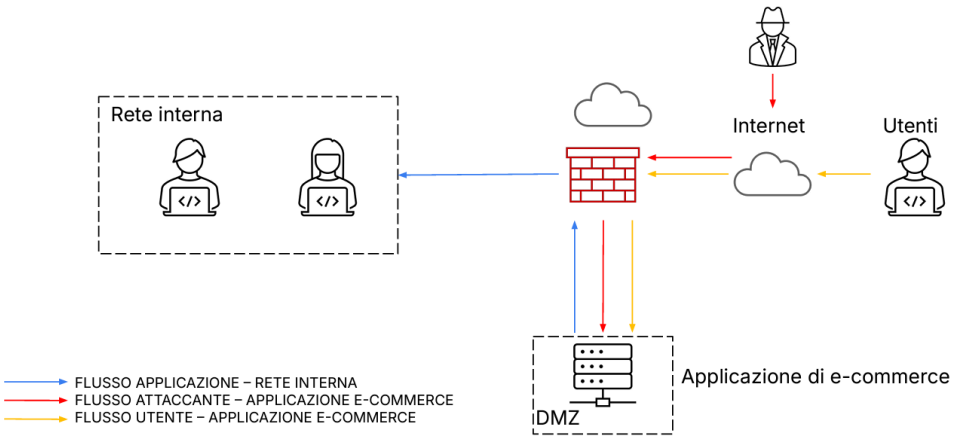
Traccia:

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



1. Azioni preventive contro SQLi e XSS

A. Web Application Firewall (WAF)

Per proteggere l'applicazione di e-commerce dagli attacchi di SQL injection (SQLi) e Cross-Site Scripting (XSS), un primo passo è l'implementazione di un Web Application Firewall (WAF). Posizionando il WAF tra Internet e la DMZ, dove si trova l'applicazione, possiamo filtrare e bloccare in tempo reale le richieste dannose. È importante configurare il WAF con regole specifiche per identificare e neutralizzare questi tipi di attacco. Inoltre, monitorare costantemente il traffico può aiutare a rilevare schemi anomali che potrebbero indicare tentativi di attacco.

B. Cifratura SSL/TLS

La cifratura delle comunicazioni è un altro aspetto cruciale. Implementando un certificato SSL valido, garantisce che le comunicazioni tra gli utenti e il server dell'e-commerce siano protette da potenziali attacchi, come quelli di tipo man-in-the-middle (MITM). È consigliabile forzare l'uso di HTTPS, reindirizzando automaticamente gli utenti che tentano di accedere tramite HTTP.

C. Validazione dell'input

Un passo importante nella prevenzione è la validazione dell'input. È fondamentale implementare controlli di validazione sia sul lato client che sul lato server, assicurandosi che i dati inseriti dagli utenti siano corretti e sicuri. Inoltre, applicare tecniche di sanitizzazione sui dati ricevuti può prevenire l'esecuzione di codice malevolo, proteggendo ulteriormente l'applicazione.

D. Limitazione dei permessi

Adottare il principio del minimo privilegio è essenziale. Assicurarsi che le applicazioni abbiano solo i permessi necessari per funzionare, riducendo così il rischio di accesso non autorizzato a dati sensibili.

E. Educazione e formazione

Offrire corsi di formazione per gli sviluppatori su pratiche di codifica sicura e sulle vulnerabilità comuni può fare la differenza nella protezione dell'applicazione.

---

2. Impatti sul business per un attacco DDoS

A. Content Delivery Network (CDN)

In caso di attacco DDoS, un'azione preventiva efficace è l'implementazione di una Content Delivery Network (CDN). Utilizzando una CDN, possiamo distribuire il traffico in modo da alleviare il carico sui server e ridurre l'impatto degli attacchi DDoS. La CDN funge da scudo, assorbendo le richieste in eccesso.

B. Rate Limiting

In aggiunta, è possibile implementare politiche di rate limiting. Questo significa limitare il numero di richieste che un singolo utente può fare in un breve intervallo di tempo, riducendo il rischio di sovraccarico del sistema.

C. Protezione DDoS avanzata

Affidarsi a servizi specializzati per la protezione DDoS è un'altra misura efficace. Questi servizi analizzano e filtrano il traffico in arrivo, bloccando automaticamente gli attacchi dannosi.

D. Ridondanza e failover

Un'architettura ridondante, con server in cluster o in modalità di failover. In caso di sovraccarico di un server, altri possono subentrare, garantendo così la continuità del servizio.

E. Monitoraggio attivo

Implementare strumenti di monitoraggio del traffico in tempo reale ci permette di rilevare picchi anomali che potrebbero segnalare un attacco DDoS in corso, consentendo di rispondere rapidamente.

---

3. Response in caso di infezione malware

A. Segmentazione della rete

La segmentazione della rete è cruciale per isolare la DMZ dalla rete interna. Aggiungere un firewall con regole di accesso rigide tra la DMZ e la rete interna aiuta a prevenire la propagazione del malware in caso di compromissione.

B. Backup regolari

Eseguire regolarmente backup dei dati è una buona prassi. In caso di infezione, avere backup recenti ci consente di ripristinare i dati senza perdite significative.

C. Piani di risposta agli incidenti

È importante avere un piano di risposta agli incidenti ben documentato. Questo piano dovrebbe delineare i passaggi da seguire in caso di compromissione, compresa la disconnessione temporanea del server compromesso.

D. Antivirus e anti-malware

Implementare soluzioni antivirus e anti-malware nella DMZ e nella rete interna è fondamentale per monitorare e rimuovere minacce note.

E. Audit di sicurezza

Infine, eseguire audit di sicurezza periodici ci consente di identificare vulnerabilità e valutare l'efficacia delle misure di sicurezza in atto.

---

4. Soluzione completa**(Immagine '*soluzione completa'* allegata a fine report)**

A. Integrazione delle misure di sicurezza

Unendo tutte queste misure di sicurezza il WAF, il firewall, la CDN e gli IDS si integrino per formare una rete sicura e protetta. Ogni componente deve essere chiaramente definito, evidenziando l'interconnessione tra di essi.

B. Monitoraggio e logging

Implementare un sistema di logging centralizzato per monitorare accessi e attività nella rete è fondamentale per l'analisi di eventuali incidenti di sicurezza. Questo ci permette di avere una visione chiara e dettagliata su ciò che accade nel nostro ambiente.

C. Test di penetrazione

Condurre test di penetrazione regolari aiuta a identificare vulnerabilità nell'infrastruttura e a valutare l'efficacia delle misure di sicurezza adottate. Questi test possono rivelare falle che potrebbero essere sfruttate da un attaccante.

5. Modifica "più aggressiva"

A. Approccio Zero Trust

Adottare un approccio Zero Trust implica applicare controlli di accesso rigorosi per ogni componente della rete. Ogni richiesta deve essere autenticata e autorizzata, garantendo un livello di sicurezza molto elevato.

B. Autenticazione multi-fattore (MFA)

L'implementazione dell'autenticazione multi-fattore per accedere a sistemi sensibili è un altro passo fondamentale. Questo riduce notevolmente il rischio di accesso non autorizzato.

C. Micro-segmentazione

La micro-segmentazione della rete permette di suddividere ulteriormente la rete in micro-segmenti. Questo limita l'accesso e riduce il rischio di movimenti laterali nel caso in cui un attaccante riesca a compromettere un'area della rete.

D. Controlli di accesso basati su ruoli (RBAC)

Adottare controlli di accesso basati su ruoli aiuta a garantire che gli utenti abbiano accesso solo alle risorse necessarie per svolgere le proprie funzioni, limitando ulteriormente il rischio di accessi non autorizzati.

E. Formazione continua

Infine, offrire programmi di formazione continua sulla sicurezza informatica per il personale è fondamentale. Questi corsi possono includere simulacri di attacchi di phishing e tecniche di ingegneria sociale per sensibilizzare il personale e migliorare la resilienza dell'organizzazione.

A seguire un'immagine con alcune implementazioni applicate: