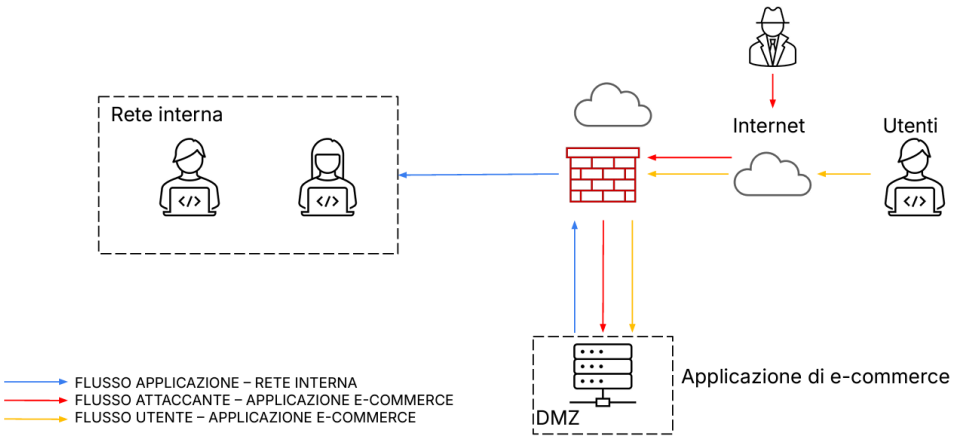
Traccia:
Con riferimento alla figura in slide, rispondere ai seguenti quesiti.



1. Azioni preventive contro SQLi e XSS

A. Web Application Firewall (WAF)
Per proteggere il sito di e-commerce da attacchi come SQL injection (SQLi) e Cross-Site Scripting (XSS), il primo passo è l'implementazione di un Web Application Firewall (WAF). Posizionando il WAF tra Internet e la DMZ, dove risiede l'applicazione, possiamo monitorare e bloccare in tempo reale le richieste sospette o dannose. È importante configurare il WAF con regole precise per riconoscere e neutralizzare questi attacchi. Inoltre, un monitoraggio costante del traffico aiuta a identificare comportamenti anomali che potrebbero segnalare tentativi di intrusione.

B. Cifratura SSL/TLS
La protezione delle comunicazioni tra gli utenti e il server è essenziale. Implementando un certificato SSL/TLS, garantiamo che i dati siano cifrati, prevenendo attacchi come il man-in-the-middle (MITM). È consigliabile obbligare l'uso di HTTPS, reindirizzando automaticamente qualsiasi tentativo di accesso tramite HTTP, per assicurare che tutte le comunicazioni siano sicure.

C. Validazione dell'input
Un'altra misura cruciale è la validazione dei dati inseriti dagli utenti. È importante implementare controlli sia lato client che lato server per verificare che i dati siano corretti e sicuri. Inoltre, la sanitizzazione dei dati può prevenire l'esecuzione di codice malevolo, aggiungendo un ulteriore livello di protezione all'applicazione.

D. Limitazione dei permessi
Adottare il principio del minimo privilegio riduce i rischi legati all'accesso non autorizzato. Ogni componente dell'applicazione deve avere accesso solo alle risorse strettamente necessarie al suo funzionamento, evitando così potenziali danni in caso di compromissione.

E. Educazione e formazione
Formare gli sviluppatori su pratiche di programmazione sicura è un fattore chiave per prevenire vulnerabilità come SQLi e XSS. Offrire corsi su come evitare questi errori può aumentare notevolmente la sicurezza dell'applicazione.

---

2. Impatti sul business per un attacco DDoS

A. Content Delivery Network (CDN)
Un modo efficace per mitigare gli attacchi DDoS è implementare una CDN. Distribuendo il traffico su più server, una CDN può ridurre il carico su quelli principali, limitando gli effetti di un sovraccarico dovuto a un attacco. La CDN agisce come uno "scudo", assorbendo l'eccesso di richieste.

B. Rate Limiting
Un'altra misura preventiva consiste nell'implementare politiche di **rate limiting**, che limitano il numero di richieste che ogni utente può inviare in un determinato intervallo di tempo, riducendo il rischio di sovraccarico.

C. Protezione DDoS avanzata
Affidarsi a servizi specializzati per la protezione DDoS può offrire una difesa ancora più efficace. Questi servizi analizzano il traffico in tempo reale, filtrando automaticamente gli attacchi prima che raggiungano i server.

D. Ridondanza e failover
Un'architettura ridondante è fondamentale per garantire la continuità del servizio. In caso di sovraccarico su un server, altri server possono subentrare, riducendo così l'impatto di un attacco.

E. Monitoraggio attivo
Strumenti di monitoraggio in tempo reale permettono di individuare picchi anomali di traffico, avvisando in caso di possibili attacchi DDoS. Questo permette di reagire tempestivamente prima che l'attacco diventi critico.

---

3. Risposta in caso di infezione da malware

A. Segmentazione della rete
La segmentazione è fondamentale per limitare la diffusione di un malware. Aggiungere un firewall tra la **DMZ** e la rete interna con regole di accesso rigide può isolare la minaccia, impedendo al malware di diffondersi all'interno della rete aziendale.

B. Backup regolari
Effettuare backup regolari dei dati è una pratica indispensabile. In caso di infezione, poter ripristinare i dati da backup recenti permette di minimizzare le perdite.

C. Piani di risposta agli incidenti
È importante avere un piano di risposta agli incidenti, che includa passaggi chiari da seguire in

caso di compromissione. Questo piano dovrebbe prevedere, tra le altre cose, la possibilità di disconnettere il server infetto per evitare ulteriori danni.

D. Antivirus e anti-malware
Installare e mantenere aggiornate soluzioni antivirus e anti-malware nella **DMZ** e nella rete interna aiuta a identificare e bloccare minacce note prima che possano causare danni.

E. Audit di sicurezza
Eseguire audit di sicurezza periodici permette di identificare vulnerabilità e valutare l'efficacia delle difese attuate, offrendo la possibilità di migliorare costantemente la protezione.

---

4. Soluzione completa (Vedi immagine allegata a fine report)

A. Integrazione delle misure di sicurezza
Un sistema di sicurezza efficace unisce tutte le componenti descritte: **WAF**, **firewall**, **CDN**, **IDS** (Intrusion Detection System) e altro ancora. Ogni elemento della rete deve essere collegato e protetto, con un'architettura chiara e ben definita che rende ogni nodo e percorso sicuro.

B. Monitoraggio e logging
Un sistema di logging centralizzato è indispensabile per tracciare attività e accessi nella rete. Questo aiuta ad analizzare eventuali incidenti di sicurezza e a identificare problemi nel minor tempo possibile.

C. Test di penetrazione
I test di penetrazione simulano attacchi reali per identificare falle nell'infrastruttura. Conducendo test periodici, si possono prevenire exploit che potrebbero essere sfruttati da attaccanti esterni.

---

5. Approccio "più aggressivo"

A. Approccio Zero Trust
Il modello **Zero Trust** è un approccio che non dà per scontato che un'entità sia sicura, anche se è già all'interno della rete. Ogni richiesta, proveniente da utenti o dispositivi, deve essere verificata e autorizzata prima di poter accedere a qualsiasi risorsa.

B. Autenticazione multi-fattore (MFA)
Implementare l'autenticazione multi-fattore (MFA) riduce il rischio di accesso non autorizzato, richiedendo agli utenti di fornire almeno due forme di autenticazione per accedere ai sistemi critici.

C. Micro-segmentazione
La micro-segmentazione suddivide la rete in segmenti ancora più piccoli, limitando il movimento laterale di un eventuale attaccante. Anche se una parte della rete viene compromessa, l'accesso ad altre aree sarà limitato.

D. Controlli di accesso basati su ruoli (RBAC)
I controlli di accesso basati sui ruoli (RBAC) garantiscono che ogni utente possa accedere solo

alle risorse necessarie per svolgere le proprie mansioni, minimizzando il rischio di accesso non autorizzato.

E. Formazione continua
La formazione continua del personale è essenziale per mantenere alta la consapevolezza sui rischi legati alla sicurezza informatica. Simulazioni di attacchi di phishing e scenari di ingegneria sociale possono sensibilizzare i dipendenti, riducendo i rischi per l'azienda.

A seguire un'immagine con alcune implementazioni applicate: