EPICODE

Esercizio
Traccia e requisiti

Traccia:

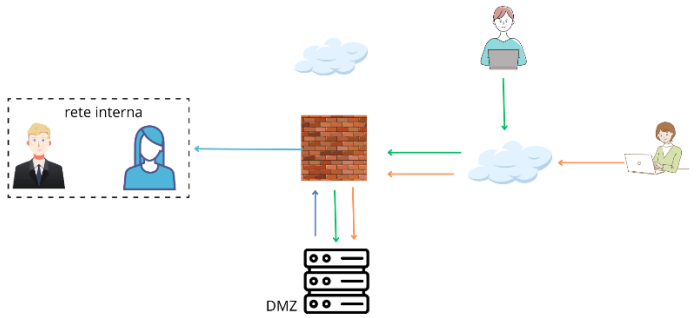
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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. **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**
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.
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

2

1. Architettura di Rete

L'architettura di rete per un'applicazione di e-commerce deve garantire accesso sicuro e disponibilità continua per gli utenti tramite Internet, proteggendo al contempo la rete interna da potenziali attacchi. L'applicazione e-commerce è disponibile su Internet per consentire agli utenti di effettuare acquisti. Tuttavia, la rete interna è raggiungibile dalla DMZ a causa delle policy del firewall, il che significa che se il server nella DMZ viene compromesso, un attaccante potrebbe potenzialmente raggiungere la rete interna.



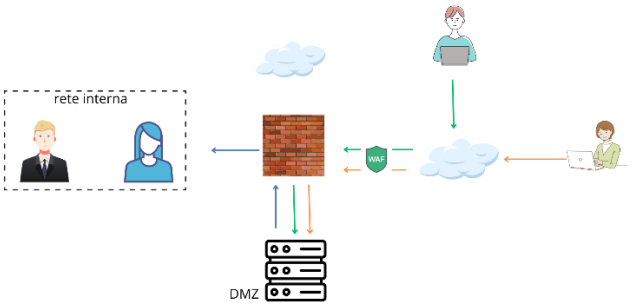
2. Azioni Preventive

2.1. Protezione contro SQLi e XSS

Per difendere l'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), sono necessarie diverse azioni preventive:

1. **Web Application Firewall (WAF)** Implementare un WAF per proteggere l'applicazione da attacchi SQLi e XSS. Il WAF filtra e monitora il traffico HTTP tra la web application e Internet, bloccando le richieste dannose.
2. **Validazione e Sanitizzazione degli Input** Assicurarsi che tutti gli input forniti dagli utenti siano validati e sanificati sia lato client che lato server. Accettare solo input che soddisfano criteri specifici e rimuovere o codificare caratteri speciali che potrebbero essere utilizzati in attacchi SQLi o XSS.
3. **Utilizzo di HTTPS** Utilizzare HTTPS per criptare il traffico tra il client e il server, proteggendo i dati in transito.

4. **Aggiornamenti e Patch di Sicurezza** Mantenere l'applicazione e il suo ambiente (server, database, framework, ecc.) aggiornati con le ultime patch di sicurezza per prevenire attacchi che sfruttano bug o vulnerabilità note.
5. **Formazione del Personale** Formare sviluppatori e personale interno sulle best practice di programmazione sicura e sui rischi di sicurezza comuni come SQLi e XSS.
6. **Limitazione dei Privilegi** Le connessioni al database dovrebbero utilizzare account con il minimo livello di privilegi necessario per svolgere il lavoro.
7. **Logging e Monitoraggio** Mantenere log dettagliati delle attività e monitorare le applicazioni e i sistemi per individuare e reagire rapidamente a qualsiasi attività sospetta o minacce.
8. **Assessment di Vulnerabilità** Condurre regolari campagne di vulnerability assessment e penetration testing per scoprire eventuali falle e porvi rimedio prima che possano essere sfruttate da malintenzionati.



Link Utili:

- OWASP SQL Injection Prevention Cheat Sheet
- OWASP XSS Prevention Cheat Sheet

3. Impatti sul Business

3.1. Calcolo dell'Impatto

Un attacco DDoS può rendere l'applicazione non raggiungibile per 10 minuti, con una perdita stimata di €15.000. Questo calcolo si basa sulla media di €1.500 spesi dagli utenti ogni minuto sulla piattaforma.

Perdita=€1.500/minuto×10minuti=€15.000 Perdita = €1.500/minuto \times 10 minuti = €15.000Perdita=€15.000/minuto×10minuti=€15.000

Immaginando uno scenario con 8 attacchi DDoS all'anno, la perdita annua sarebbe di €120.000.

3.2. Azioni Preventive

1. **Content Delivery Network (CDN)** Utilizzare una CDN come Cloudflare per distribuire il carico di traffico su server globalmente distribuiti, riducendo il rischio di sovraccarico del server principale durante un attacco DDoS.

2. **Miglioramento dell'Infrastruttura** Implementare server multipli e sistemi di failover per garantire la continuità operativa anche durante un attacco. Un sistema di failover promuove un altro server a server principale in caso di guasto del server originale.

Link Utili:

- Cloudflare DDoS Protection
- ENISA Threat Landscape for DoS Attacks

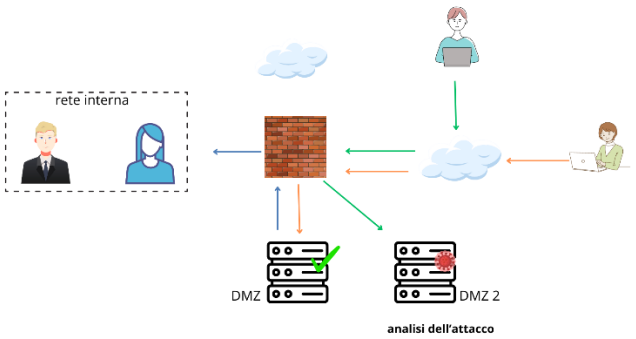
4. Response

4.1. Isolamento del Server Infetto

In caso di infezione da malware, isolare il server infetto dalla rete interna e metterlo in una rete di quarantena con accesso limitato. Ciò consente di studiare l'attacco senza rischiare la propagazione del malware.

4.2. Ripristino del Servizio

Ripristinare il sito su un nuovo server utilizzando backup recenti. Configurare le impostazioni DNS per puntare al nuovo server e implementare misure di hardening del sistema per prevenire ulteriori attacchi.



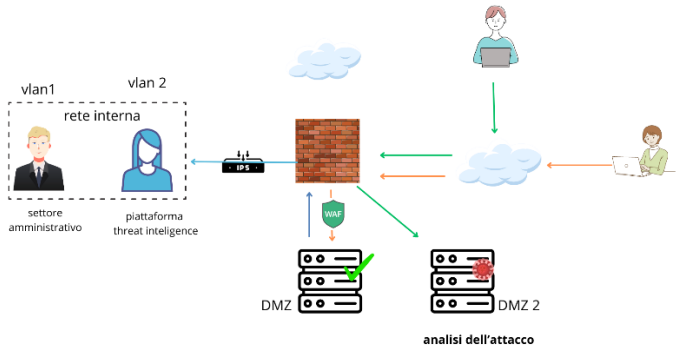
Link Utili:

- IBM Security SIEM

5. Soluzione Completa

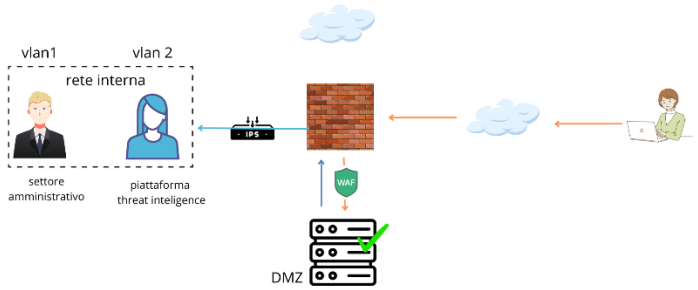
Unire le azioni preventive e le risposte agli incidenti per creare una strategia di sicurezza integrata:

1. **Protezione del Nuovo Server** Implementare un WAF e condurre campagne di vulnerability assessment e penetration testing per il miglioramento continuo del sito.
2. **Policy di Firewall e IPS** Creare policy di firewall adeguate e implementare un IPS per proteggere la rete interna da intrusioni provenienti dalla DMZ.
3. **Threat Intelligence** Utilizzare una piattaforma di Threat Intelligence per ottenere informazioni aggiornate sulle minacce.



6. Modifica Aggressiva dell'Infrastruttura

Se il server infettato è compromesso e dichiarato inaffidabile, rimuoverlo fisicamente dalla rete e distruggere i dischi prima dello smaltimento mediante metodi adeguati. Considerare l'adozione di soluzioni di Disaster Recovery as a Service (DRaaS) per garantire la continuità operativa.



Link Utili:

- Disaster Recovery as a Service (DRaaS)