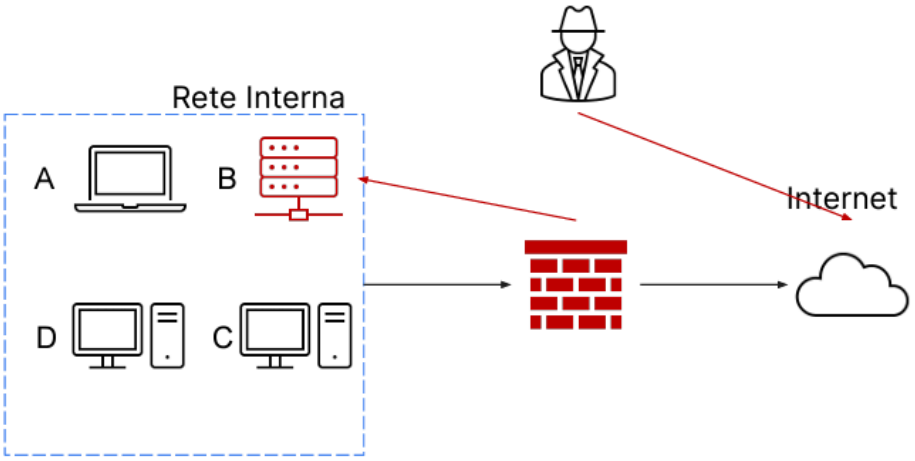

L’attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

- 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

La prima tecnica di isolamento per prevenire questo tipo di incidenti di sicurezza su una rete è la segmentazione, che include sia la segmentazione di tipo LAN e VLAN.
L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l’accesso alla rete interna da parte dell’attaccante.
I firewall sono dispositivi hardware o software che possono essere configurati per bloccare o consentire il traffico di rete in base a delle regole.
La rimozione del sistema B infetto si può fare in diversi modi, per esempio con la rimozione completa del sistema dalla rete internet, dall’utilizzo di software anti virus, formattazione e ripristino di sistema con anche la reinstallazione del sistema operativo.

Queste tecniche vengono utilizzate dopo essere sicuri che le informazioni sul dispositivo non siano accessibili a nessuno, dopo aver fatto ciò si utilizzano queste tecniche:

- Purge: 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: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.
- Clear: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;

La differenza tra purge e destroy sta nel fatto che il purge rimuove i contenuti con anche un approccio fisico, per esempio con l’utilizzo di magneti sul dispositivo dove sono salvati i

dati. Mentre destroy è un approccio molto più efficace perché riguarda la disintegrazione, quindi vengono bruciati e eliminati i dispositivi dove sono salvati i dati rendendoli inaccessibili, però richiedono un effort maggiore in termini economici rispetto al purge.