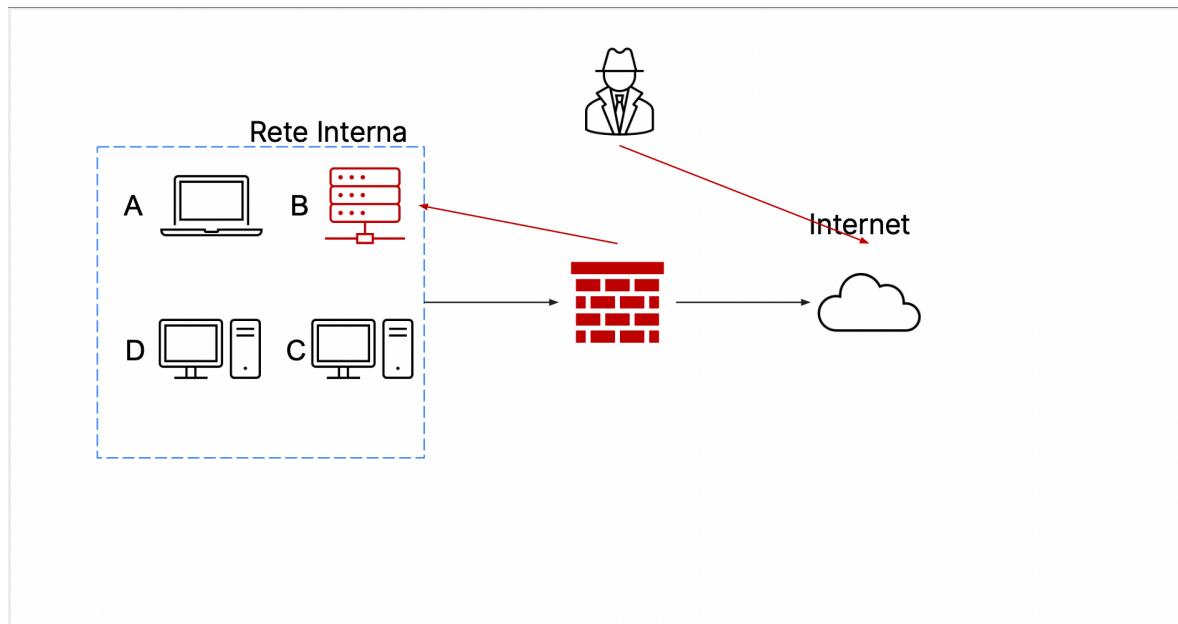


Incident response

TRACCIA:

È attualmente in corso un attacco e siamo parte del team CSIRT.
Come riportato in figura, 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.

1. Mostrare le tecniche di isolamento e rimozione del sistema infetto.
2. Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



Per ridurre gli impatti causati dall'incidente di questo attacco occorre contenere il danno causato dall'incidente di sicurezza, che deve iniziare quanto prima possibile. Terminata la fase di analisi, le attività di contenimento hanno lo scopo primario di

isolare l'incidente, in modo tale che non possa creare ulteriori danni a reti / sistemi. Ad esempio, se un computer o il server di una rete è stato infettato con un malware, come prima attività per contenere gli impatti è di isolare il sistema rispetto al resto della rete in modo tale che il malware non si riproduca su altri nodi.

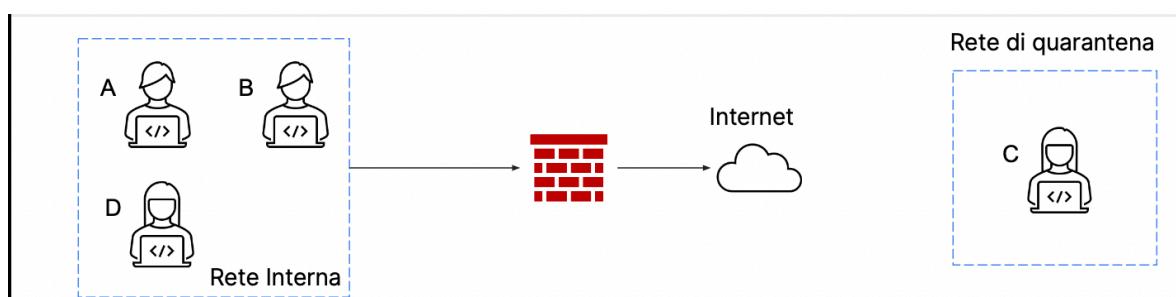
Una tecnica preventiva e strategica per la gestione degli incidenti di sicurezza sulla rete è la “segmentazione”, che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso.

La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN.

Infatti la segmentazione permette di separare il server dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata generalmente “rete di quarantena”.

Con le dovute configurazioni a livello network, il malware risulterebbe così separato dal resto della rete ed incapace di riprodursi.

Ci sono casi in cui l'isolamento non è abbastanza come tecnica di contenimento. A questo punto si procede alla completa rimozione del sistema dalla rete sia interna, sia internet.



A questo punto procede la fase di rimozione dell'incidente. In questa fase lo scopo è di eliminare tutte le attività, le componenti e i processi che sono rimasti all'interno della rete o sui sistemi.

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la fase di recupero.

La fase di recupero consiste nel ristabilire la normale operatività delle applicazioni e dei servizi. Include ad esempio il recupero dei dati e delle informazioni perse, l'applicazione delle patch dove disponibili per eventuali sistemi obsoleti, la revisione delle politiche dei firewall, IPS e IDS oppure l'aggiornamento delle firme degli antivirus.

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

-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

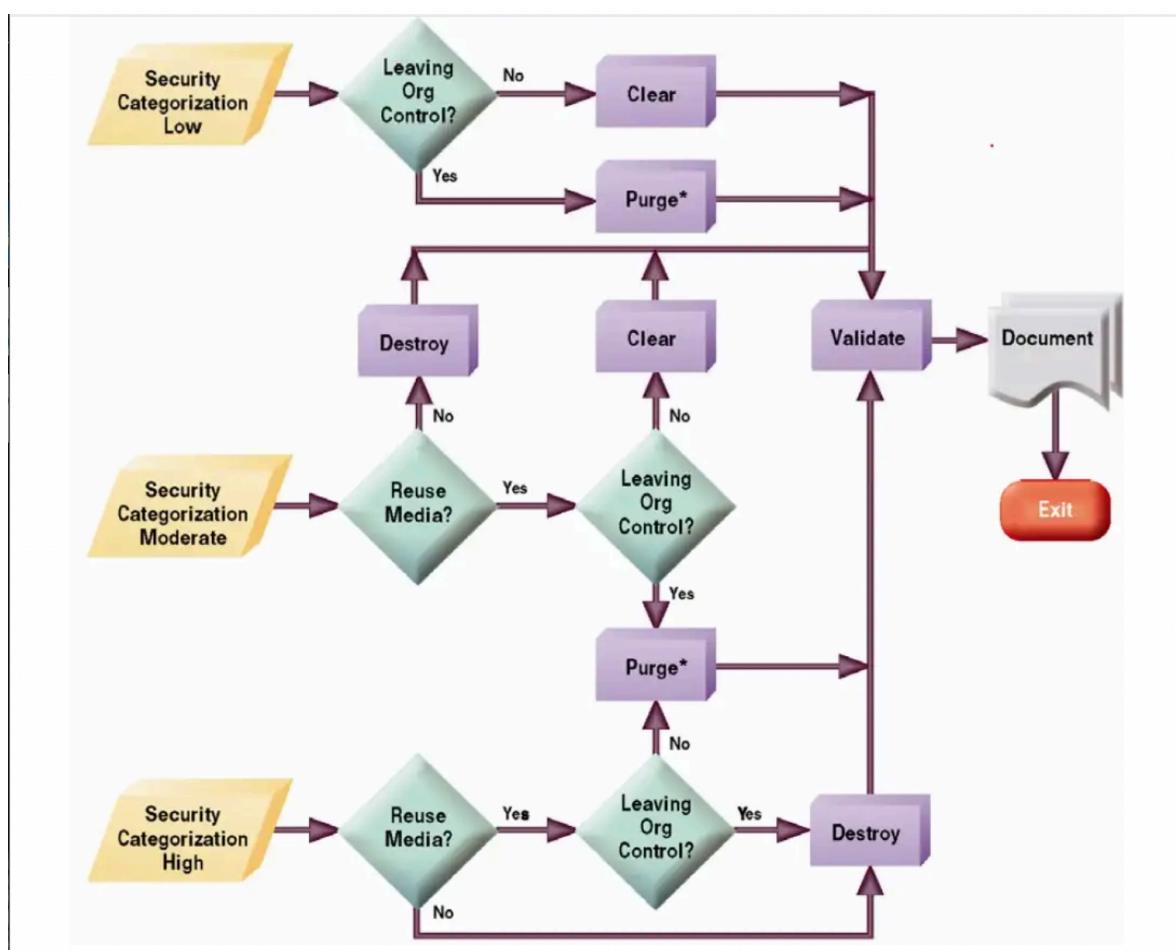
dispositivo nello stato iniziale

-Purge: è **eliminazione** delle informazioni e dei contenuti sensibili. Ma a differenza di *Clear*, utilizza tecniche di rimozione fisica come dei forti magneti che rendono inaccessibili i dati su determinati dispositivi. È un processo di **sanificazione** che protegge la riservatezza delle informazioni da un eventuale attacco.

Clear non garantisce la resistenza agli attacchi, mentre *purge* si. Come possiamo immaginare, *Clear* sarà un metodo relativamente più veloce o più economico. Non significa che non possiamo usare *Clear* perché non è sicuro, dipende dalla **classificazione dei dati**.

-Destroy: “La distruzione dei media è l'ultima forma di sanificazione. Dopo che i supporti sono stati distrutti, non possono essere riutilizzati come originariamente previsto. La distruzione fisica può essere realizzata utilizzando una varietà di metodi, tra cui la disintegrazione, l'incenerimento, la polverizzazione, la tritazione e la fusione”.

Qui sotto vi è riportato in figura un esempio di come questi protocolli vengono utilizzati a seconda dei casi.





GRAZIE

EPCODE