PROGETTO S9-L5

INDICE:

TRACCIA:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

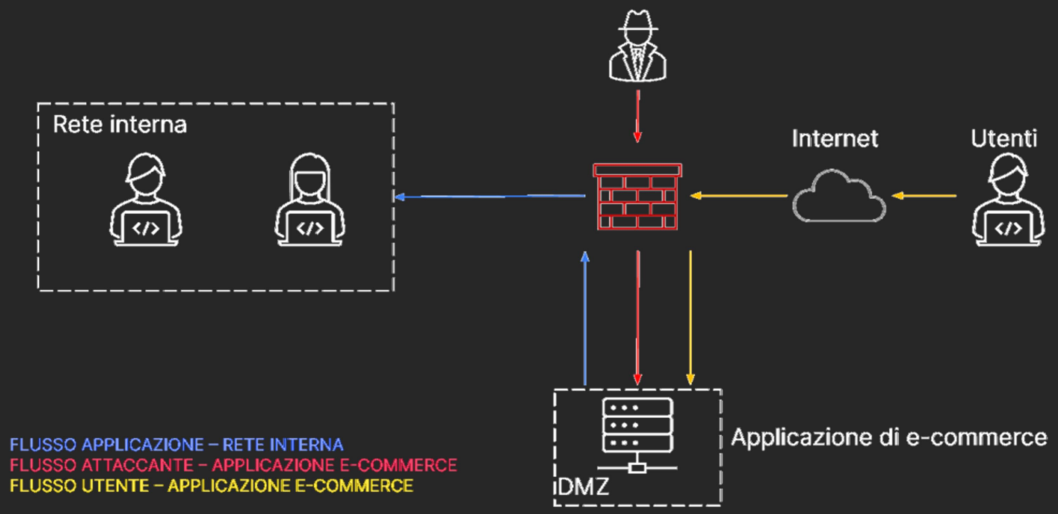
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. 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.

3. 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.

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.



PROGETTO S9-L5

AZIONI PREVENTIVE

Per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS è possibile adottare una soluzione preventiva basata su un Web Application Firewall (WAF), dove agisce come filtro per il traffico in ingresso proveniente da internet.

Cos'è il WAF ?

Il WAF sta per "Web Application Firewall". Si tratta di un sistema di sicurezza progettato per proteggere le applicazioni web da varie minacce e attacchi informatici, in particolare da attacchi di tipo SQL injection (SQLi), cross-site scripting (XSS), e altri exploit mirati alle vulnerabilità delle applicazioni web.

E' un'applicazione di sicurezza che si trova tra una Web App e il traffico di rete, filtrando e monitorando tutte le comunicazioni tra l'applicazione web e il traffico in ingresso. Utilizza un insieme di regole predefinite o personalizzabili per identificare e bloccare potenziali minacce e attacchi.

ALCUNE CARATTERISTICHE:

- **Filtraggio del traffico:** Il WAF analizza il traffico in entrata e in uscita tra la Web App e gli utenti, identificando e filtrando le richieste che possono rappresentare una minaccia.

- **Regole di sicurezza:** Il WAF utilizza regole predefinite o personalizzate per rilevare modelli di comportamento sospetto o tentativi di sfruttare vulnerabilità specifiche. Ad esempio, può bloccare richieste che contengono codice SQL malevolo o script XSS.

- **Protezione contro attacchi noti:** Il WAF è progettato per difendere contro attacchi noti e ben noti, aiutando a mitigare le minacce senza richiedere modifiche dirette al codice dell'applicazione.

- **Monitoraggio e reportistica:** Oltre a bloccare attacchi, il WAF fornisce funzionalità di monitoraggio e reportistica per consentire agli amministratori di sistema di tenere traccia delle attività sospette e analizzare potenziali minacce.

PROGETTO S9-L5

IMPATTI SUL BUSINESS

L'attacco di tipo DDoS provoca un breve periodo di inaccessibilità della piattaforma di e-commerce, durante il quale gli utenti non possono effettuare acquisti. Per valutare l'impatto finanziario, abbiamo considerato che i clienti spendono una somma significativa di denaro al minuto. Moltiplicando questa spesa potenziale per il numero di minuti in cui il servizio è stato indisponibile, otteniamo una stima approssimativa dei mancati guadagni. Pertanto, l'impatto sul business può essere calcolato come il prodotto tra la spesa potenziale degli utenti per minuto e la durata dell'indisponibilità del servizio. In questo caso specifico, l'azienda ha subito una perdita di 15.000 € a causa dei 10 minuti di inattività della piattaforma.

OPERAZIONE

Impatti sul business = Media guadagno al minuto X tempo inattività = Perdita potenziale

Impatto sul business = 1.500€ x 10 Minuti = 15.000€

Cos'è un attacco DDoS ?

Un attacco DDoS, acronimo di "Distributed Denial of Service," è un tipo di attacco informatico che mira a rendere inaccessibile un servizio, un sito web o una risorsa online, sovraccaricandoli con un volume enorme di richieste. Tecnicamente, un attacco DDoS coinvolge l'invio simultaneo di un grande numero di richieste da parte di molteplici dispositivi distribuiti in una rete. L'obiettivo principale è sopraffare il sistema di destinazione, facendolo diventare incapace di rispondere alle richieste legittime degli utenti.

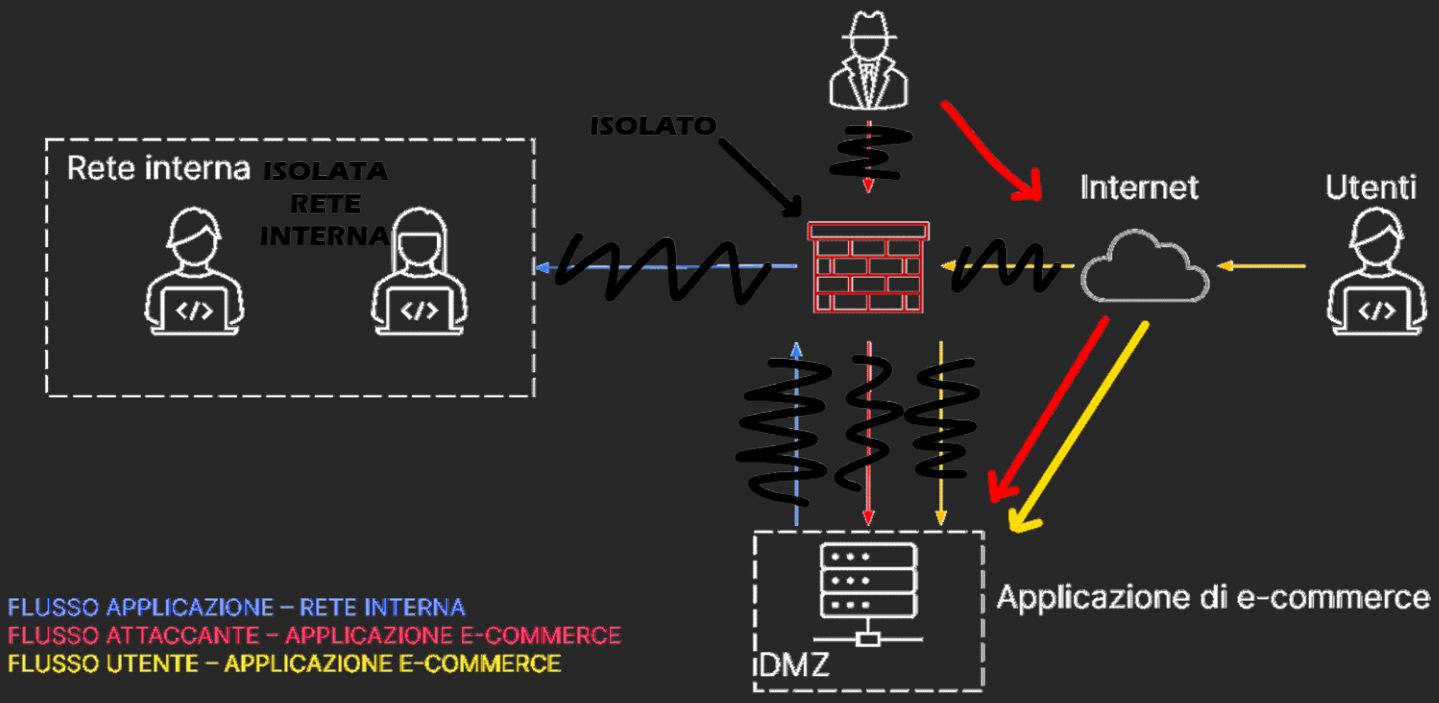
ALCUNE CARATTERISTICHE:

- **Zombie Network (Botnet): Gli attacchi DDoS spesso coinvolgono un insieme di computer o dispositivi compromessi chiamato "botnet." Questi dispositivi possono essere infettati da malware senza che i proprietari se ne rendano conto.**
- **Generazione di Traffico Fittizio: Una volta che la rete di dispositivi compromessi è pronta, il malintenzionato invia comandi al botnet per generare un'enorme quantità di traffico fittizio.**
- **Sovraccarico delle Risorse del Target: Tutte queste richieste provenienti dal botnet vengono indirizzate al bersaglio dell'attacco, che può essere un server web, un'applicazione o un servizio online. L'obiettivo è sovraccaricare le risorse del bersaglio**
- **Negazione del Servizio: A causa dell'enorme volume di traffico, il sistema di destinazione non è in grado di gestire tutte le richieste, rendendo il servizio inaccessibile per gli utenti legittimi.**

PROGETTO S9-L5

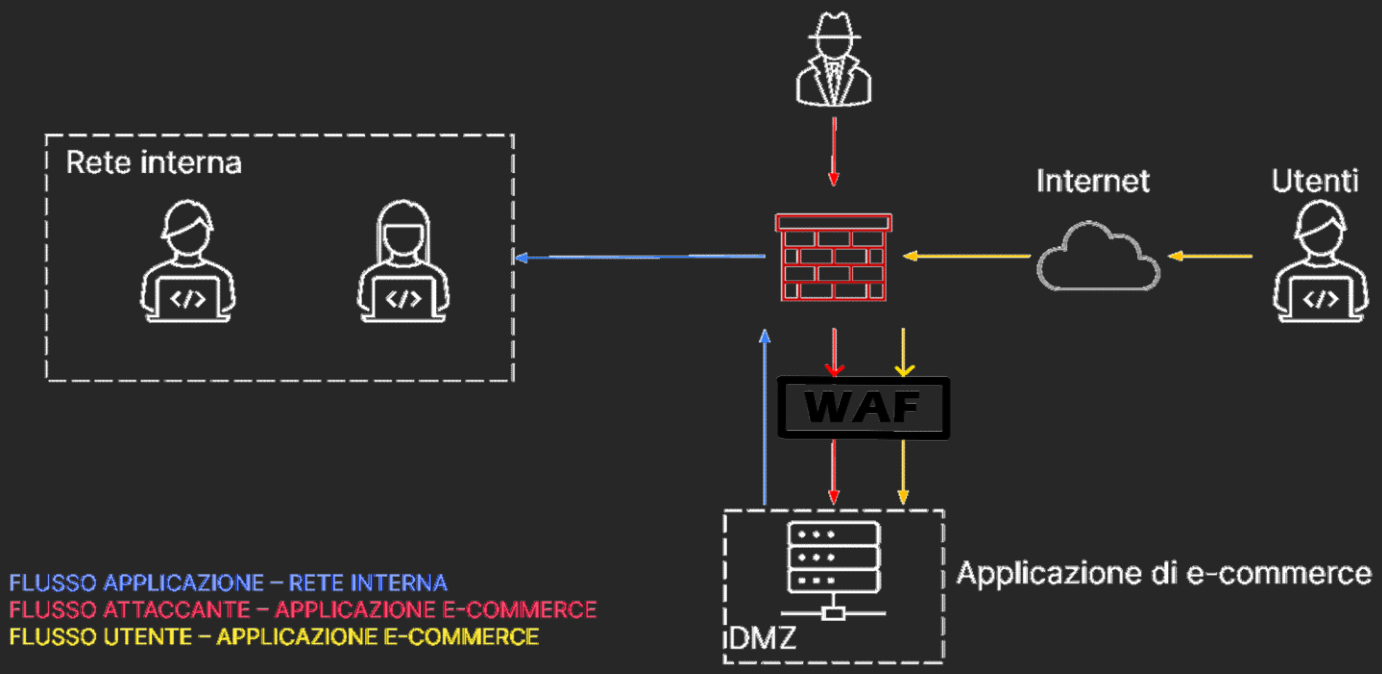
RESPONSE

Considerando la priorità, è possibile implementare una strategia focalizzata sull'isolamento della macchina compromessa. In questo scenario, la macchina sarebbe collegata direttamente a Internet, rendendola accessibile all'attaccante, ma interrompendo la connessione con la rete interna. Nella successiva illustrazione, possiamo osservare la soluzione che adotta la strategia di isolamento della macchina infetta.



PROGETTO S9-L5

ARCHITETTURA DI RETE



La DMZ (Demilitarized Zone), generalmente funge da zona intermedia tra la rete interna sicura e Internet, ha accesso alla rete interna a causa delle politiche del firewall. Questo potrebbe essere un problema di configurazione o di regole del firewall che consentono una comunicazione diretta dalla DMZ alla rete interna.

Per comprendere il potenziale rischio, è utile considerare la funzione principale della DMZ. La DMZ è progettata per ospitare servizi che sono destinati ad essere accessibili da Internet, come server web, e-mail o altri servizi pubblici. La sua esistenza è finalizzata a impedire che gli attaccanti possano compromettere direttamente la rete interna se riescono ad accedere alla DMZ.

Se il server nella DMZ viene compromesso e, attraverso questa compromissione, l'attaccante ottiene un accesso non autorizzato, e se le politiche del firewall consentono la comunicazione dalla DMZ alla rete interna, allora potenzialmente l'attaccante potrebbe utilizzare la DMZ come punto di ingresso per raggiungere la rete interna. Questo aumenterebbe il rischio di un'espansione dell'attacco oltre la DMZ, compromettendo eventualmente i sistemi interni più sensibili.

Per mitigare questo rischio, è fondamentale configurare attentamente le regole del firewall in modo da limitare le comunicazioni tra la DMZ e la rete interna, permettendo solo il traffico necessario per i servizi specifici ospitati nella DMZ. Inoltre, è importante monitorare attentamente la sicurezza nella DMZ, adottando misure come la segmentazione della rete e l'implementazione di sicurezza avanzata per proteggere gli asset critici.

PROGETTO S9-L5

Il Web Application Firewall (WAF) viene utilizzato per l'isolamento di una macchina infetta e la possibilità di raggiungere la rete interna dalla DMZ.

Ecco perché un WAF potrebbe essere adottato in questa situazione:

Filtraggio e Monitoraggio del Traffico: Un WAF agisce come un filtro tra la DMZ e la rete interna, controllando il traffico in entrata e in uscita. Può identificare e bloccare le potenziali minacce, inclusi gli attacchi DDoS, tentativi di infiltrazione o traffico malevolo.

Protezione della DMZ: Nel contesto di un'eventuale compromissione di un server nella DMZ, il WAF può essere configurato per bloccare o rilevare attività sospette, limitando l'espansione dell'attacco oltre la DMZ stessa.

Mitigazione degli Attacchi di Applicazioni Web: Considerando il contesto in cui la DMZ può ospitare servizi esposti a Internet, un WAF è particolarmente utile per proteggere tali servizi da attacchi di applicazioni web, come quelli che sfruttano vulnerabilità nei codici delle applicazioni.

Controllo degli Accessi: Un WAF può contribuire a implementare politiche di controllo degli accessi, limitando le comunicazioni tra la DMZ e la rete interna solo a quelle strettamente necessarie per il funzionamento dei servizi nella DMZ.

CONCLUSIONE

In sostanza, l'adozione di un WAF mira a rafforzare la sicurezza della DMZ, limitare la potenziale esposizione degli asset interni e proteggere le applicazioni web dalla gamma di attacchi che possono essere rivolti verso di esse.