L4

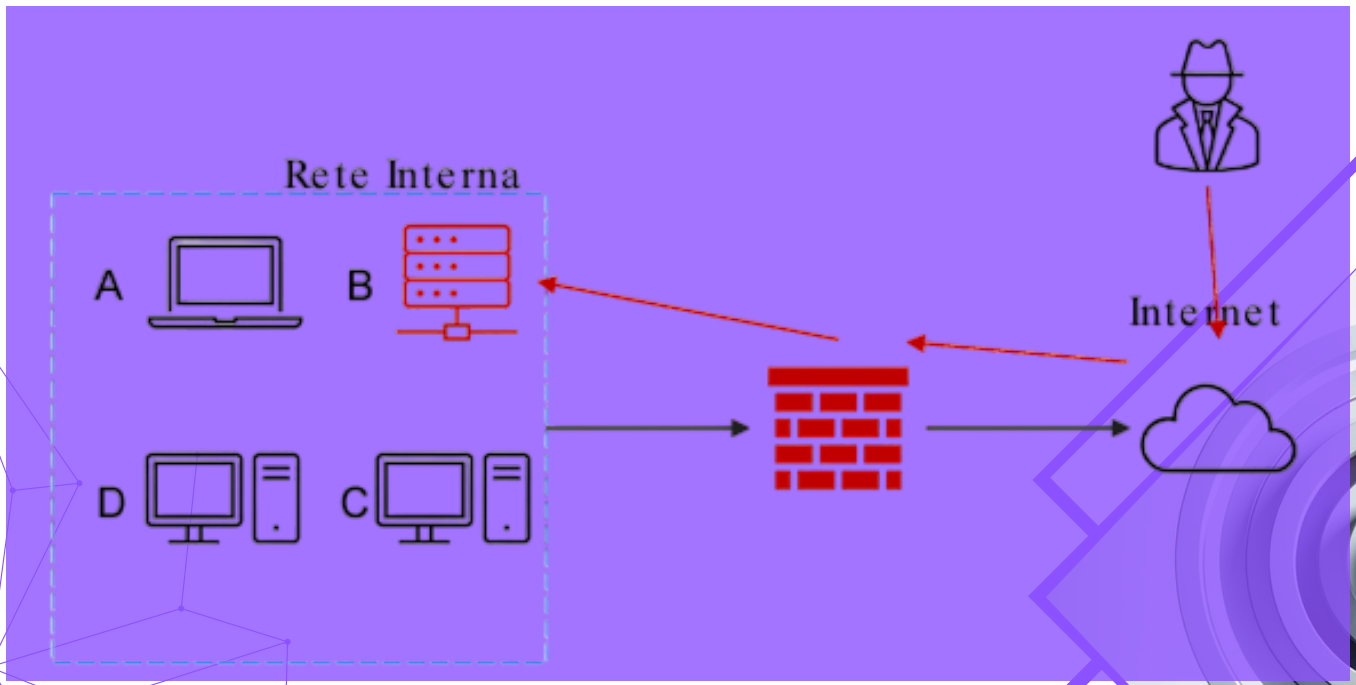
Con riferimento alla figura sotto, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

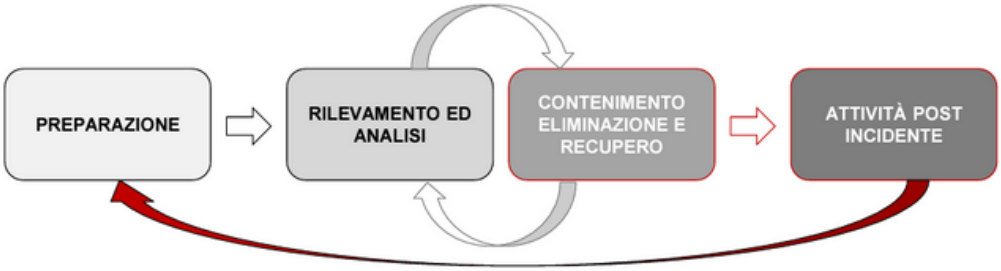
• Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto

• Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



Incident Response

Sebbene le aziende possano adottare precauzioni e preparare la protezione perimetrale per gli incidenti di sicurezza, la possibilità che si verifichi un incidente non è mai nulla.
Pertanto, le aziende devono prevedere che prima o poi si verificherà un incidente di sicurezza, come un virus o una fuga di dati sensibili, e creare un cosiddetto "**incident response plan**", ovvero un piano di risposta agli incidenti.
Il team responsabile di attuare il piano di risposta agli incidenti è il **CSIRT** (**Computer Security Incident Response Team**). Il CSIRT deve essere in grado di rispondere all'incidente di sicurezza in maniera calma e consistente.
Il processo di incident response non è un processo lineare, ma include dei cicli per tornare alle fasi precedenti dove necessario, e si articola generalmente come mostrato sotto.

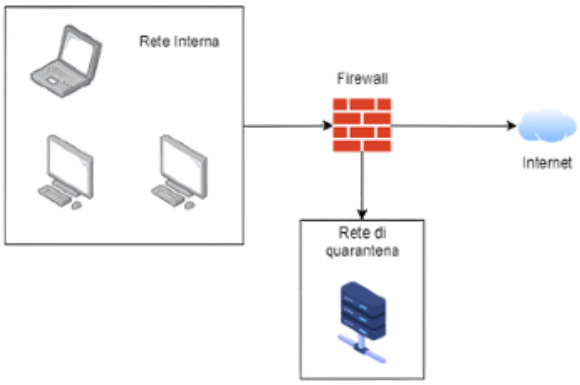


Completate le valutazioni, il CSIRT deve trovare una soluzione per ridurre al minimo gli impatti dell'incidente. Inizia la fase di contenimento, eliminazione e recupero che ha come scopo principale:

- La riduzione degli impatti causati dall'incidente;
- L'eliminazione dell'incidente dalla rete e dai sistemi;
- Il recupero dei servizi e delle operatività standard.

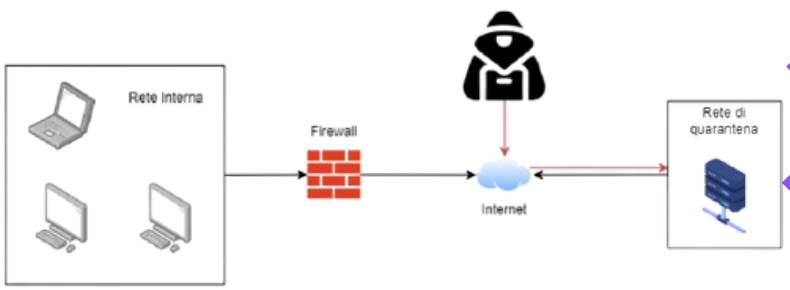
Tecniche di contenimento

Nella seconda fase del piano di risposta agli incidenti, ci si preoccupa del contenimento dei danni, eliminazione dell'incidente e recupero dei servizi standard.



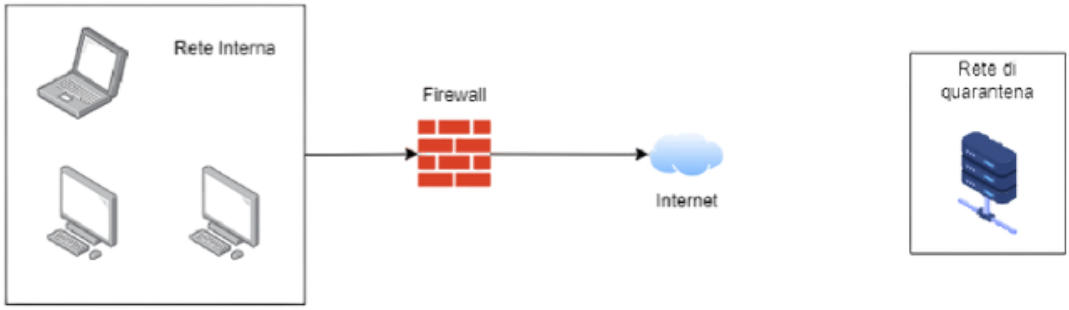
SEGMENTAZIONE:
La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN. Consiste nel dividere la rete o i sistemi in segmenti più piccoli per limitare la diffusione dell'incidente all'interno dell'organizzazione. In questo modo si riduce l'impatto dell'incidente isolando le parti compromesse del sistema, limitando la possibilità che l'incidente si propaghi ad altre parti della rete.
In questo caso la segmentazione permette di separare il dispositivo infetto, creando una rete ad hoc detta "rete di quarantena".

ISOLAMENTO:
Quando la segmentazione non basta, è necessario un contenimento maggiore: si utilizza la tecnica dell'isolamento.
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante e impedire che la minaccia possa influenzare altre parti del sistema. In questo caso si nota come l'attaccante abbia ancora accesso al dispositivo isolato tramite internet.

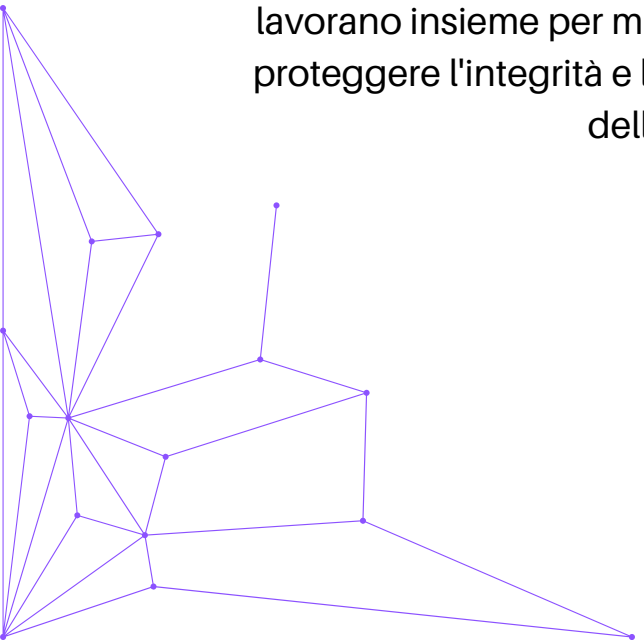


Tecniche di contenimento

RIMOZIONE: Se l'isolamennto non è ancora abbastanza, si utilizza la tecnica di contenimento più stringente: la rimozione completa del sistema dalla rete sia interna sia internet. In questo modo l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.
Lo scopo di questa tecnica è quello di garantire che i sistemi compromessi siano puliti e sicuri prima di essere rimessi in produzione.



Le tecniche di contenimento sono essenziali nella gestione degli incidenti di sicurezza. La segmentazione aiuta a limitare la diffusione dell'incidente, l'isolamento protegge immediatamente le risorse critiche, e la rimozione garantisce che le minacce siano eliminate e che i sistemi siano sicuri prima di tornare operativi. Queste tecniche lavorano insieme per minimizzare l'impatto di un incidente e proteggere l'integrità e la disponibilità dei sistemi informatici dell'organizzazione.



Rimozione
Informazioni Sensibili

Clear

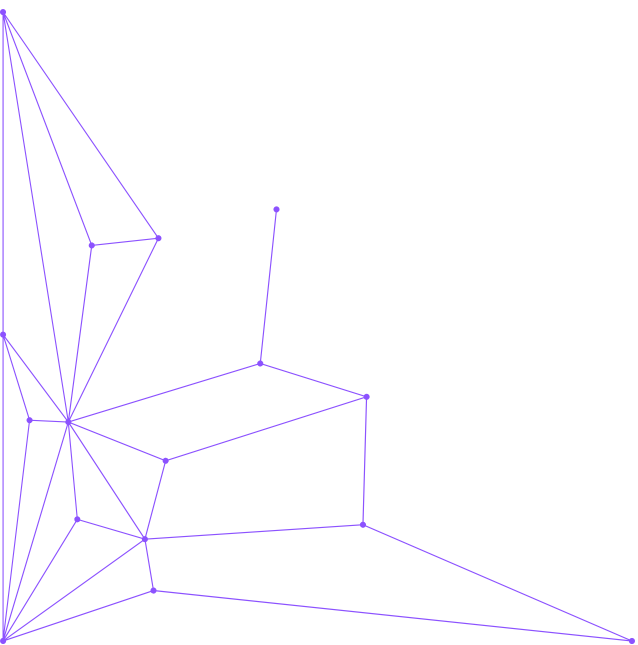
- Definizione: Eliminare i dati in modo che non possano essere recuperati utilizzando strumenti software standard.
- Esempio: Formattare rapidamente un disco rigido o eliminare file utilizzando comandi di cancellazione.

Purge

- Definizione: Eliminare i dati in modo che non possano essere recuperati nemmeno con strumenti avanzati di recupero dati.
- Esempio: Sovrascrivere i dati su un disco rigido con modelli specifici di dati casuali più volte.

Destroy

- Definizione: Distruggere fisicamente i supporti di memorizzazione per garantire che i dati non possano essere recuperati in alcun modo.
- Esempio: Frantumare un disco rigido, incenerire i supporti o usare un dispositivo di demagnetizzazione per rendere i dati illeggibili.



Confronto
Purge - Destroy

Purge

- **Approccio**: "Purge" adotta sia metodi logici che fisici per rimuovere i contenuti sensibili. Include tecniche come la degaussing, che utilizza forti campi magnetici per alterare i dati memorizzati su dispositivi magnetici, rendendoli inaccessibili.
- **Efficacia**: Sebbene efficace, non garantisce la distruzione fisica del dispositivo, quindi alcune tracce residue di dati potrebbero teoricamente essere recuperate con tecniche molto avanzate.

Destroy

- **Approccio**: "Destroy" è un metodo più radicale e definitivo. Oltre ai metodi logici e fisici, coinvolge tecniche di laboratorio che fisicamente distruggono il supporto di memorizzazione, rendendo impossibile qualsiasi tentativo di recupero dei dati.
- **Efficacia**: Garantisce la completa distruzione dei dati e del dispositivo, eliminando ogni possibilità di recupero. È il metodo più sicuro, ma anche il più costoso e complesso.

- **Effort e Costi**: "Purge" richiede meno risorse economiche e tecnologiche rispetto a "Destroy", ma offre un livello di sicurezza inferiore. "Destroy" è costoso e richiede apparecchiature specializzate, ma è estremamente sicuro.
- **Applicazioni:** "Purge" può essere sufficiente per dati meno sensibili o quando è necessaria una soluzione più economica. "Destroy" è preferibile per dati altamente sensibili dove la sicurezza è una priorità assoluta.

CONCLUSIONI

In questo esercizio, il sistema B della rete aziendale è stato compromesso da un attaccante attraverso l'accesso a Internet. Per mitigare l'incidente, si possono implementare delle tecniche di isolamento scollegando il sistema dalla rete e creando una VLAN quarantena. La rimozione delle minacce può essere effettuata tramite scansioni antimalware, applicazione di patch e, se necessario, ripristino da backup sicuri.
Per eliminare definitivamente le informazioni sensibili, è necessario utilizzare tecniche di purge per sovrascrivere i dati, e successivamente distruggere fisicamente i dischi compromessi per garantire la non recuperabilità delle informazioni.
Queste azioni combinate permettono di contenere l'incidente, rimuovere la minaccia e garantire la sicurezza dei dati sensibili, minimizzando l'impatto sull'infrastruttura aziendale e proteggendo l'integrità delle informazioni.