti non autorizzate. Di solito avviene tramite l'utilizzo di magneti, dispositivi utilizzati per eliminare definitivamente le informazioni memorizzate su supporti magnetici (come dischi rigidi), questi magneti sono particolarmente utilizzati in contesti in cui è necessario distruggere i dati in modo irreversibile in vista di informazione altamente sensibili.
- Destroy: implica un'azione più radicale rispetto alla semplice cancellazione dei dati. Indica l'azione di eliminare definitivamente un'intera risorsa digitale, un dispositivo, un server. Avviene attraverso tecniche di laboratorio, come la disintegrazione/trapanazione, l'eliminazione ad alte temperature. Sicuramente è il metodo più efficace ma anche quello più dispendioso economicamente.