1. Azioni preventive

Per difendere l'applicazione web da attacchi SQLi (SQL Injection) e XSS (Cross-Site Scripting) da parte di utenti malintenzionati, si possono implementare diverse azioni preventive. Ecco un elenco più dettagliato delle azioni preventive:

- WAF (Web Application Firewall): Un WAF monitora e filtra il traffico HTTP verso l'applicazione web, identificando e bloccando i tentativi di attacco SQLi e XSS. Può essere configurato per riconoscere e mitigare le firme di attacco comuni e proteggere l'applicazione da richieste malevole.

- Sanificazione degli input: È essenziale filtrare e sanificare tutti gli input forniti dagli utenti prima di processarli. Questo può essere fatto utilizzando funzioni di escape e validazione che rimuovono o neutralizzano i caratteri dannosi.

- Utilizzo di tecniche di codifica. Quando si visualizzano input utente nelle pagine web, è importante applicare codifiche appropriate (come HTML encoding) per prevenire l'esecuzione di script dannosi.

- Aggiornamento del software: Mantenere aggiornato tutto il software utilizzato nell'applicazione, inclusi framework, librerie e server, per assicurarsi di avere le ultime patch di sicurezza che correggono vulnerabilità note.

- Security Headers: Configurare header HTTP di sicurezza, come Content Security Policy (CSP), X-Content-Type-Options, X-Frame-Options e altri, per prevenire vari tipi di attacchi.

Modifica della figura

- Aggiungi un WAF tra il firewall e l'applicazione di e-commerce per mostrare la protezione aggiuntiva.

- Inserisci una rappresentazione grafica della sanificazione degli input nel percorso dei dati tra gli utenti e l'applicazione web.

2. Impatti sul business

Considerando un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, il calcolo dell'impatto economico sarà:

{Perdita economica} = {Tempo di inattività} \times \{Spesa media al minuto}

Dove la spesa media al minuto è di 1.500€:

{Perdita economica} = 10 \text{ minuti} \times 1.500 \text{ €/minuto} = 15.000 € \]

Azione preventiva:

- CDN (Content Delivery Network): Utilizzare una CDN distribuisce il traffico e aiuta a mitigare gli attacchi DDoS riducendo il carico sul server principale.

- Protezione DDoS: Implementare soluzioni di protezione DDoS che possono rilevare e mitigare automaticamente gli attacchi, mantenendo l'applicazione disponibile anche sotto attacco.

3. Response

In caso di infezione da malware, la priorità è impedire che il malware si propaghi sulla rete. Le azioni immediate da prendere includono:

- Isolamento del server infetto: Rimuovere immediatamente il server compromesso dalla rete per evitare la propagazione del malware ad altri sistemi.

- Scansione e pulizia: Eseguire una scansione approfondita del server utilizzando strumenti antivirus e antimalware per identificare e rimuovere il malware.

- Analisi forense: Condurre un'indagine dettagliata per determinare l'origine e il vettore dell'infezione, al fine di prevenire future violazioni.

Modifica della figura

- Aggiungi una rappresentazione dell'isolamento del server infetto, come una linea rossa che lo separa dalla rete interna.
- Inserisci simboli per la scansione antivirus e l'analisi forense accanto al server infetto.

4. Soluzione completa

Unendo le soluzioni preventive (punto 1) e di risposta (punto 3), si ottiene una strategia robusta per proteggere l'applicazione e rispondere agli incidenti:

- **Implementa un WAF e pratiche di sanificazione degli input** per prevenire attacchi SQLi e XSS.
- **Utilizza una CDN e protezione DDoS** per mitigare gli attacchi DDoS.
- **Isola e pulisci rapidamente i server infetti** per prevenire la propagazione del malware.

5. Modifica più aggressiva dell'infrastruttura

Per rendere l'infrastruttura più resiliente, si possono adottare ulteriori misure:

- **Segmentazione della rete**: Implementare una segmentazione della rete per limitare l'accesso tra diverse sezioni della rete e contenere eventuali compromissioni.
- **Replica geografica**: Avere server di backup in diverse location geografiche per garantire la disponibilità dell'applicazione anche in caso di attacco DDoS o disastri naturali.
- **Monitoraggio continuo**: Implementare sistemi di monitoraggio continuo che rilevino anomalie e possano avvisare gli amministratori di sicurezza in tempo reale.

Con queste soluzioni, l'applicazione di e-commerce sarà ben protetta contro vari tipi di minacce, garantendo la continuità operativa e minimizzando l'impatto di eventuali incidenti di sicurezza.