CS0424IT — ESERCITAZIONE S9L4
INCIDENT RESPONSE

Simone La Porta

GitHub

---

25 luglio 2024

INDICE

1 TRACCIA

Con riferimento alla Figura 1, il 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:

1. Mostrate le tecniche di **isolamento** per contenere il sistema compromesso.
2. Mostrate le tecniche di **rimozione del sistema infetto** dalla rete.
3. Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicate anche la tecnica **Clear**.

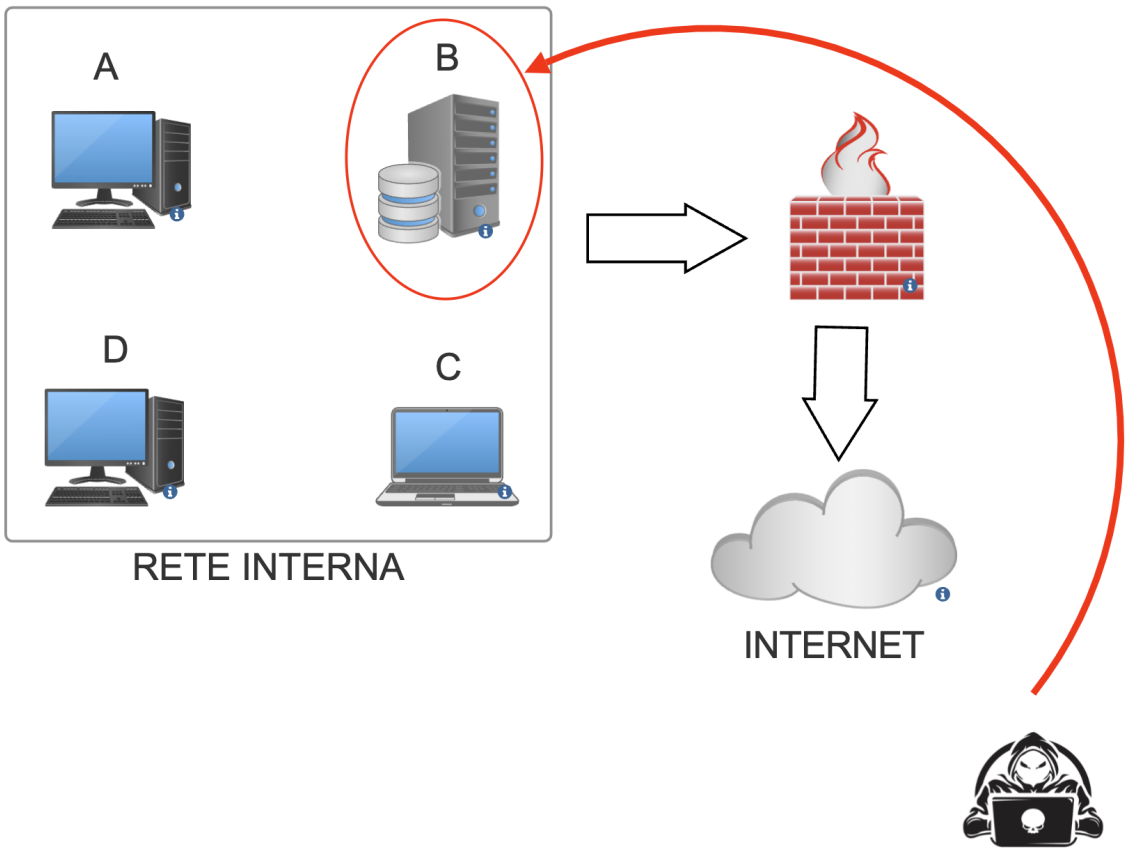

Figura 1: Diagramma della rete

2 DESCRIZIONE DELL'INCIDENTE

Questo report descrive i passaggi intrapresi dal team CSIRT in risposta a un incidente di sicurezza che ha coinvolto la compromissione di un server di database. L'incidente è stato rilevato mentre l'attacco era in corso e sono state necessarie azioni immediate per mitigare il danno e mettere in sicurezza la rete. Come illustrato nella Figura 2, il server di database (etichettato come B) all'interno della rete interna è stato compromesso da un attaccante che ha ottenuto accesso tramite Internet. L'attacco è attualmente in corso.

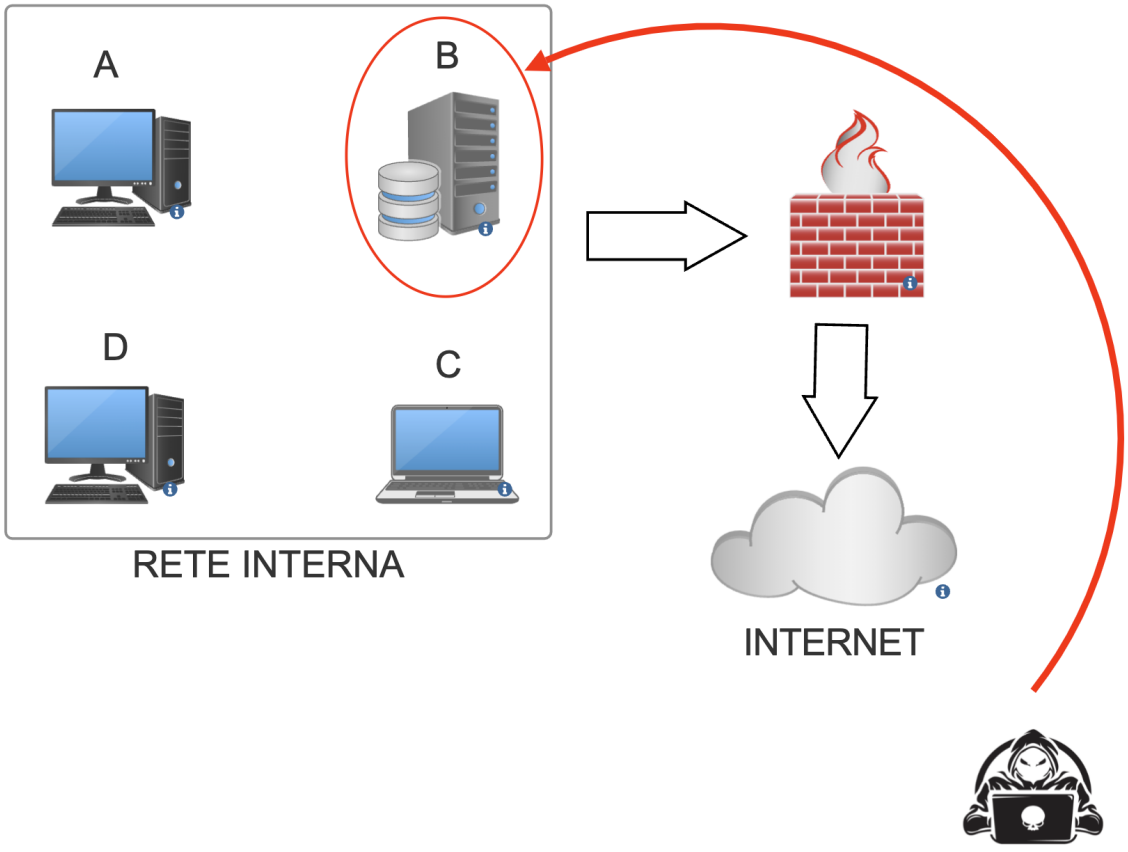

Figura 2: Diagramma della rete

3 RILEVAMENTO E ANALISI

La fase di rilevamento e analisi è una delle più complicate da gestire come un processo automatizzato e continuativo di routine. Infatti, sebbene ci siano diversi mezzi messi a disposizione per la fase di monitoraggio e analisi, alcuni degli incidenti sono rilevabili solamente da personale con forte esperienza sul campo.

Tra gli indicatori di attacchi in corso troviamo:

- Gli alert che hanno origine da un sistema di prevenzione e rilevamento intrusioni (IPS/IDS) o da un SIEM o da un sistema antivirus. Gli alert automatici «scattano» quando un evento sospetto si manifesta.
- I log generati da un sistema operativo, da un servizio o da un'applicazione, un dispositivo di rete e tutti i dispositivi hardware e software che sono in grado di produrre log.
- Informazioni pubbliche circa nuove vulnerabilità ed exploit appena scoperti (0-day), o scoperti in ambienti controllati.
- Persone interne o esterne alla compagnia che riportano attività sospette che potrebbero indicare un incidente di sicurezza in corso.

L'analisi è un processo piuttosto complesso che può essere supportato da alcune azioni per migliorare l'efficacia:

- Profilazione delle rete e dei sistemi.
- Implementazione di tool UEBA (User and Entity Behavior Analytics).
- Creazione di policy di logging efficaci.
- Correlazione degli eventi.
- Cattura del traffico.

4 TECNICHE DI RISPOSTA ALL'INCIDENTE

4.1 *Segmentazione della rete vs contenimento*

Segmentando la rete, spostiamo il server infetto in un'altra subnet, comunemente chiamata "rete di quarantena", come mostrato in Figura 3. Questo consente di limitare l'accesso dell'attaccante ad altri dispositivi presenti nella rete interna e, in caso di malware, ne impedisce la diffusione verso altri sistemi. Tuttavia, il server rimane accessibile tramite Internet, il che può rappresentare un rischio residuo.

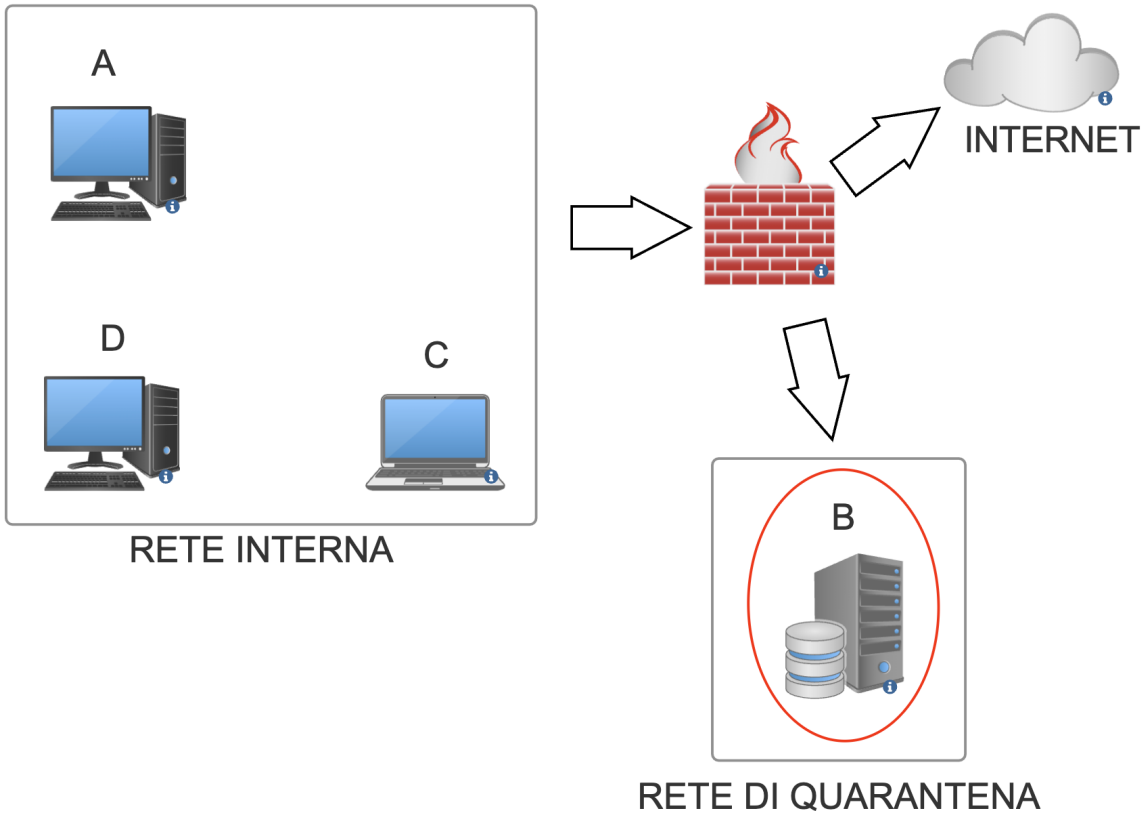

Figura 3: Segmentazione della rete

Per garantire una maggiore sicurezza, è essenziale implementare politiche di controllo degli accessi rigorose all'interno della rete di quarantena. Questo include l'uso di firewall avanzati e sistemi di rilevamento delle intrusioni (IDS) per monitorare e bloccare attività sospette. Inoltre, è consigliabile limitare il traffico in entrata e in uscita dal server infetto solo ai servizi strettamente necessari per le attività di analisi e risoluzione del problema. Nel caso in cui la

segmentazione non sia sufficientemente efficace, si procede con il contenimento, una strategia di risposta agli incidenti che mira a limitare l'impatto di una minaccia identificata e impedire la sua diffusione.

4.1.1 Tecniche di segmentazione

La segmentazione è una tecnica di sicurezza informatica utilizzata per dividere una rete in subnet più piccole e gestibili, chiamate segmenti, ciascuno con i propri controlli di sicurezza. Questo approccio migliora la sicurezza riducendo la superficie d'attacco e limitando il movimento laterale di eventuali intrusi all'interno della rete. Ecco alcune caratteristiche principali della segmentazione:

- Isolamento delle risorse: le risorse critiche vengono isolate dagli altri segmenti della rete, riducendo il rischio di accesso non autorizzato.
- Controllo degli accessi: politiche di accesso più restrittive possono essere applicate a ciascun segmento, basate sul principio del minimo privilegio.
- Miglior monitoraggio e risposta: la segmentazione facilita il monitoraggio delle attività e la risposta agli incidenti, permettendo una rapida identificazione e contenimento delle minacce all'interno di un segmento specifico.
- Performance migliorata: riducendo il traffico di rete attraverso una segmentazione intelligente, si possono migliorare le performance della rete.

4.1.2 Differenze chiave

Proattività vs Reattività La segmentazione è una misura proattiva, progettata per prevenire attacchi futuri attraverso la strutturazione della rete. Il contenimento, invece, è una misura reattiva, applicata in risposta a un incidente in corso.

Scope La segmentazione riguarda la configurazione della rete a lungo termine, mentre il contenimento si concentra sull'immediata limitazione dei danni durante un incidente di sicurezza.

In sintesi, entrambe le tecniche sono fondamentali per una strategia di sicurezza informatica completa, con la segmentazione che funge da misura preventiva e il contenimento che fornisce una risposta efficace agli incidenti.

4.2 *Isolamento*

L'isolamento è una tecnica impiegata quando è necessario un contenimento più rigoroso del sistema infetto. In questo scenario, come mostrato in Figura 4, il sistema viene completamente disconnesso dalla rete interna, riducendo ulteriormente le possibilità dell'attaccante di accedere ad altri dispositivi all'interno della rete aziendale. Tuttavia, anche in questo caso, il dispositivo infetto potrebbe rimanere accessibile tramite Internet, il che rappresenta ancora un potenziale rischio di sicurezza.

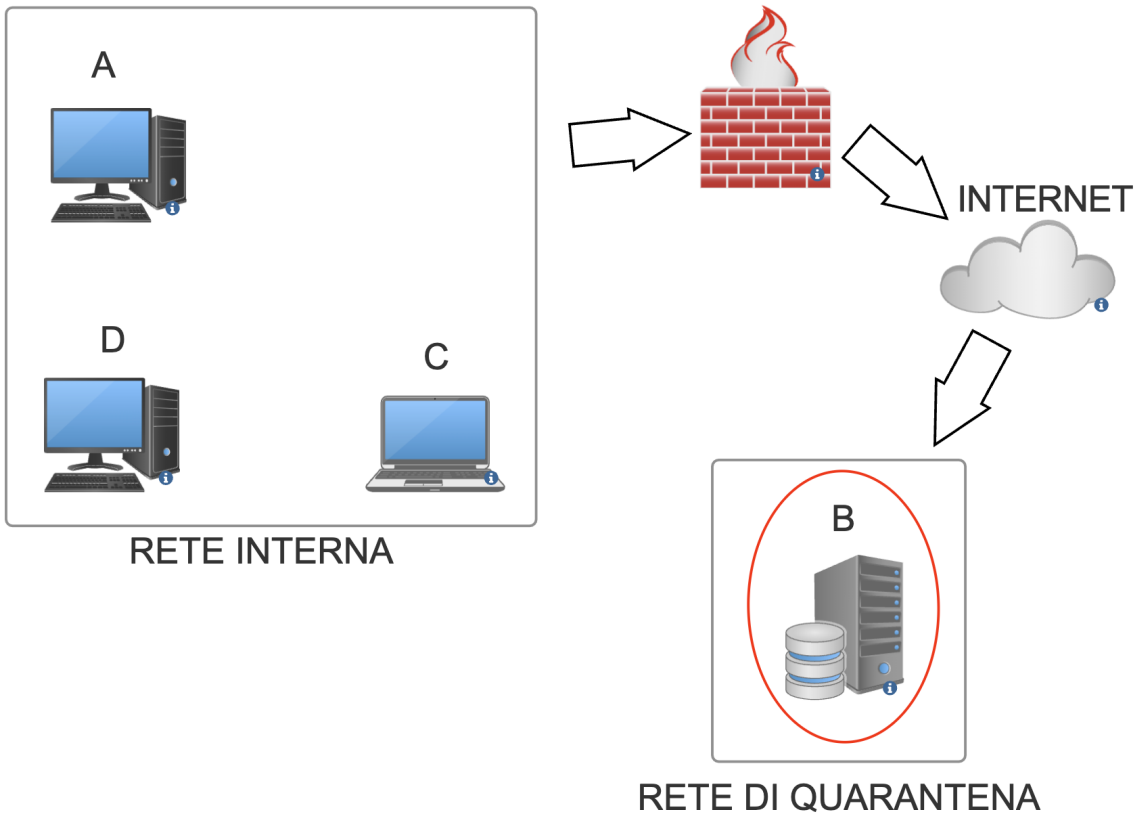

Figura 4: Isolamento dalla rete interna

Caratteristiche principali dell'isolamento includono:

- Isolamento del sistema:
  - Disconnessione fisica o logica: il sistema compromesso viene scollegato fisicamente dalla rete o isolato logicamente tramite configurazioni di rete, come la disabilitazione delle interfacce di rete.
  - Mantenimento della funzionalità limitata: in alcuni casi, il sistema può rimanere operativo ma con accesso limitato, permettendo ulteriori analisi senza rischiare la propagazione della minaccia.
- Isolamento del segmento di rete:
  - Segmentazione temporanea: segmentare temporaneamente parti della rete per contenere l'incidente all'interno di un'area specifica.
  - Controllo del traffico: utilizzare firewall e altre soluzioni di sicurezza per bloccare il traffico tra segmenti della rete.
- Isolamento degli utenti:
  - Blocco degli account: disabilitare gli account utente compromessi per prevenire ulteriori accessi non autorizzati.
  - Restrizione dei privilegi: ridurre i privilegi degli utenti sospetti per limitare le loro capacità all'interno del sistema.
- Isolamento delle applicazioni:
  - Containerizzazione: eseguire applicazioni in contenitori separati per limitare l'impatto di un compromesso a livello applicativo.
  - Virtualizzazione: utilizzare macchine virtuali per isolare applicazioni e servizi critici, rendendo più facile il contenimento in caso di attacco.

4.2.1 Benefici dell'isolamento

- Limitazione della propagazione: l'isolamento impedisce alla minaccia di diffondersi ad altri sistemi e segmenti della rete.

- Facilitazione dell'analisi: separare il sistema compromesso consente una migliore analisi forense senza il rischio di ulteriori contaminazioni.
- Riduzione dell'impatto: minimizza i danni operativi e finanziari limitando l'incidente a una parte controllata dell'infrastruttura.

4.2.2 Tecniche di isolamento comune

- Network Quarantine: isolamento della macchina compromessa in una rete di quarantena per ulteriori indagini.
- Virtual LANs (VLANs): utilizzo di VLAN per separare il traffico di rete e limitare l'accesso tra segmenti.
- Endpoint Isolation: utilizzo di software di sicurezza per isolare endpoint compromessi.

4.2.3 Esempi di applicazione

- Ransomware Attack: in caso di attacco ransomware, isolare i sistemi infetti per prevenire la crittografia di ulteriori dati.
- Phishing Compromise: disabilitare l'account email compromesso e isolare i sistemi coinvolti per prevenire l'ulteriore diffusione di email malevoli.

4.3 *Rimozione del sistema infetto*

Nel caso in cui anche l'isolamento non sia sufficientemente efficace, si procede con la rimozione (o isolamento completo) del server. Questo implica la rimozione di tutte le connessioni di rete, sia interne che esterne, garantendo che il server non possa comunicare con alcun altro dispositivo o rete, come rappresentato in Figura 5. Durante questa fase, è fondamentale eseguire un'analisi approfondita del server infetto per identificare la natura dell'attacco e implementare le misure di riparazione necessarie.

4.3.1 Rimozione nelle tecniche di contenimento

La rimozione è una tecnica di contenimento utilizzata nella risposta agli incidenti di sicurezza informatica per eliminare le minacce identificate da un sistema o una rete. Questa tecnica è

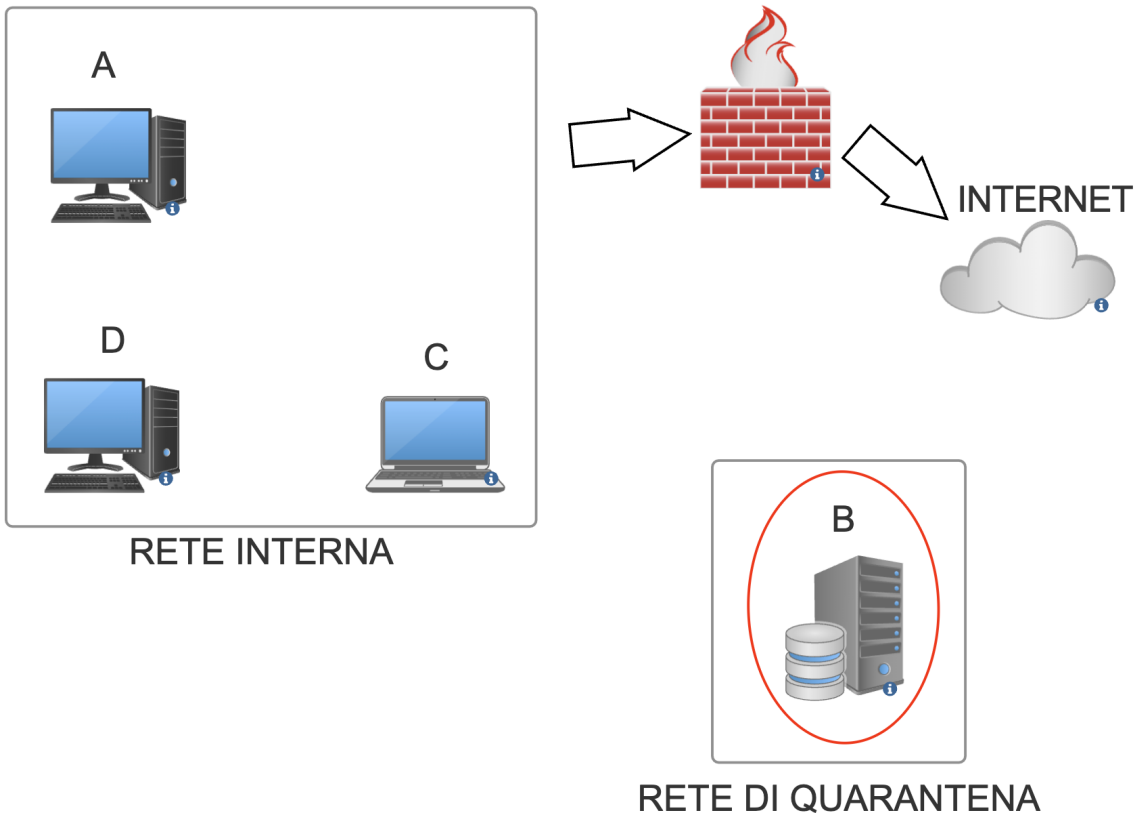

Figura 5: Rimozione completa dalla rete

finalizzata a neutralizzare completamente la minaccia, ripristinare la sicurezza del sistema e prevenire future compromissioni. Caratteristiche principali della rimozione includono:

- Identificazione completa della minaccia:
  - Scansione e Analisi: utilizzo di strumenti di sicurezza come antivirus, antimalware e scanner di vulnerabilità per identificare tutti i componenti malevoli presenti nel sistema.
- Eliminazione del Malware:
  - Pulizia del sistema: rimozione dei file infetti, chiavi di registro malevole e altri artefatti del malware tramite software di sicurezza.
  - Ripristino di file modificati: ripristino dei file di sistema critici che potrebbero essere stati alterati dall'attacco.

- Correzione delle vulnerabilità:
  - Patch e aggiornamenti: applicazione di patch di sicurezza e aggiornamenti per correggere le vulnerabilità sfruttate dall'attacco.
  - Modifiche alla configurazione: aggiustamenti alla configurazione di sicurezza per rafforzare le difese e prevenire future compromissioni.
- Rimozione degli accessi non autorizzati:
  - Disabilitazione degli account: rimozione o disabilitazione di account utente compromessi o creati dagli attaccanti.
  - Cambio delle password: richiesta di cambio delle password per gli account utenti per prevenire accessi non autorizzati futuri.
- Ripristino dei sistemi compromessi:
  - Ripristino da backup: utilizzo di backup recenti per ripristinare i sistemi compromessi a uno stato sicuro.
  - Verifica dell'integrità del sistema: controllo dell'integrità del sistema dopo la rimozione per assicurarsi che tutte le minacce siano state eliminate.

4.3.2 Benefici della rimozione

- Eliminazione della minaccia: la rimozione assicura che il sistema sia libero da malware e altre componenti malevoli.
- Ripristino della sicurezza: ripristina la sicurezza del sistema permettendo di tornare a operare in modo normale e sicuro.
- Prevenzione di future compromissioni: correggendo le vulnerabilità e rafforzando le difese, si riduce il rischio di future compromissioni.

4.3.3 Tecniche di rimozione comuni

- Antivirus e Antimalware: utilizzo di software specializzati per rilevare e rimuovere malware e altre minacce.

- Strumenti di pulizia manuale: in alcuni casi, potrebbe essere necessaria una rimozione manuale di artefatti malevoli da parte di esperti di sicurezza.
- Formattazione e reinstallazione: nei casi più gravi, la formattazione del sistema e la reinstallazione completa possono essere necessarie per garantire la completa rimozione della minaccia.

5 ELIMINAZIONE DELLE INFORMAZIONI SENSIBILI

Quando si tratta di eliminare informazioni sensibili da dischi compromessi prima dello smaltimento, esistono diverse metodologie riconosciute, tra cui Clear, Purge e Destroy.

5.1 *Clear*

Metodo che rende i dati inaccessibili tramite tecniche logiche, ma non necessariamente irrecuperabili tramite tecniche avanzate di recupero dati.

- **Overwrite:** utilizzare comandi software per ripristinare il disco alle impostazioni di fabbrica.
- **Reset:** sovrascrivere tutti i settori del disco con dati casuali o con uno schema specifico (ad esempio, tutti zeri, tutti uno o una combinazione ripetuta).

Clear è generalmente sufficiente per eliminare dati in ambienti in cui il rischio di accesso non autorizzato è considerato basso o dove non sono presenti informazioni altamente sensibili.

5.2 *Purge*

Metodo che adotta sia un approccio logico che delle tecniche di rimozione fisica.

- **Degaussing:** utilizzare un dispositivo degausser per smagnetizzare il disco, cancellando tutti i dati memorizzati.
- **Sanitization software:** utilizzare software specializzato per eseguire la sovrascrittura multipla del disco con schemi complessi e variabili, rendendo molto difficile il recupero dei dati.
- **Cryptographic erase:** sovrascrivere le chiavi di cifratura utilizzate per proteggere i dati memorizzati, rendendo i dati stessi indecifrabili.

Purge è adatto per scenari in cui i dati sono considerati altamente sensibili e vi è un rischio maggiore che qualcuno tenti di recuperarli con strumenti avanzati.

5.3 *Destroy*

Metodo più sicuro e definitivo per garantire che i dati non possano essere recuperati in alcun modo.

- **Shredding:** utilizzare macchine specializzate per distruggere fisicamente il disco in piccoli pezzi.
- **Incineration:** bruciare i dischi in forni ad alta temperatura.
- **Chemical erase:** utilizzare sostanze chimiche per dissolvere i materiali del disco.

Destroy è necessario quando i dati sono estremamente sensibili e devono essere completamente e permanentemente irrecuperabili, indipendentemente dalle tecnologie disponibili.

5.4 *Confronto tra Clear, Purge e Destroy*

- **Clear:** rende i dati inaccessibili tramite metodi standard, ma può essere vulnerabile a tecniche avanzate di recupero.
- **Purge:** rende i dati inaccessibili anche tramite metodi avanzati, ma non distrugge fisicamente il disco.
- **Destroy:** elimina fisicamente il disco, garantendo l'impossibilità assoluta di recupero dei dati.

La scelta tra queste tecniche dipende dal livello di sensibilità dei dati e dalle politiche di sicurezza dell'organizzazione.

6 FASE DI RECUPERO

La fase di recupero ha l'obiettivo di ristabilire la normale operatività delle applicazioni e dei servizi dopo un attacco informatico. Questo processo include diverse attività essenziali, come il recupero dei dati e delle informazioni perse, l'applicazione di patch per sistemi obsoleti, la revisione delle politiche di firewall, IPS e IDS, e l'aggiornamento delle firme degli antivirus. Lo

scopo della fase di recupero è non solo ripristinare la funzionalità, ma anche prevenire futuri attacchi simili.

Quando sistemi, server e host vengono compromessi, devono essere considerati non più affidabili. È fondamentale ripulirli a fondo prima di rimetterli in produzione, utilizzando tecniche di ”reconstruction” o ”rebuilding”:

- **Reconstruction:** questa tecnica mira a recuperare e ripristinare le parti ancora affidabili di un sistema compromesso, eliminando solo le componenti danneggiate o infette.
- **Rebuilding:** qesta tecnica implica la ricostruzione completa del sistema compromesso, partendo da zero. È utilizzata quando il sistema è considerato completamente inaffidabile.

Per quanto riguarda le applicazioni, i server e i software, prima di procedere con la fase di recupero, è cruciale identificare il punto di ingresso dell'attacco. Capire dove si trovano le vulnerabilità consente di implementare le patch necessarie e rafforzare la sicurezza, prevenendo il ripetersi dell'incidente. Questo approccio analitico garantisce che le misure correttive siano efficaci e mirate, migliorando la resilienza complessiva del sistema.

In sintesi, la fase di recupero non solo ripristina la funzionalità, ma rappresenta anche un'opportunità per rafforzare le difese contro future minacce, assicurando che i sistemi siano adeguatamente protetti e pronti per operare in modo sicuro e affidabile.

7 CONCLUSIONE

La gestione efficace degli incidenti di sicurezza informatica richiede una combinazione di tecniche di rilevamento, analisi e risposta ben coordinate. Questo report ha illustrato le diverse fasi e strategie adottate dal team CSIRT per rispondere a un attacco informatico in corso che ha compromesso un server di database.

Durante la fase di **rilevamento e analisi**, è emerso che il monitoraggio continuo e l'esperienza del personale sono fondamentali per identificare tempestivamente le minacce. Gli indicatori di compromissione, come gli alert dei sistemi di prevenzione e rilevamento delle intrusioni, i log di sistema e le segnalazioni di vulnerabilità pubbliche, hanno svolto un ruolo cruciale nel riconoscere l'attacco.

Per quanto riguarda la fase di **risposta all'incidente**, sono state discusse in dettaglio le tecniche di segmentazione della rete e di contenimento. La segmentazione ha permesso di

isolare il server compromesso in una rete di quarantena, riducendo il rischio di diffusione del malware e limitando l'accesso non autorizzato. Il contenimento ha ulteriormente mitigato l'impatto dell'attacco, grazie all'implementazione di misure di sicurezza aggiuntive come il blocco degli account compromessi e la limitazione del traffico di rete.

Nella fase di **isolamento**, il sistema infetto è stato completamente disconnesso dalla rete interna, consentendo un'analisi più approfondita senza rischi di propagazione della minaccia. Tecniche come la disconnessione fisica o logica e l'isolamento delle applicazioni e degli utenti hanno assicurato un controllo più rigoroso sulla situazione.

La **rimozione del sistema infetto** ha incluso la scansione e l'eliminazione del malware, la correzione delle vulnerabilità e il ripristino dei sistemi compromessi tramite backup sicuri. Questa fase ha garantito che il sistema fosse ripulito da qualsiasi traccia di minaccia, ripristinando la sicurezza e la funzionalità operativa.

Per quanto riguarda l'**eliminazione delle informazioni sensibili**, le tecniche di Clear, Purge e Destroy sono state esaminate. Ogni tecnica presenta vantaggi specifici in base al livello di sensibilità dei dati e alle esigenze di sicurezza dell'organizzazione. La scelta della metodologia più appropriata dipende dal contesto specifico e dalla necessità di garantire l'irrecuperabilità dei dati compromessi.

Infine, la **fase di recupero** ha sottolineato l'importanza di ripristinare la normale operatività delle applicazioni e dei servizi, rafforzando al contempo le difese contro futuri attacchi. Tecniche di reconstruction e rebuilding sono state impiegate per garantire che i sistemi fossero completamente affidabili prima di rimetterli in produzione.

In sintesi, il processo di risposta agli incidenti descritto in questo report dimostra l'importanza di una strategia ben pianificata e coordinata per affrontare le minacce informatiche. Adottando misure proattive e reattive, è possibile mitigare l'impatto degli attacchi, proteggere le informazioni sensibili e assicurare la continuità operativa dell'organizzazione. La collaborazione tra i vari team e l'uso di tecnologie avanzate sono elementi chiave per garantire una risposta efficace e tempestiva agli incidenti di sicurezza informatica.