Progetto M5

Fabrizio Meini

1. Azioni preventive contro SQLi e XSS

Per proteggere l'applicazione Web da attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS), si possono implementare le seguenti azioni preventive:

-Prevenzione SQLi:

Utilizzo di prepared statements e query parametrizzate.
Validazione e sanificazione degli input da parte degli utenti.
Utilizzo di ORM (Object-Relational Mapping) per l'interazione con il database.
Implementazione di un Web Application Firewall (WAF) per bloccare richieste sospette.

-Prevenzione XSS:

Escaping di output HTML.
Content Security Policy (CSP) per limitare le fonti di script.
Validazione e sanificazione degli input da parte degli utenti.
Implementazione di un Web Application Firewall (WAF) per bloccare richieste sospette.

2. Impatti sul business di un attacco DDoS

Se l'applicazione Web subisce un attacco DDoS che la rende non raggiungibile per 10 minuti, l'impatto economico può essere calcolato come segue:

Media spesa degli utenti per minuto: 1.500 €
Durata dell'inaccessibilità: 10 minuti
Impatto sul business: 1.500 € * 10 minuti = 15.000 €

-Azioni preventive contro DDoS:

Implementazione di soluzioni di mitigazione DDoS come servizi di protezione cloud-based.
Utilizzo di load balancer per distribuire il traffico e ridurre il carico su un singolo punto.
Implementazione di rate limiting per limitare il numero di richieste per utente.
Monitoraggio continuo del traffico di rete e risposta automatica a picchi sospetti.

3. Response in caso di infezione da malware
Se l'applicazione Web viene infettata da un malware, la priorità è impedire la propagazione sulla rete interna. La soluzione proposta include:

Isolamento del server infetto nella DMZ.
Implementazione di segmentazione di rete per limitare la comunicazione tra la DMZ e la rete interna.
Utilizzo di firewall con policy restrittive per bloccare il traffico non autorizzato.
Monitoraggio continuo del traffico e dei log per identificare attività sospette.

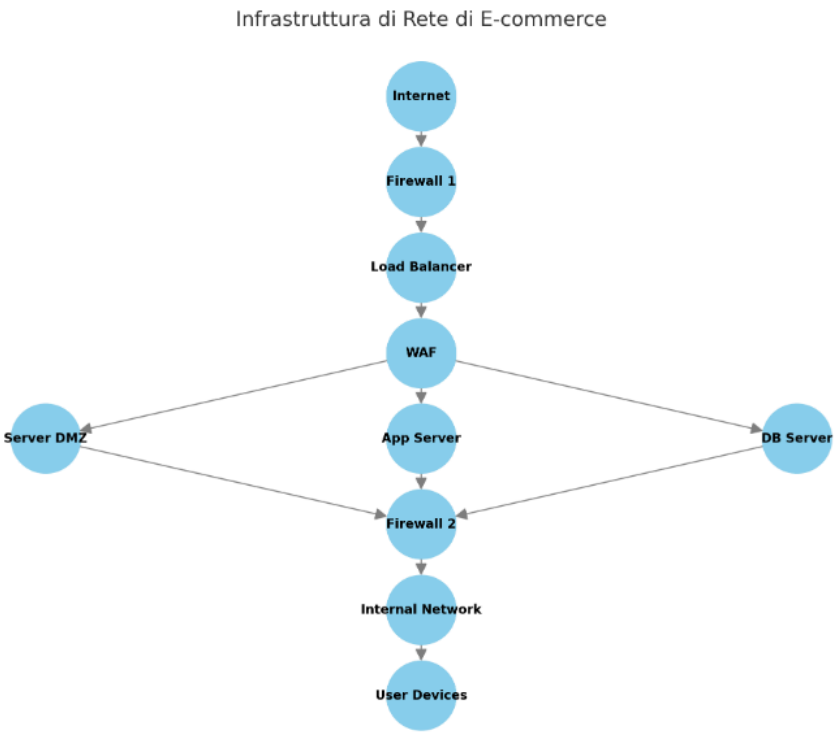
4. Soluzione completa (unione delle azioni preventive e di response)
Combiniamo le soluzioni preventive contro SQLi e XSS con la strategia di response in caso di infezione da malware:

Isolamento del server infetto nella DMZ.
Segmentazione della rete con firewall e policy restrittive.
Implementazione di prepared statements, escaping di output HTML, CSP e WAF.
Monitoraggio continuo del traffico di rete e dei log.

5. Modifica più aggressiva dell'infrastruttura (integrazione della soluzione al punto 2)
Per migliorare ulteriormente la sicurezza e includere la prevenzione contro DDoS:

Implementazione di soluzioni di mitigazione DDoS.
Segmentazione di rete avanzata con VLAN e firewall.
Utilizzo di load balancer e rate limiting.
Monitoraggio e risposta automatizzata ai picchi di traffico sospetti.
Aggiunta di un sistema di rilevamento delle intrusioni (IDS) e un sistema di prevenzione delle intrusioni (IPS).

Immagine aggiornata con le implementazioni:



Internet: Punto di ingresso per gli utenti.
Firewall 1: Protezione iniziale della rete.
Load Balancer: Distribuzione del traffico.
WAF (Web Application Firewall): Protezione contro SQLi e XSS.
Server DMZ: Isolato per limitare la propagazione del malware.
App Server: Server dell'applicazione.
DB Server: Server del database.
Firewall 2: Ulteriore protezione tra la DMZ e la rete interna.
Internal Network: Rete interna aziendale.
User Devices: Dispositivi degli utenti interni.