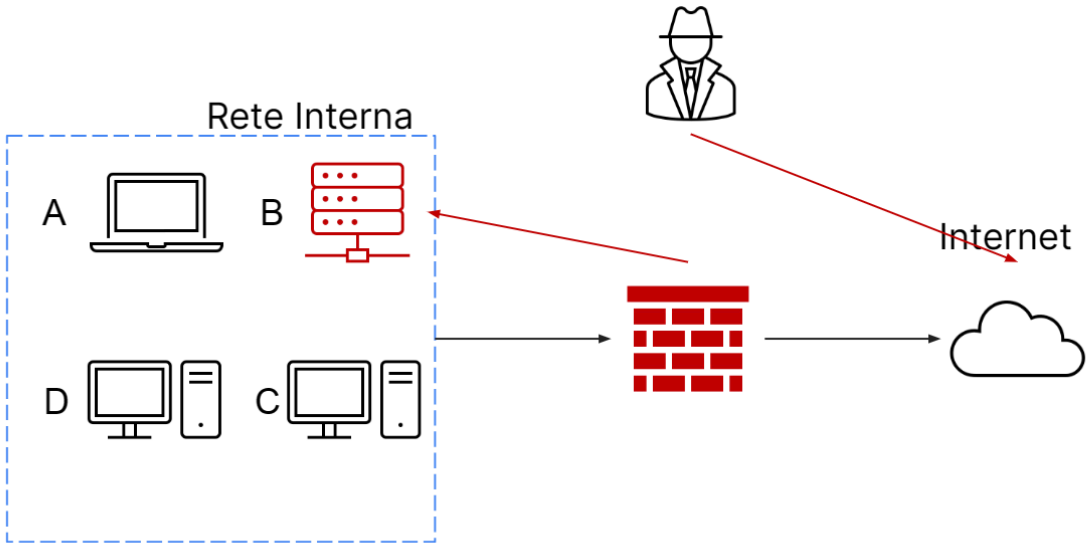
FASI IRP

Incident Response Plan(I)



TRACCIA

- - - - X

Con riferimento all'immagine in sovraimpressione, 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 ai sistemi 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

“

MOSTRARE LE TECNICHE DI ISOLAMENTO E RIMOZIONE DEL SISTEMA INFETTO

”

INTRODUZIONE.

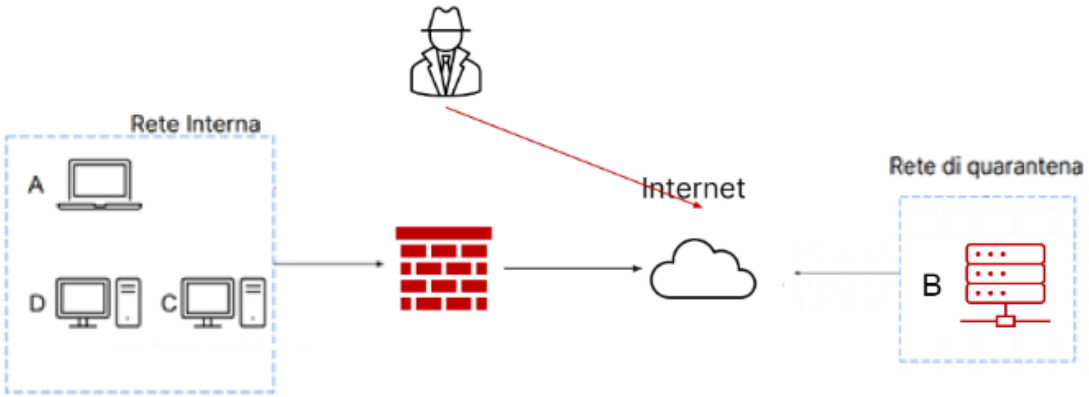
Una volta che il team CSIRT ha repentinamente rilevato ed analizzato l’origine dell’incidente, i sistemi implicati e potenziali rischi che tale incidente può apportare, deve altrettanto agire rapidamente per trovare una soluzione e ridurre al minimo gli impatti dell’incidente…

Inizia formalmente la fase di contenimento, eliminazione e recupero, e come si può evincere dal nome:

- riduzione degli impatti causati dall’incidente
- eliminazione dell’incidente dalla rete e dai sistemi
- recupero dei servizi e delle operatività standard.

Come nel nostro caso, nel caso in cui un computer su una rete, è stato infettato, la prima attività da fare per contenere gli impatti, è isolare il sistema, rispetto al resto della rete.

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza della rete, è la cosiddetta ‘segmentazione’ o ‘rete di quarantena’.



ISOLAMENTO

La segmentazione, include tutte quelle attività che permettono di separare una rete in diverse LAN o VLAN, in modo tale da separare il sistema infetto dagli altri computer sulla rete, creando una rete ad hoc, chiamato generalmente ‘rete di quarantena’. Nonostante la segmentazione riesca a limitare la riproduzione del sistema B infetto e l’accesso alla rete da parte dell’attaccante, spesso non è sufficiente per chiudere la fase di contenimento.

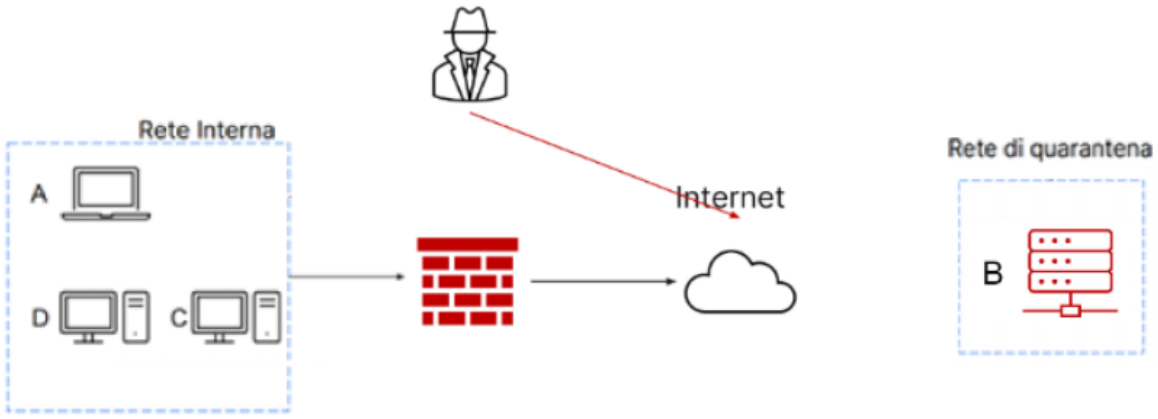
In questi casi, quando è necessario un contenimento maggiore, si utilizza la tecnica dell’isolamento. L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere maggiormente l’accesso alla rete interna da parte dell’attaccante. In questo scenario l’attaccante ha ancora accesso al sistema B tramite internet.

RIMOZIONE DEL SISTEMA B INFETTO

Ci sono ulteriori casi in cui l'isolamento non è abbastanza. In questi casi si procede con la tecnica di contenimento ancora più stringente, che comporta la completa rimozione del sistema dalla rete sia interna sia internet.

Un sistema infetto dalla rete CSIRT dovrebbe essere rimosso nel caso in cui il malware causi danni gravi o comprometta la sicurezza dei dati sensibili. Questa è una misura di emergenza per contenere la diffusione del malware e proteggere le altre risorse della rete. Tuttavia, prima di rimuovere il sistema, è importante segnalare l'incidente al CSIRT italiano, che ha il compito di monitorare, intercettare, analizzare e rispondere alle minacce cyber. Il CSIRT italiano offre anche una sezione dedicata sul suo sito per le comunicazioni volontarie di incidenti.

Per rimuovere il malware dal sistema infetto, è possibile seguire le istruzioni fornite da fonti affidabili, come il sito IONOS, che suggerisce di spegnere il dispositivo, cercare informazioni sul malware da un altro dispositivo e utilizzare un software antivirus o antimalware per eliminare il codice dannoso.
In quest'ultimo scenario, l'attaccante non avrà nè accesso alla rete interna né tantomeno alla macchina infetta

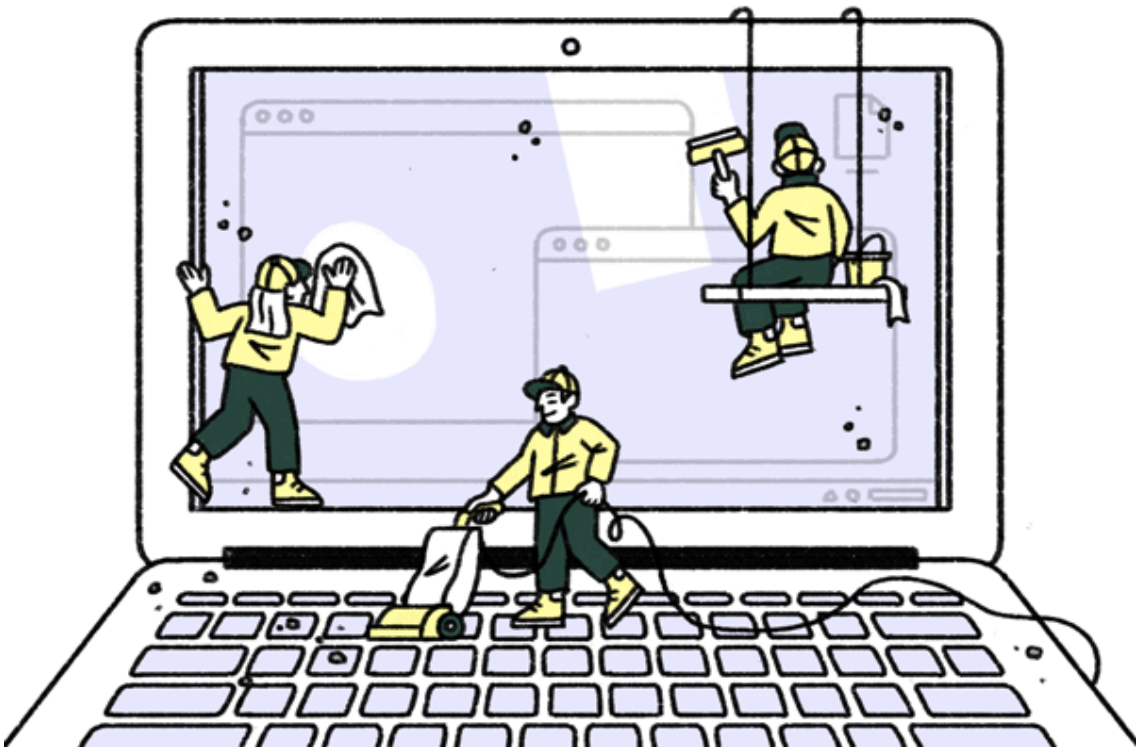


DIFFERENZA TRA PURGE E DESTROY:

Per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear

Durante la fasi di recupero, ci si ritrova a dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di una sistema compromesso. Bisognerà accertarsi in primo luogo, che le informazioni presenti sul disco siano completamente inaccessibili prima di smaltire/utilizzare nuovamente il disco.

Generalmente possiamo individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:



PURGE

Tradotto dall’inglese, significa ‘purificare’/’depurare’ e nel linguaggio informatico si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

DESTROY

Tradotto dall’inglese, significa ‘distruggere’ ed è quindi l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Si utilizzano meccanismi logici e fisici, ma anche tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperatura e trapanazione. Questo metodo risulta più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

CLEAR

Tradotto dall’inglese ‘pulire’. In questo caso il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche. Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di ‘factory reset’ per riportare il dispositivo nello stato iniziale.