4 FEBBRAIO 2024

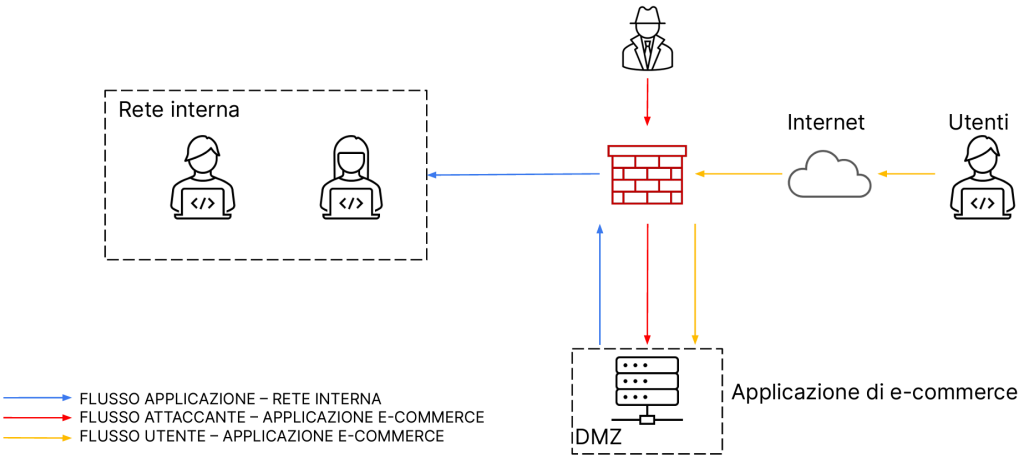
PROGETTO S9-L5

INDICE

ARCHITETTURA DI RETE

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE

TRACCIA

Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

SEGMENTAZIONE

Una delle configurazioni di rete maggiormente utilizzate prevede l'implementazione della "SEGMENTAZIONE"; una tecnica di sicurezza che consiste nel dividere una rete in diverse LAN o VLAN, particolarmente utile nella fase di contenimento di un incidente in corso.
In questo caso specifico l'applicazione di e-commerce è così configurata:

-segmento DMZ: per i server accessibili da internet
-segmento rete interna: per i dispositivi utilizzati dai dipendenti

La DMZ è progettata per essere una zona di sicurezza che isola i server accessibili da internet dalla rete interna privata.
In questo caso specifico la DMZ è configurata in modo tale da comunicare direttamente con la rete interna aumentando il rischio di compromissione da parte di un utente malintenzionato.

WEB APPLICATION FIREWALL

L'implementazione di un WAF può essere un modo efficace per migliorare la sicurezza delle applicazioni web e ridurre il rischio di data breach(compromissione di dati sensibili).

Un web application firewall, generalmente è strutturato come segue:

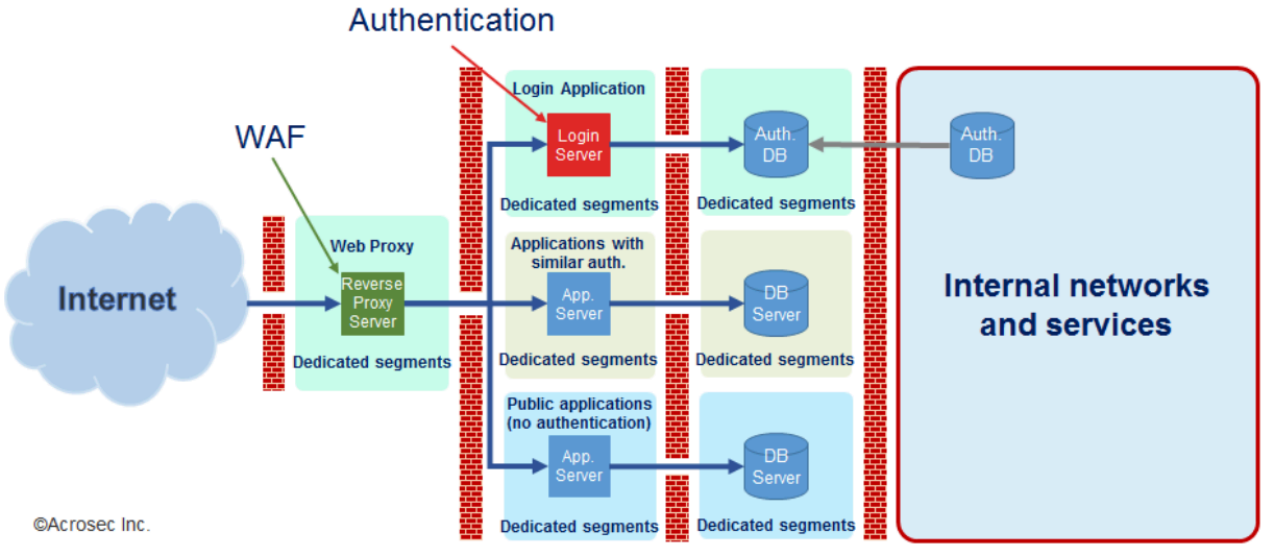
INTERFACCIA DI RETE:
Il WAF è collegato alla rete e posizionato tra il server delle applicazioni web e l'esterno (ad esempio, Internet). Ha almeno due interfacce di rete, una orientata verso il server delle applicazioni web (backend) e l'altra verso l'esterno o la rete client (frontend).

REGOLE DI SICUREZZA:
Criteri che il WAF utilizza per identificare e bloccare il traffico dannoso, le regole possono essere basate su firme, comportamento del traffico, anomalie...
Le firme spesso corrispondono a modelli noti di attacchi, come SQL injection, cross-site scripting XSS...

MODULI DI SICUREZZA:
Il WAF può essere suddiviso in moduli di sicurezza che affrontano specifiche categorie di minacce, ad esempio potrebbe esserci un modulo specifico per la prevenzione di attacchi SQL injection e così via.

RISPOSTA AGLI INCIDENTI:
Il WAF può essere configurato in modo tale da rispondere automaticamente nel caso in cui rilevi un attacco, bloccando l'accesso ad un indirizzo IP sospetto o attivando altri meccanismi di mitigazione.

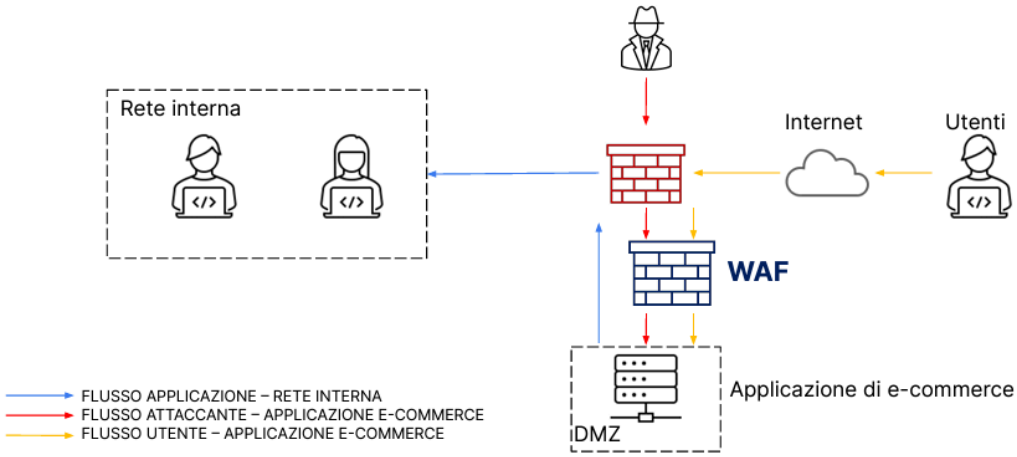
SVANTAGGI:
La configurazione e la gestione possono essere complesse e richiedere un certo grado di competenza tecnica, inoltre l'implementazione e la manutenzione possono comportare costi significativi in termini di risorse.
Un WAF è efficace contro attacchi noti e ben definiti, ma potrebbe non essere altrettanto efficace contro minacce emergenti; è quindi necessario aggiornare periodicamente il database di firme di possibili exploit



DIFESA CONTRO ATTACCHI ALLE WEB APPLICATION

La motivazione principale che ci porta in questo caso specifico ad implementare un WAF piuttosto che un altro tipo di firewall è il contesto in cui lavora l'applicazione di e-commerce;
A differenza di un comune firewall, un WAF è progettato per identificare e bloccare una varietà di attacchi alle applicazioni web, come SQL injection, XSS ed altri exploit comuni, fornendo un'ulteriore strato di difesa oltre alle misure di sicurezza implementate a livello di codice.
Il WAF è in grado di fornire informazioni preziose sugli attacchi alle applicazioni web, questo consente di identificare le vulnerabilità migliorando l'attuale stato di sicurezza. il traffico in ingresso e in uscita viene filtrato , consentendo il passaggio di dati leciti e bloccando le richieste sospette, questo aiuto a proteggere le applicazioni web da exploit e attacchi di livello applicativo.

Vediamo nel dettaglio l'impatto del WAF all'interno della configurazione di rete dell'e-commerce



il WAF posizionato tra un firewall e una DMZ svolge un ruolo chiave nella difesa delle applicazioni web esposte dall'esterno, filtrando il traffico dannoso prima che raggiunga la DMZ e, successivamente, la rete interna.

MISURE DI SICUREZZA AGGIUNTIVE

Se un Web Application Firewall (WAF) dovesse risultare insufficiente a garantire una sicurezza adeguata, è importante considerare strategie aggiuntive e implementare una difesa in profondità. Ecco alcune misure che potrebbero essere adottate:

SICUREZZA DEL CODICE:
Assicurarsi che il codice delle applicazioni web sia sicuro è fondamentale. Questo può essere ottenuto attraverso l'utilizzo di funzioni di sanificazione all'interno del codice, l'implementazione delle migliori pratiche di sviluppo sicuro e l'uso di strumenti di analisi statica e dinamica del codice.

AGGIORNAMENTI E PATCHING:
Mantenere costantemente aggiornati sia il software delle applicazioni web che i componenti di sistema. Applicare prontamente patch e aggiornamenti di sicurezza per ridurre le vulnerabilità.

GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI(IAM):
Implementare controlli rigorosi sull'accesso, garantendo che gli utenti e i servizi ottengano solo i privilegi di cui hanno bisogno. L'uso di soluzioni IAM aiuta a limitare i rischi legati alle credenziali utente.

PROTEZIONE DA DDoS:
Per proteggere le applicazioni web da attacchi distribuiti del tipo DDoS (Distributed Denial of Service), implementare soluzioni di mitigazione DDoS che possano riconoscere e mitigare attacchi volumetrici.

MONITORAGGIO E ANALISI DEL TRAFFICO:
implementare sistemi di monitoraggio avanzato del traffico per rilevare in tempo reale attività sospette o anomalie. Utilizzare strumenti di analisi del comportamento per identificare pattern di attacco.

SISTEMI DI RILEVAMENTO DELLE INTRUSIONI (IDS) E SISTEMI DI PREVENZIONE DELLE INTRUSIONI (IPS):
Integrare IDS e IPS nella strategia di sicurezza per rilevare e prevenire attacchi avanzati. Questi sistemi possono individuare attività anomale e intrusione nella rete.

BACKUP E RIPRISTINO:
Mantenere regolarmente backup delle applicazioni e dei dati critici. In caso di compromissione, i backup consentono un rapido ripristino dei sistemi.

FORMAZIONE E CONSAPEVOLEZZA DEGLI UTENTI:
Formare gli utenti sulla sicurezza informatica e promuovere una cultura di sicurezza all'interno dell'organizzazione. Gli utenti consapevoli sono meno inclini a cadere vittima di attacchi di social engineering.

SERVIZI DI SICUREZZA GESTITI (MSSP):
Considerare l'impiego di servizi di sicurezza gestiti forniti da provider specializzati. Gli MSSP possono offrire monitoraggio costante, risposta agli incidenti e consulenza specialistica.

IMPATTI SUL BUSINESS

TRACCIA

> **Impatti sul business**: l'applicazione Web subisce un attacco di tipo Ddos dall'esterno che rende l'applicazione non raggiungibile per **10 minuti**. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** sulla piattaforma di e-commerce.

ATTACCO DDOS

Un attacco DDoS (Distributed Denial of Service) è un tipo di attacco informatico in cui un CC server invia tramite un vasto numero di sistemi compromessi (zombie) pacchetti di dati per sovraccaricare e rendere inaccessibili i servizi di una risorsa target, come un sito web o un'applicazione online. L'obiettivo di un attacco DDoS è di saturare le risorse del sistema, impedendo agli utenti legittimi di accedervi.
Si tratta dunque di una "botnet" gestita in modo centralizzato.
L'impatto di un attacco DDos sul business può essere significativo, con perdite di fatturato e danni all'immagine e alla reputazione del brand. È importante quindi avere misure di sicurezza adeguate per prevenire e mitigare gli attacchi DDos

PERDITA DI FATTURATO STIMATO (PFS)

PARAMETRI: MSU media spesa utenti per minuto
MI minuti di inattività

PFS = MSU*MI

PFS= 1.500€ * 10

PFS = 15.000€

VALUTAZIONE DELL'IMPATTO COMPLESSIVO

Perdita finanziaria diretta: 15.000€

Complessivamente ci sono altri aspetti fondamentali da valutare tra cui:

Perdita di vendite future
L'indisponibilità del servizio potrebbe causare la perdita di opportunità di vendita durante e dopo l'attacco, gli utenti potrebbero decidere di cercare alternative e non tornare sulla piattaforma dopo l'incidente.

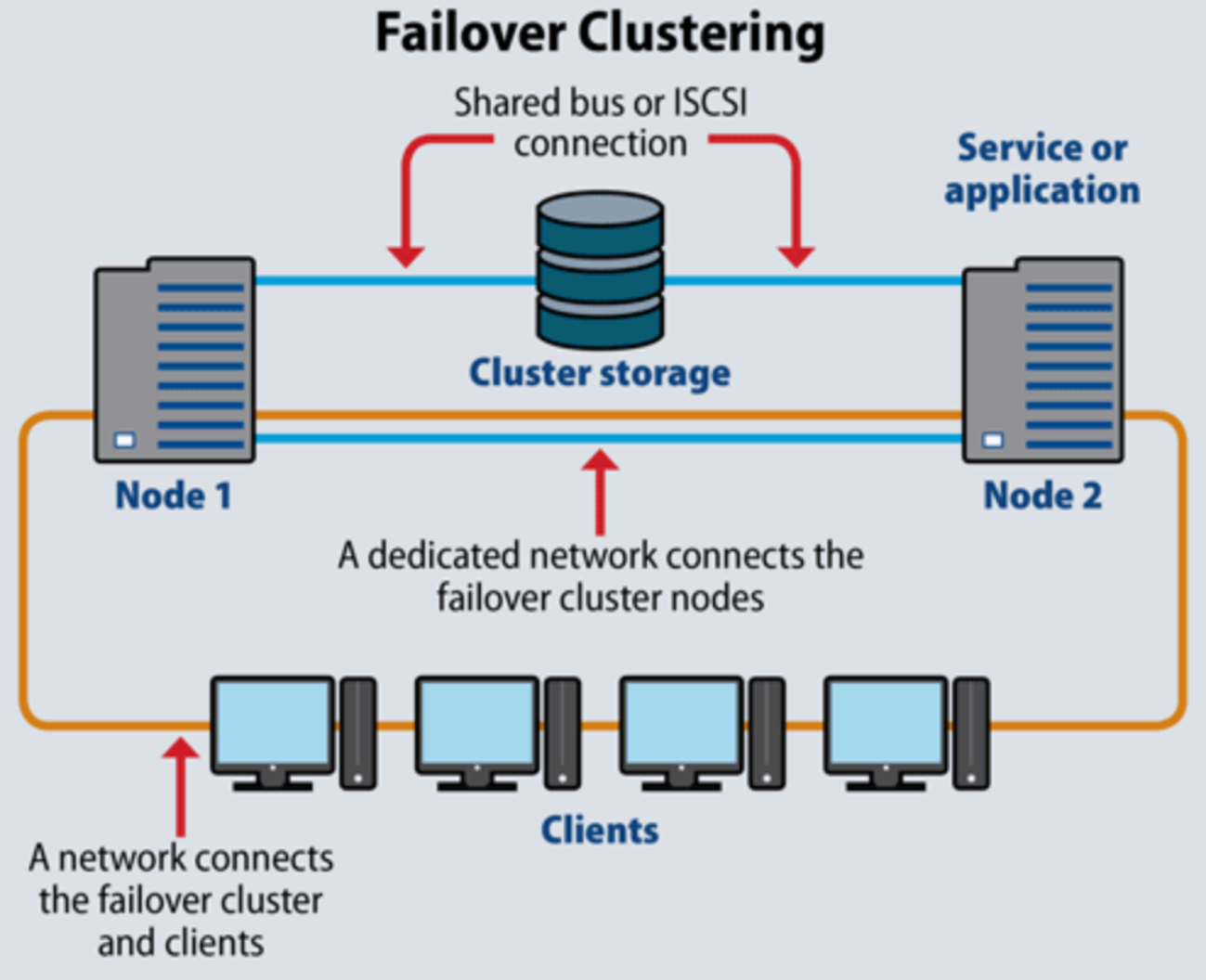
Danno alla reputazione
Un'indisponibilità prolungata o ripetuta della piattaforma può danneggiare la reputazione dell'azienda. La percezione negativa degli utenti può influire sulla fedeltà del cliente e sulla fiducia nel marchio

Costi di mitigazione
È necessario investire in soluzioni di mitigazione DDos, servizi aggiuntivi o altre misure per prevenire futuri attacchi.

MISURE DI PREVENZIONE

FAILOVER CLUSTER

Un failover cluster è una configurazione di sistema che collega più server (o nodi) in modo che possano lavorare insieme come un'unica unità coesa. L'obiettivo principale di un failover cluster è garantire l'alta disponibilità e la continuità operativa dei servizi o delle applicazioni ospitate dai nodi del cluster.
In caso di guasto su uno dei nodi del cluster, le risorse vengono automaticamente spostate su un nodo funzionante senza interrompere il servizio. Questo processo è noto come failover.



HOT SITE/COLD SITE

Hot Site:
Un hot site è una replica completa e funzionante dell'ambiente IT primario di un'azienda. Tutti i dati, le applicazioni e l'infrastruttura sono duplicati e mantenuti aggiornati in tempo reale con l'ambiente primario. In caso di un'interruzione, le operazioni possono essere commutate immediatamente sull'hot site. Gli hot site richiedono un investimento significativo in termini di risorse e costi operativi.
Caratteristiche principali:

Replica completa dell'ambiente IT primario.

Continuamente sincronizzato con l'ambiente primario.

Tempi di ripristino rapidi.

Costi operativi elevati.

Cold Site:
Un cold site è una struttura fisica senza hardware o software operativi. È un'infrastruttura di base che può essere attivata solo quando è necessario. Mentre gli ambienti primari e i cold site sono fisicamente separati, i dati e i sistemi critici possono essere ripristinati nel cold site in caso di emergenza. Il processo di attivazione di un cold site richiede più tempo rispetto a un hot site.
Caratteristiche principali:

Struttura di base senza hardware o software operativi.

Richiede l'installazione e la configurazione di sistemi e dati in caso di attivazione.

Tempi di ripristino più lunghi rispetto agli hot site.

Costi operativi inferiori rispetto agli hot site.

DISASTER RECOVERY AS A SERVICE (DRaaS)

Disaster recovery as a service (DRaaS) è un servizio cloud che consente alle aziende di recuperare rapidamente i propri dati e applicazioni in caso di disastro.

Come funziona DRaaS:

Backup dei dati e delle applicazioni**:** I dati e le applicazioni aziendali vengono regolarmente copiati e archiviati nel cloud del provider DRaaS.

Replica in tempo reale**:** Alcuni fornitori DRaaS offrono anche la replica in tempo reale dei dati, garantendo che la copia archiviata nel cloud sia sempre aggiornata.

Failover automatico**:** In caso di disastro, il servizio DRaaS esegue automaticamente un failover, spostando le applicazioni e i dati su un ambiente cloud dedicato.

Accesso alle applicazioni**:** Gli utenti possono quindi accedere alle applicazioni e ai dati dall'ambiente cloud fino a quando l'infrastruttura IT primaria non viene ripristinata.

DRaas elimina la necessità di investire e mantenere una propria infrastruttura di disaster recovery, riducendo i costi IT. così facendo però le aziende dipendono dal provider per ripristinare le proprie applicazioni, sebbene sia spesso più conveniente in quanto l'azienda paga solo l'attivazione del cloud quando necessario, i costi DRaas possono comunque essere significativi.
Tra gli svantaggi va considerato che l'accesso alle applicazioni e ai dati durante un failover potrebbe avere una latenza maggiore rispetto all'infrastruttura locale.

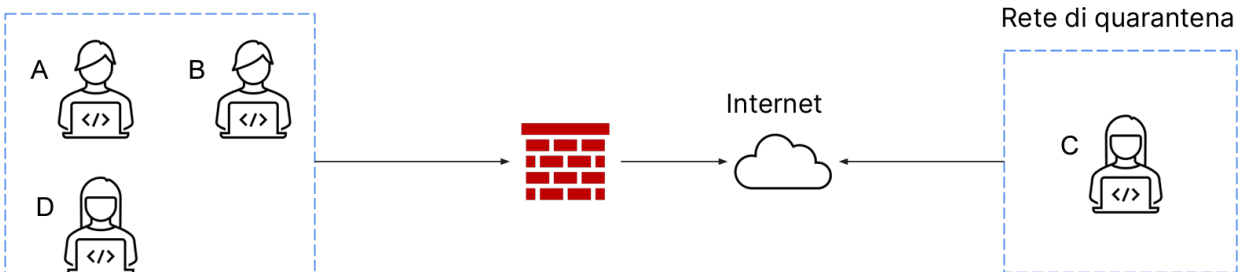
RESPONSE

TRACCIA

Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

ISOLAMENTO E CONTENIMENTO

L'isolamento è un passo fondamentale nell'ambito dell'Incident Response (IR), ovvero il processo di identificazione, contenimento, eradicazione e ripristino dopo un incidente di sicurezza informatica. L'obiettivo dell'isolamento è limitare la diffusione di un attacco, mitigare i danni e accelerare la risoluzione dell'incidente.



L'isolamento tempestivo della macchina infetta è fondamentale per limitare i danni. Esistono due modalità per attuarlo:

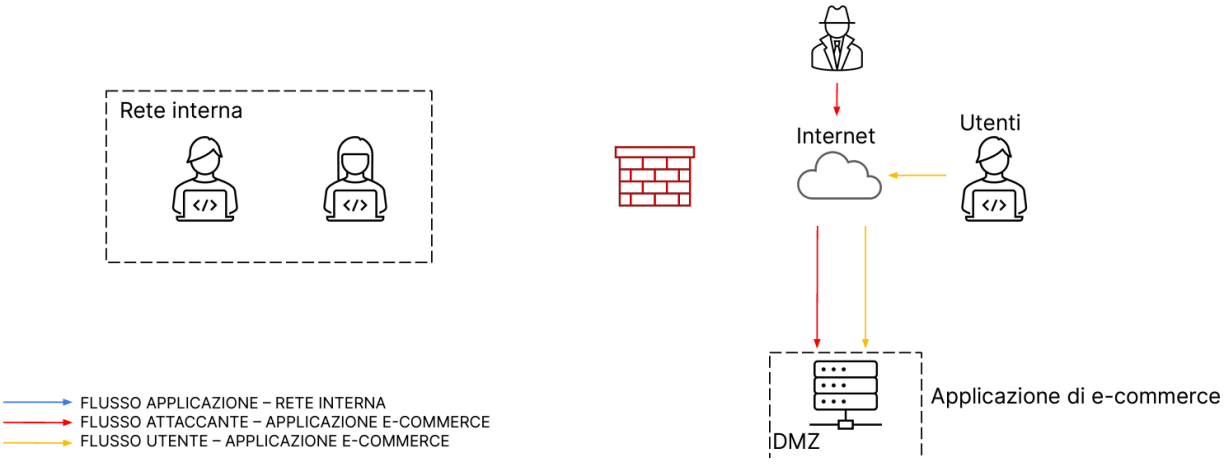
Isolamento a livello di rete:
Scollegamento fisico: La soluzione più semplice e sicura consiste nel disconnettere la macchina infetta dalla rete fisica. Tuttavia, questo metodo può risultare scomodo se la macchina in questione è utilizzata regolarmente per attività lavorative.
VLAN di quarantena: Un'alternativa più flessibile è l'utilizzo di una VLAN di quarantena. Questa tecnica crea una rete virtuale separata per la macchina infetta, consentendole di accedere ad internet ma isolandola dal resto della rete aziendale, è la scelta ottimale nel caso in cui la macchina infetta risulta essere critica per il business, è importante minimizzare l'interruzione del servizio.

Isolamento a livello di software:
Software di sicurezza di rete: Esistono software specifici che possono isolare la macchina infetta reindirizzando il suo traffico su una rete virtuale separata.
Virtualizzazione: Se la macchina infetta è virtualizzata, è possibile spostarla in un ambiente virtuale isolato, garantendo una maggiore sicurezza e controllo.

L'isolamento di una macchina infetta direttamente a Internet rappresenta una strategia alternativa con vantaggi e svantaggi da valutare attentamente prima dell'implementazione.

VANTAGGI:
Riduzione del rischio di propagazione: L'isolamento impedisce al malware di diffondersi all'interno della rete aziendale, limitando i danni potenziali.
Accesso per l'analisi: L'attaccante potrebbe ancora accedere alla macchina infetta, fornendo un'opportunità per l'analisi del malware e la comprensione delle sue tattiche e tecniche.
Minore impatto sull'attività aziendale: Collegando la macchina direttamente a Internet, si evita di disconnetterla completamente dalla rete, minimizzando l'interruzione del servizio per gli utenti.

SVANTAGGI:
Rischio di esposizione di dati sensibili: La macchina infetta potrebbe contenere dati sensibili aziendali che potrebbero essere esposti all'attaccante se si collega direttamente a Internet.
Difficoltà di analisi: L'accesso da parte dell'attaccante potrebbe ostacolare l'analisi del malware, in quanto potrebbe modificare il suo comportamento o attivare contromisure.
Mancanza di controllo: L'azienda non ha il controllo completo dell'ambiente in cui opera il malware, rendendo difficoltosa la rimozione e la bonifca



RIMOZIONE E RECUPERO

A valle delle attività di contenimento, il team CSIRT passa alla fase di rimozione dell'incidente, lo scopo è quello di eliminare tutte le attività, componenti e i processi che restano dell'incidente all'interno della rete o sui sistemi. Quest'attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette usb compromesse.
È importante implementare strumenti di monitoraggio attivo per tenere traccia delle attività sul dispositivo isolato, conducendo un analisi forense sulla macchina isolata è possibile raccogliere prove sull'incidente e comprendere la portata dell'attacco.
Queste informazioni saranno preziose per migliorare la sicurezza complessiva del sistema.
Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattai, inizia la fase di recupero, ovvero ristabilire la normale operatività delle applicazioni e dei servizi.
Bisogna procedere con la revisione delle politiche dei firewall, IPS e IDS, e con l'aggiornamento delle firme degli antivirus.
Lo scopo finale è quello di evitare che lo stesso attacco possa nuovamente verificarsi.