Progetto S9-L5

Difesa da attacchi esterni

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

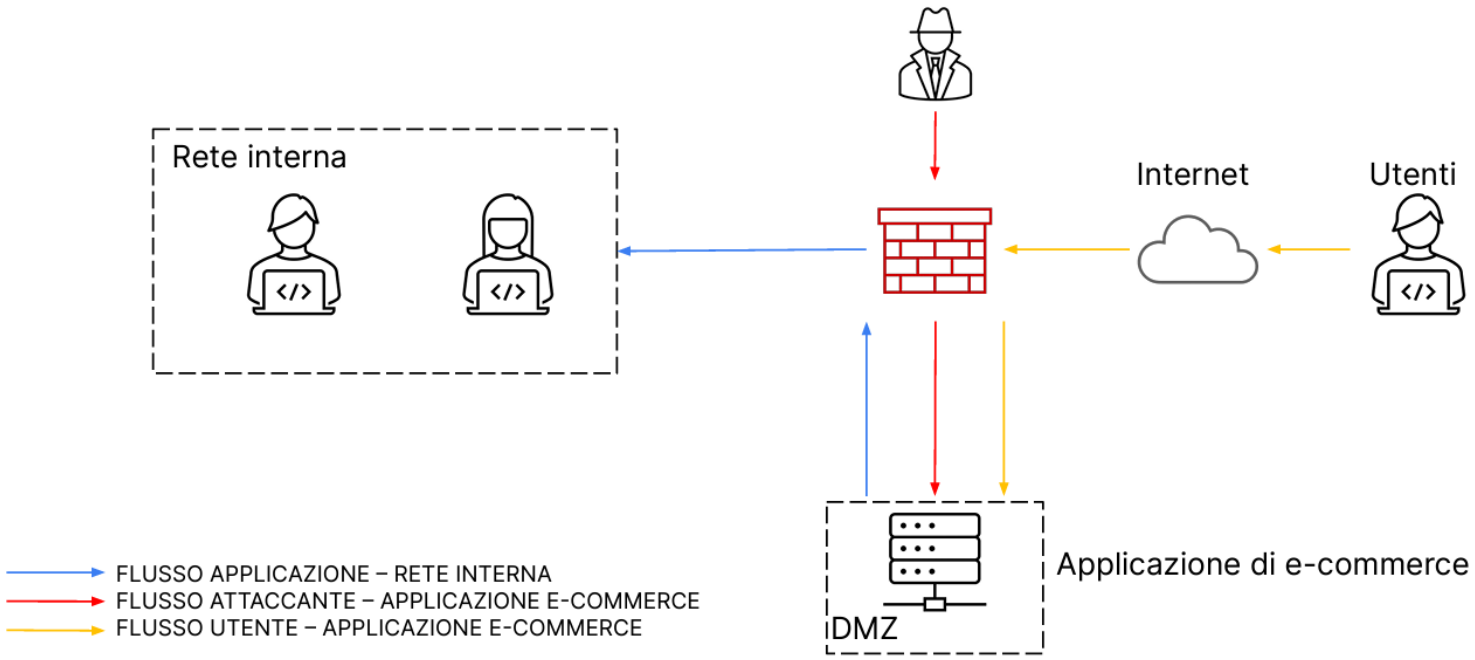
Impatti sul business: l'applicazione Web subisce un attacco di tipo Ddos dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma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

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.

Traccia

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.



Traccia

Per la difesa da attacchi di tipo SQLi e XSS ci sono diverse azioni preventive che si possono implementare:

Validazione dei dati di input: Implementare una corretta validazione dei dati di input per garantire che solo informazioni conformi alle aspettative vengano accettate.

Principio del privilegio minimo: Limitare i privilegi dei database account assegnando loro solo i minimi necessari.

Validazione: Implementare una solida validazione lato server per filtrare e rifiutare dati non validi. Utilizzare escape dei dati di output per prevenire l'esecuzione di script dannosi, assicurando che i dati visualizzati siano privi di potenziali minacce.

Web Application firewall: Questo componente filtra il traffico in arrivo e in uscita, consentendo solo comunicazioni autorizzate e utilizzando whitelist e blacklist per gestire l'accesso.

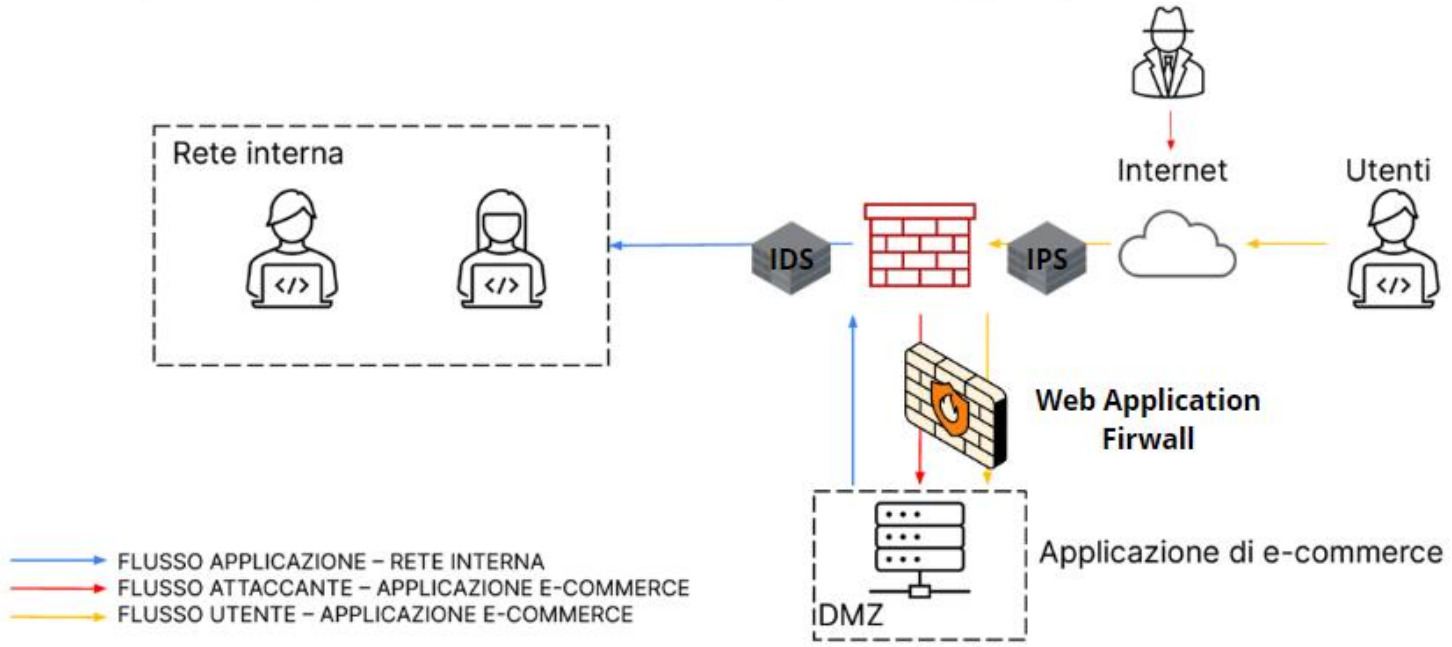
Sistemi IDS e IPS: contribuisce a monitorare il traffico di rete in tempo reale. Gli IDS individuano pattern anomali o comportamenti sospetti, mentre gli IPS intervengono attivamente per prevenire o mitigare gli attacchi, migliorando così la resistenza dell'applicazione web contro minacce potenziali.

Implementazione sistemi di sicurezza

Supponendo che l'attacco provenga dall'esterno, una soluzione ottimale consisterebbe nell'implementare un IPS per prevenire possibili minacce, affiancato da un IDS per rilevarle e comunicarle all'intera rete. Aggiungere un firewall dedicato all'applicazione di e-commerce posizionato nella DMZ aumenta ulteriormente la sicurezza complessiva del sistema.

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.



Impatto sul businees

Se l'applicazione Web, considerando che gli utenti spendono 1.500 € al minuto sulla piattaforma di e-commerce, risultasse non disponibile per 10 minuti, l'impatto negativo sul business può essere calcolato utilizzando la seguente formula:

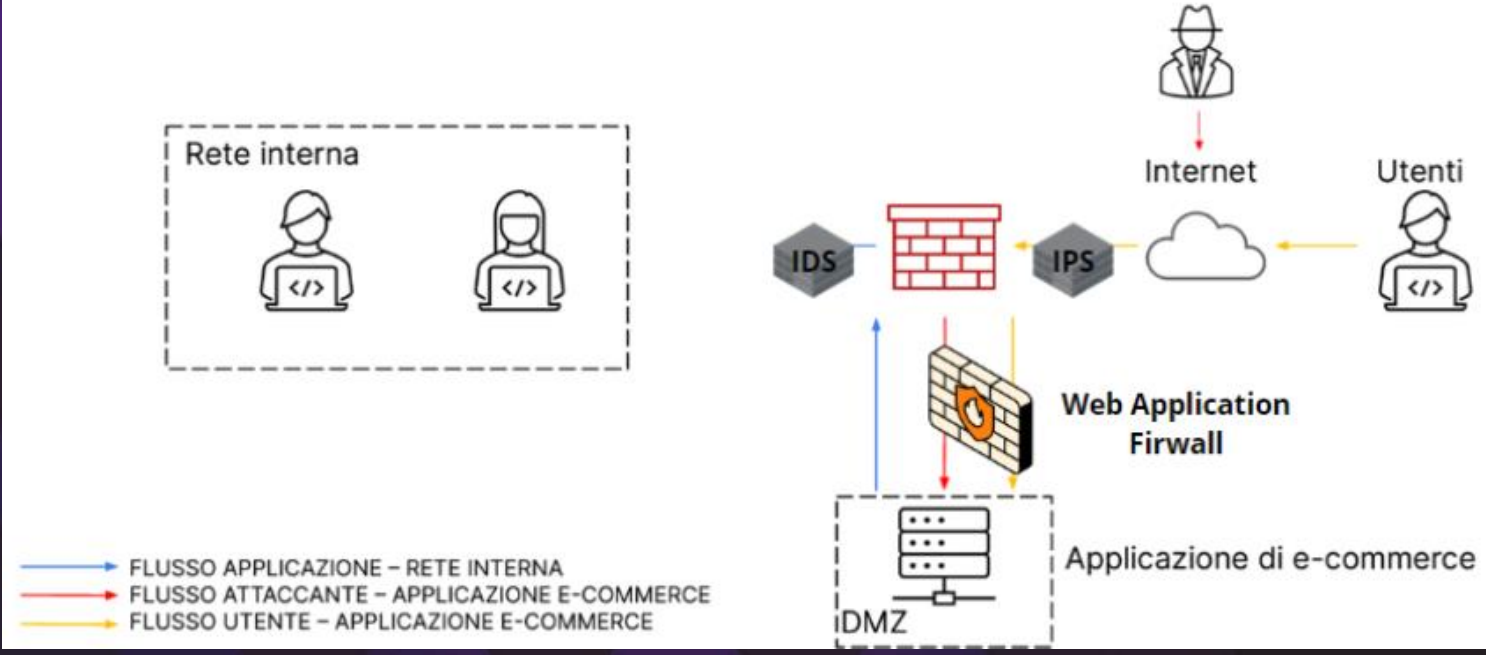
Impatto sul business = 1.500 € x 10 minuti = 15.000 €.

Response

In caso di infezione da malware nell'applicazione di e-commerce, una strategia cruciale per proteggere la rete interna è isolare immediatamente l'applicazione dal resto della rete. Questo isolamento garantisce che il malware non possa diffondersi ad altri segmenti della rete, limitando così l'impatto e consentendo di contenere e gestire più efficacemente l'incidente di sicurezza.

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.



Fine del progetto

Presentazione di Amedeo Natalizi