Esercizio di Fine Modulo – M5- SECURITY OPERATION

Report di Daniele Renga

1. Azioni preventive – Protezione da SQLi e XSS

Per prevenire attacchi di tipo SQL injection (SQLi) e Cross-Site Scripting (XSS) all'interno dell'applicazione e-commerce, propongo le seguenti azioni tecniche:

- Web Application Firewall (WAF): posizionato tra Internet e il server dell'applicazione, in grado di filtrare e bloccare richieste malevole contenenti payload sospetti.

- Validazione e sanitizzazione degli input: da implementare a livello di codice per impedire che vengano eseguiti script o query dannose.

- ModSecurity: modulo open-source integrabile con Apache/Nginx per difesa automatica da vulnerabilità comuni.

- Aggiornamenti software regolari: per ridurre le vulnerabilità dovute a versioni obsolete.

- Controllo degli accessi: per limitare l'accesso alle aree critiche dell'app solo a utenti autorizzati.

Modifica architettura: aggiunta di un WAF tra firewall e server web.

2. Impatti sul business – DDoS

Scenario: un attacco DDoS blocca l'e-commerce per 10 minuti.

Perdita stimata: 10 minuti × 1.500 €/minuto = 15.000 €

Azioni preventive consigliate:

- CDN con protezione DDoS (es. Cloudflare): per mitigare il traffico prima che raggiunga il server.

- Rate Limiting sul WAF: per bloccare richieste ripetute dallo stesso IP.

- Firewall avanzato con regole dedicate al filtraggio del traffico.

- IDS/IPS per rilevamento e blocco attacchi volumetrici o anomali.

Modifica architettura: inserimento di una CDN/Anti-DDoS tra Internet e il firewall, più configurazione di regole di protezione.

3. Response – Malware

Scenario: un malware compromette il server e-commerce.

Azioni da eseguire:

- Segmentazione della rete (DMZ): il server e-commerce deve essere isolato dalla rete interna.

- Network Isolation immediata del server infetto.

- EDR/Antivirus installato sul server per analisi e contenimento.

- Firewall in uscita configurato per bloccare comunicazioni verso IP sospetti (es. C2 server).

Modifica architettura: Blocco del traffico dal server e-commerce verso la rete interna. Comunicazioni consentite solo per logging e monitoraggio.

4. Soluzione completa – Design finale

La soluzione finale prevede:

- WAF per difesa da SQLi e XSS

- CDN + firewall avanzato per difesa contro DDoS

- IDS/IPS per rilevamento intrusioni

- DMZ isolata per contenere compromissioni

- Logging centralizzato e controllo accessi

- Comunicazioni minime e controllate tra DMZ e rete interna

5. Modifica “più aggressiva” – Sicurezza avanzata

Per aumentare ulteriormente la sicurezza:

- Reverse Proxy tra client e server web

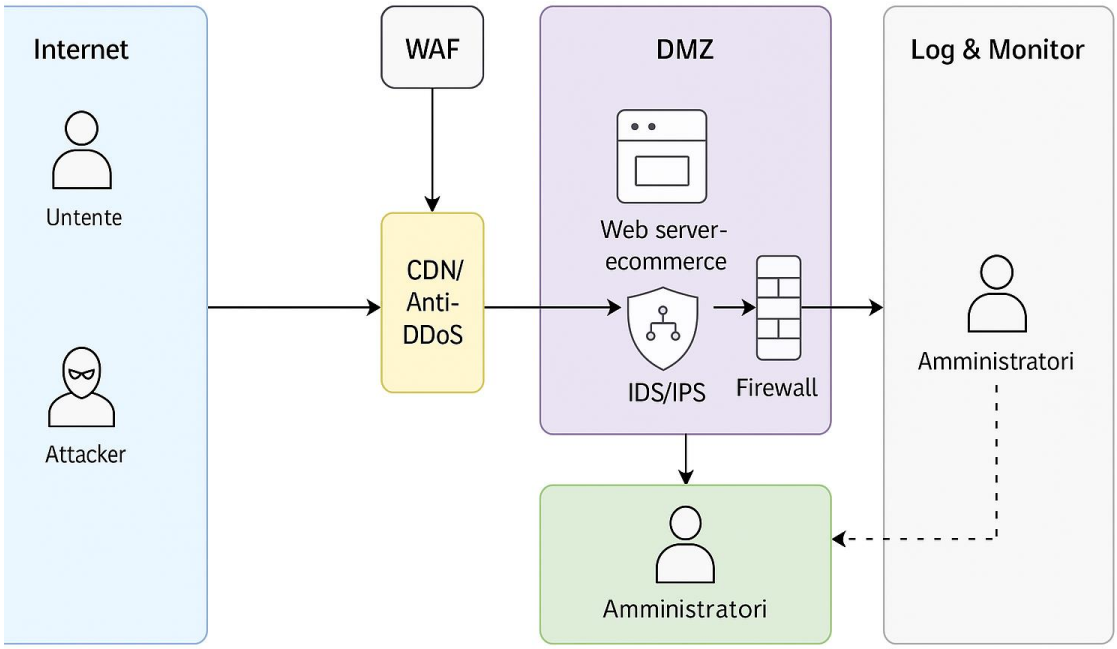
- Accesso amministrativo solo da IP autorizzati

- Alta disponibilità (HA): server in cluster e load balancer

- Zero Trust Network: ogni componente deve autenticarsi per comunicare

Allegato: Schema Architettura di Sicurezza

Lo schema che segue rappresenta graficamente l’architettura di rete proposta nel report.


Internet
Untente
Attacker
WAF
CDN/
Anti-
DDoS
DMZ
Web server-
ecommerce
IDS/IPS
Firewall
Amministratori
Log & Monitor
Amministratori