Floriana Feminò

22/12/2022

INCIDENT RESPONSE

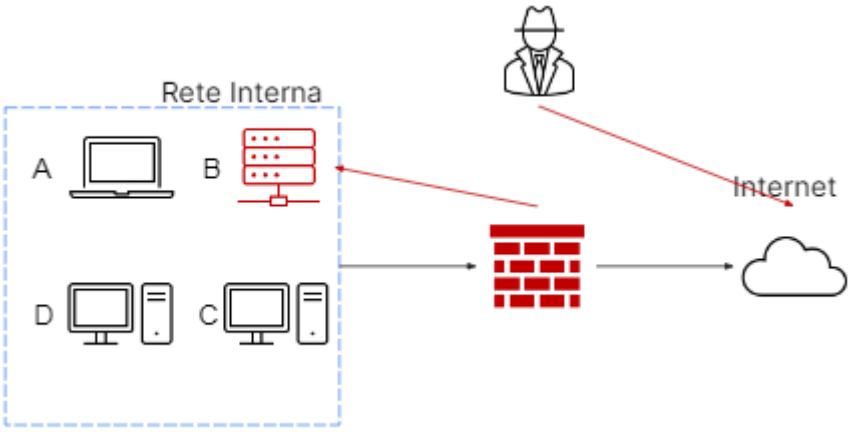
Tasks:

1. **Attuazione delle tecniche di segmentazione, isolamento e rimozione del sistema "B" infetto**
2. **Illustrazione delle metodologie di eliminazione delle informazioni sensibili presenti sui dischi compromessi destinati allo smaltimento**

---

1. Attuazione delle tecniche di segmentazione, isolamento e rimozione del sistema "B" infetto

Le attività odierne si focalizzano sulla gestione di un sistema "B" – costituito da un database contenente diversi dischi per lo storage – oggetto di compromissione da parte di un attaccante che è riuscito ad avervi accesso illecitamente, come illustrato nella figura sottostante:

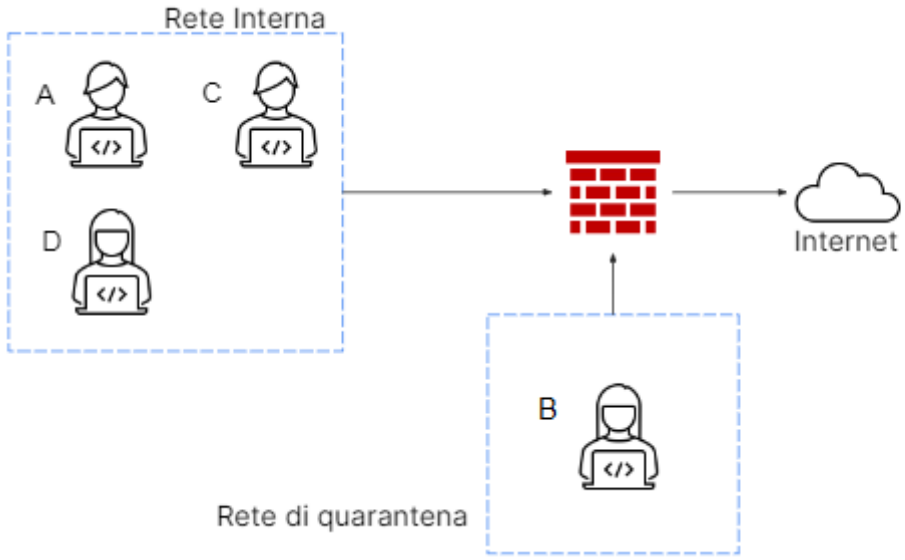


Il primo step della fase di incident response è il **contenimento del danno** causato dall'incidente di sicurezza, da effettuarsi nel minor tempo possibile onde evitare il propagarsi della minaccia su ulteriori sistemi, applicazioni e asset aziendali oltre quello/i già colpiti. La finalità di tale processo è isolare l'incidente – in modo da non creare ulteriori danni a reti/sistemi – riducendo dunque l'impatto causato dall'incidente. Le tecniche utilizzate a tale scopo sono:

- Segmentazione
- Isolamento
- Rimozione

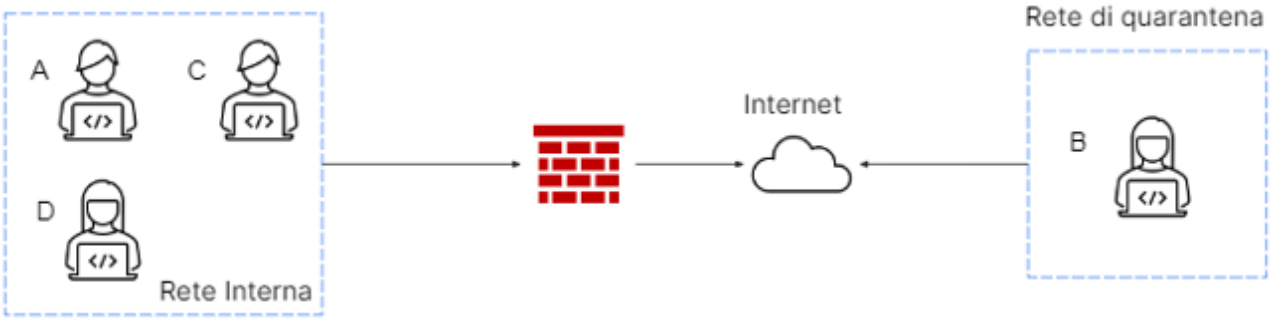
Segmentazione

La segmentazione include tutte quelle attività che permettono di suddividere una rete in diverse LAN o VLAN tramite subnetting. Questa tecnica permette dunque di separare il sistema "B" dagli altri computer sulla rete, creando una rete ad hoc generalmente definita "**rete di quarantena**". Con le dovute configurazioni a livello network, la minaccia viene contenuta e separata dal resto della rete interna; in caso di infezione da malware o codici malevoli di vario tipo, dunque, questi sarebbero incapaci di riprodursi e trasmettersi su ulteriori sistemi interni all'azienda.



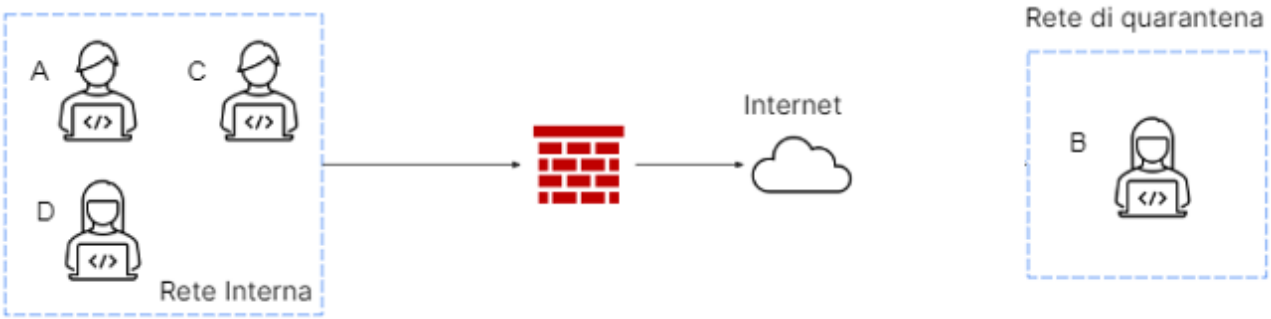
Isolamento

La segmentazione limita la riproduzione e diffusione di un malware o codice malevolo, tuttavia a volte non è sufficiente a far considerare conclusa la fase di contenimento. Quando è necessario un contenimento maggiore, si ricorre alla tecnica dell'**isolamento**: si effettua la **completa disconnessione** del sistema infetto dalla rete, allo scopo di restringere ancor più l'accesso alla rete interna da parte dell'attaccante. In questo scenario, l'attaccante ha ancora accesso al sistema "B" tramite la rete Internet: infatti, l'isolamento costituisce una tecnica spesso utilizzata per raccogliere più informazioni possibili circa l'attacco in corso (ad esempio tramite operazioni di monitoraggio del traffico di rete) e l'attaccante in questione senza mettere a repentaglio gli asset dell'intera compagnia.



Rimozione

In alcuni casi, la tecnica dell'isolamento si rivela non abbastanza efficace a contenere la minaccia in corso: in questi casi si ricorre alla tecnica della **rimozione**. Si tratta della metodologia di contenimento del danno più stringente, in quanto consiste nella **rimozione del sistema infettato sia dalla rete interna che dalla rete Internet**. Infatti, è bene sottolineare che in caso di creazione di una rete di quarantena, l'attaccante ha comunque accesso ad un sistema, ossia quello collegato sulla suddetta rete, attraverso la rete Internet. Adoperando la tecnica della rimozione, invece, l'attaccante non avrà più alcun accesso né alla rete interna né alla macchina infettata tramite Internet.



2. Illustrazione delle metodologie di eliminazione delle informazioni sensibili presenti sui dischi compromessi destinati allo smaltimento

Durante la fase di recupero dei servizi e delle operatività standard a valle di un incidente di sicurezza, non è raro dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un dispositivo compromesso. In questo caso è fondamentale accertarsi, in prima istanza, che le informazioni presenti sul disco/componente di storage siano completamente inaccessibili prima di smaltire o utilizzare nuovamente il disco.

Possiamo individuare tre metodologie di gestione dei media contenenti informazioni sensibili:

CLEAR

Il dispositivo viene completamente ripulito dal suo contenuto con tecniche **logiche**. Si utilizza ad esempio un approccio ***read and write***, in cui il contenuto viene sovrascritto più volte; in alternativa si può utilizzare la funzione di **factory reset** per riportare il dispositivo allo stato iniziale.

PURGE

In questo caso viene adottato non solo un approccio logico per la rimozione dei contenuti sensibili, ma anche metodologie di rimozione **fisica** dei dati presenti: è frequente l'utilizzo di **tecniche di smagnetizzazione** (ad esempio tramite degausser) che hanno la finalità di rendere le informazioni inaccessibili su determinati dispositivi.

DESTROY

Si tratta dell'approccio più radicale per lo smaltimento di dispositivi contenenti dati sensibili: oltre a meccanismi logici e fisici, vengono utilizzate tecniche di laboratorio come la **disintegrazione**, polverizzazione ad alte temperature e la foratura dei dischi. Questo metodo è senza dubbio il più efficace per rendere le informazioni inaccessibili, ma è anche quello che comporta un maggiore effort in termini economici.