# REPORT INCIDENT RESPONSE

Preso in esame è un caso ipotetico di attacco in cui un utente malintenzionato sia riuscito a compromettere l'integrità di un sistema (database con diversi dischi per lo storage) , in questo caso riconosciuto come "sistema B", intromettendosi tramite internet.

Una volta rilevata una minaccia o potenziale tale, è il team CSIRT (Computer Security Incident Response Team) che ha il compito di intercettare, analizzare e rispondere alla minaccia tramite policy e procedure di incident response preventivamente pianificate in fase di preparazione .

Presupponendo un avvenuta categorizzazione del tipo di attacco e dell'impatto negativo che esso avrebbe sugli asset della compagnia in termini funzionali e monetari.

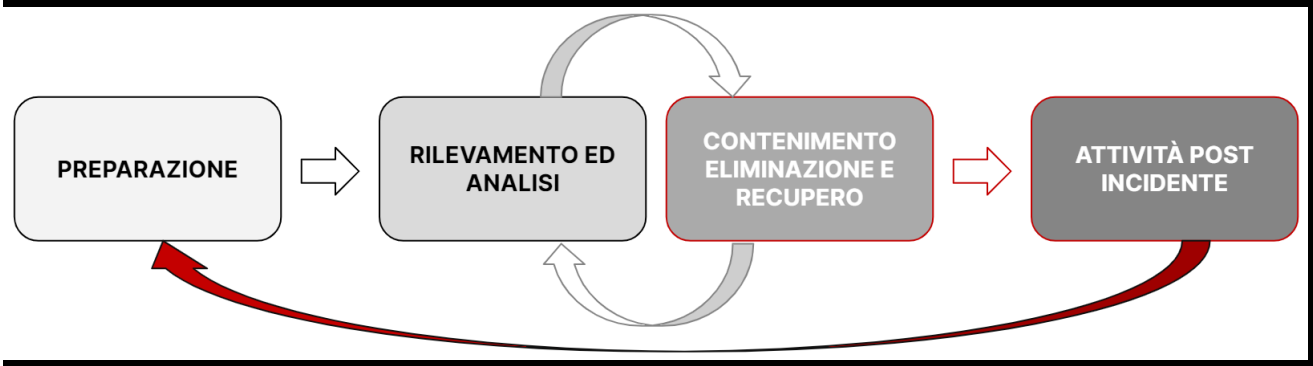
| CRITICITÀ | IMPATTO SUI SERVIZI (FUNZIONALE) | IMPATTO FINANZIARIO |
|---|---|---|
| NESSUNA | Nessun impatto sui servizi e sugli utenti. La compagnia riesce a fornisce tutti i servizi a tutti gli utenti | La compagnia non si aspetta nessuna perdita economica |
| BASSA | Minimo impatti su servizi ed utenti. Tutti i servizi critici erogati dalla compagnia sono attivi | La compagnia si aspetta un impatto economico limitato (e.g. 10.000€) |
| MEDIA | La compagnia non riesce ad erogare alcuni dei servizi critici o parte di essi ad un sottoinsieme limitato di utenti | La compagnia si aspetta un impatto economico non indifferente (e.g. 10.000 / 500.000€) |
| ALTA | La compagnia non riesce ad erogare servizi critici per tutti gli utenti | La compagnia si aspetta un grosso impatto economico (e.g. >500.000€) |

Essendo stato impattato un database con dischi di storage si potrebbe ipotizzare una criticità medio/bassa

Avendo definito i sistemi coinvolti e compromessi, ed aver stabilito un piano di contenimento che sia più rapido ed efficiente possibile, sarà opportuno effettuare un

“Eradication” dell’attaccante  in modo tale da evitare ulteriori danni o reazioni, ed una “Remediation” dell’incidente di sicurezza.

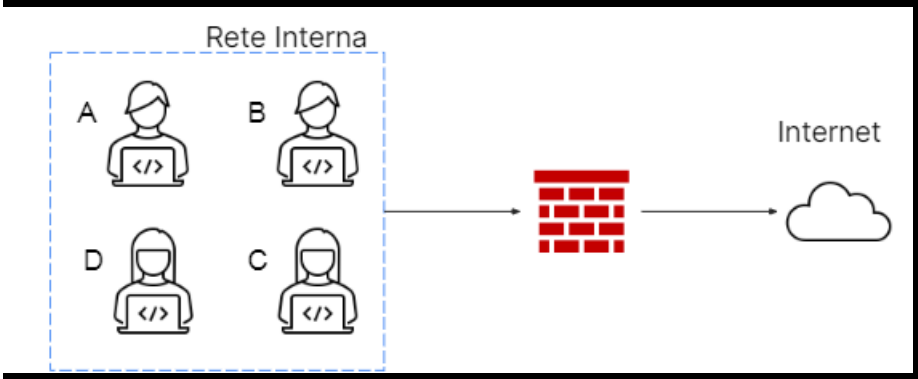
Lo step del processo di Incident response in cui il team si trova è quindi il terzo, definito “Contenimento/Eliminazione e recupero” (sebbene sia doveroso specificare che il processo non è lineare ma include loop e turn back per l’ottimizzazione di risposte future ad incidenti similari e/o uguali.

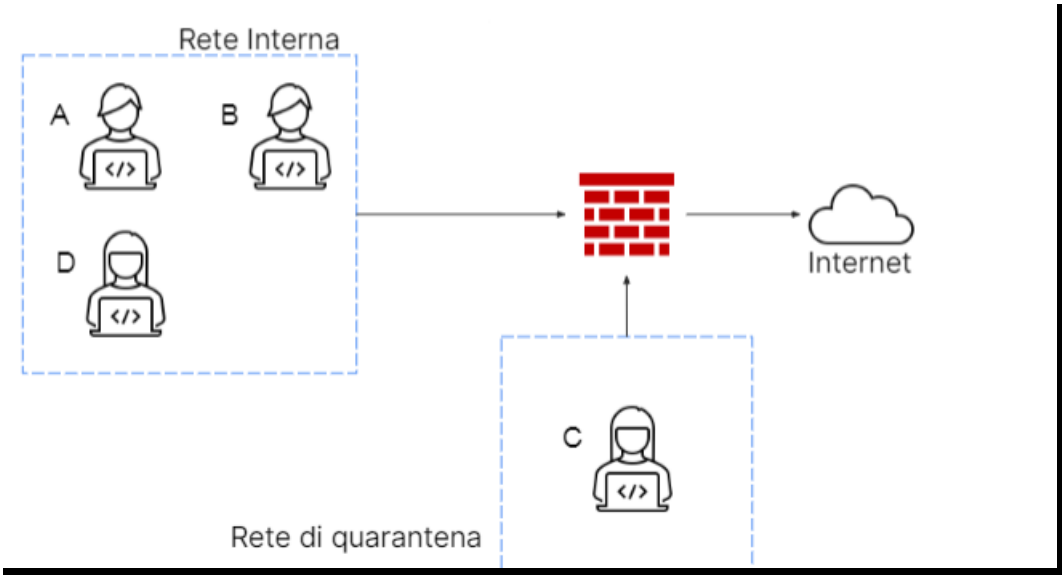



La fase di contenimento ha come obbiettivo principale l’isolamento dell’incidente, risultando appunto essenziale per la circoscrizione  ad un minor numero possibile di servizi, sistemi, dispositivi e nodi aziendali;

Esso può avvenire tramite diverse tecniche:

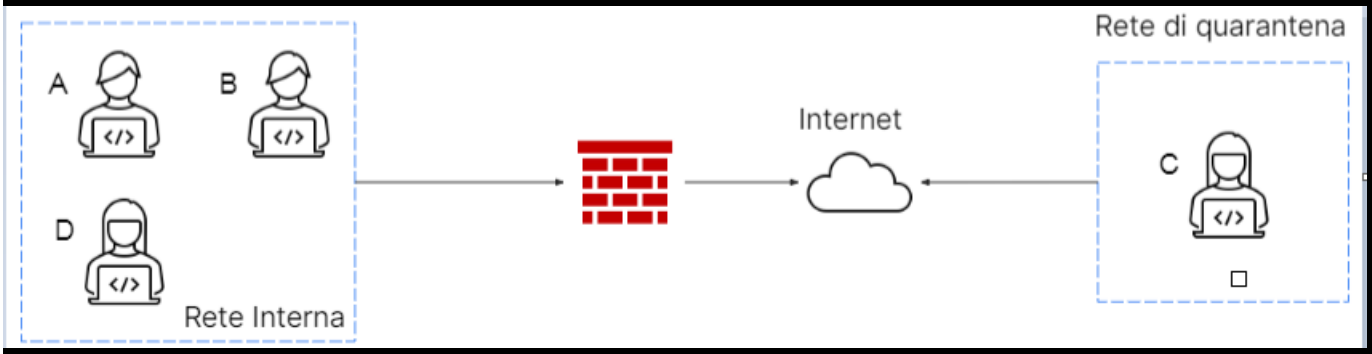
- La segmentazione, tecnica sia preventiva che di response, includendo metodi per dividere una rete in diverse LAN o VLAN, separando il sistema compromesso dagli altri sistemi.



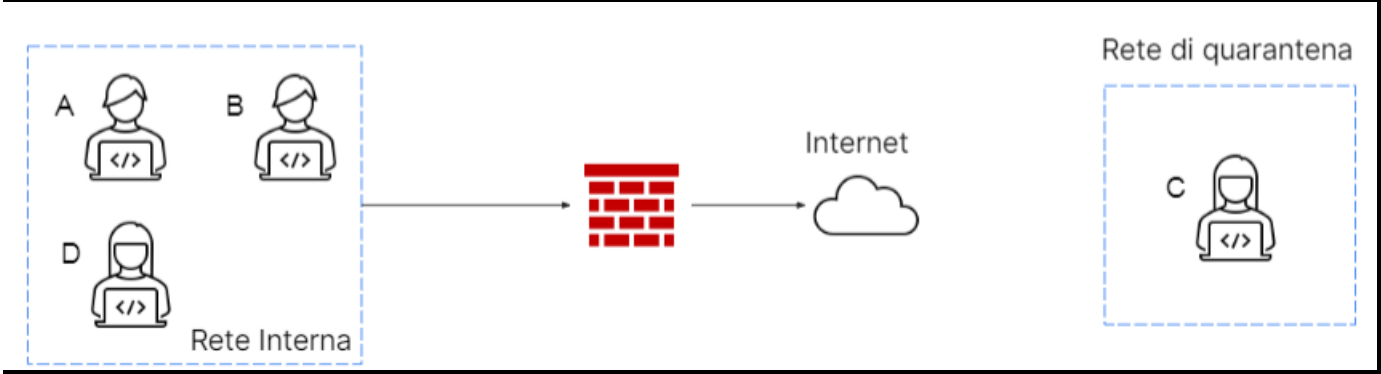



Separando appunto il sistema colpito e creando una rete apposita, chiamata “Rete di quarantena”

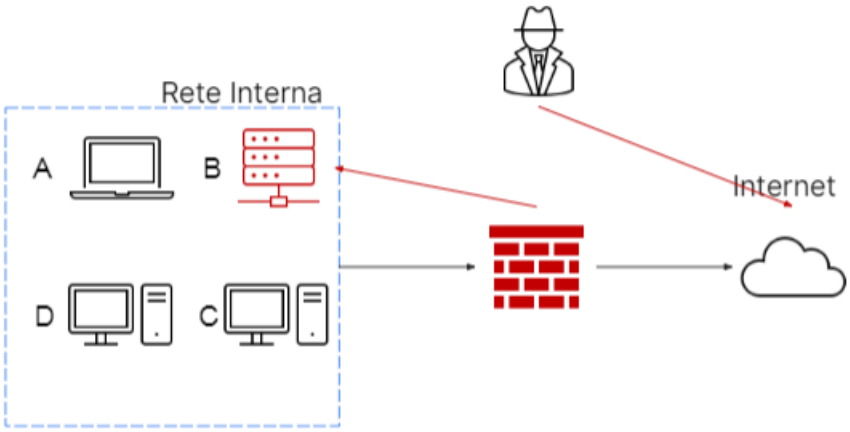
Quando la segmentazione però non risulta sufficiente , e si ritiene necessario un livello di isolamento maggiore, si ricorre alla tecnica d’isolamento, disconnettendo completamente il sistema/dispositivo dalla rete, per restringere ed allontanare quanto più possibile all’attaccante dalla rete interna aziendale.




Infine per rendere completamente impossibile la possibilità di accesso attaccante tramite sistema infetto è possibile effettuarne la rimozione completa dalla rete sia esterna che interna



A valle di questa veloce analisi delle tecniche di contenimento, esaminiamo il caso ipotetico specifico strutturato come illustrato in figura




In questo caso sarà opportuno rimuovere completamente il sistema denominato B dalla rete sia esterna che interna per evitare appunto la contaminazione e che l'attaccante possa ancora avere accesso ai dati sensibili presenti su database.

Dopo aver eseguito con successo la fase di contaminazione della minaccia, il team CSIRT avvia la fase di rimozione dell'incidente, eliminando di fatto ogni attività, componente e processi dell'incidente restanti all'interno di rete e sistemi.

Le tre opzioni possibili di effettuazione della rimozione sono :

1. Clear : In caso di attacchi non troppo invasivi e /o compromettenti, dove il dispositivo viene solamente ripulito con tecniche logiche, quali la ripetuta sovrascrittura o funzioni "factory reset" riportando il dispositivo allo stato iniziale.

2. Purge: In caso di attacchi/compromissione di media entità, in cui si utilizzano sia tecniche logiche del metodo "Clear" che tecniche di rimozione fisica quali l'utilizzo di potenti magneti per rendere le informazioni presenti inaccessibili.

3. Destroy: In caso di attacchi/compromissione di livello critico, approccio in cui oltre che strategie logiche e fisiche vengono utilizzate tecniche di laboratorio volte alla completa distruzione dei dispositivi, tramite polverizzazione ad alte temperature. Opzione radicale e e netta, richiedente un effort finanziario superiore alle prime due.