S9-L5

INDICE

Sommario

ESERCIZIO

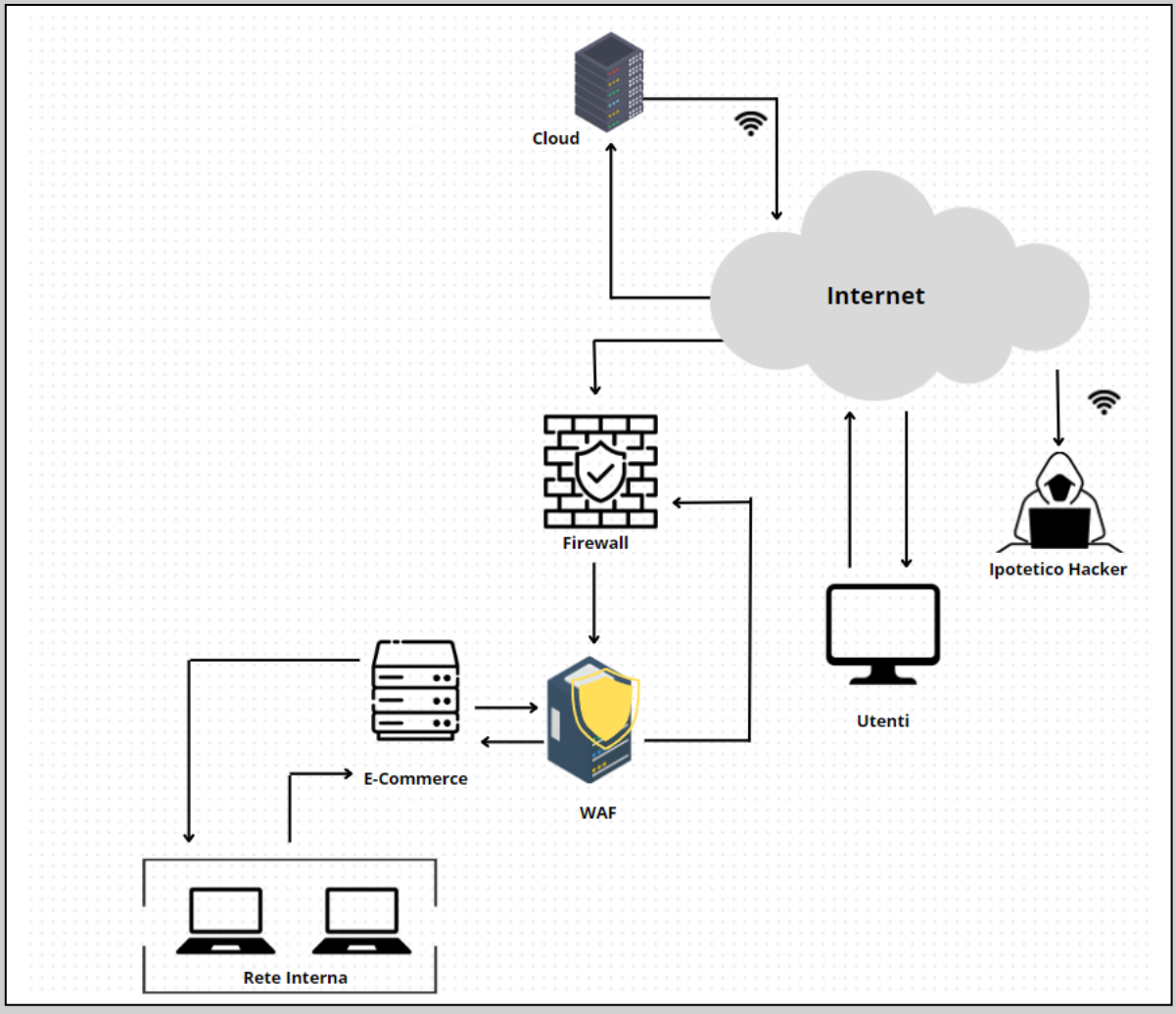
Traccia: Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

- **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
- **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.
- **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

Azioni preventive

Azioni preventive contro attacchi SQLi e XSS:

- **Validazione Input Lato Server:** Assicurarsi che tutti gli input ricevuti dall'applicazione web siano sottoposti a una rigorosa validazione lato server per prevenire l'iniezione di codice SQL e script.
- **Sanitizzazione Input:** Utilizzare funzioni di sanitizzazione per neutralizzare qualsiasi input sospetto prima che sia processato dall'applicazione.
- **Content Security Policy (CSP):** Implementare una CSP per ridurre il rischio di attacchi XSS, specificando quali risorse possono essere caricate dall'applicazione.
- **Preparazione delle Query SQL:** Utilizzare query preparate con parametri legati o ORM (Object-Relational Mapping) che evitano l'uso di stringhe di query SQL costruite dinamicamente.
- **Web Application Firewall (WAF):** Posizionare un WAF nella DMZ per monitorare e filtrare il traffico HTTP/HTTPS sospetto.
- **Aggiornamento e Patching:** Mantenere aggiornati i sistemi e le applicazioni con le ultime patch di sicurezza.
- **Autenticazione e Controllo Accessi:** Rafforzare le politiche di autenticazione e controllo degli accessi per l'accesso alla rete interna dalla DMZ.



IMPATTI SUL BUSINESS ATTACCO DDOS

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.

Impatto = Spesa media al minuto X Durata dell’inattività

Impatto = 1.500 € / minuto X 10 minuti = 15.000 €

RESPONSE

Per affrontare il problema di un'applicazione web infettata da malware, con l'obiettivo di impedire la propagazione del malware nella rete senza necessariamente rimuovere l'accesso all'attaccante, si può adottare una strategia che includa sia misure preventive che reattive. Di seguito, verrà descritta una soluzione proposta che potrebbe essere rappresentata modificando la figura in una slide, illustrando l'architettura di rete modificata.

Architettura di Rete Esistente

Prima di tutto, è importante comprendere l'architettura di rete attuale:

- **DMZ (Demilitarized Zone):** contiene il server dell'applicazione web di e-commerce, accessibile agli utenti Internet.
- **Rete Interna:** contiene risorse critiche dell'azienda, raggiungibili dalla DMZ attraverso policy sul firewall.

Problema

Il server dell'applicazione web nella DMZ è stato compromesso da un malware. Questo espone la rete interna a potenziali rischi, dato che l'attaccante potrebbe sfruttare la connessione tra la DMZ e la rete interna per propagare il malware o per accedere a dati sensibili.

Soluzione Proposta

- **Isolamento del Server Compromesso:**
  Modificare le policy del firewall per isolare il server compromesso, impedendo qualsiasi comunicazione tra il server e la rete interna, ma mantenendo l'accesso a Internet per non interrompere il servizio. Questo impedisce al malware di propagarsi nella rete interna.
- **Monitoraggio e Analisi:**

Implementare soluzioni di monitoraggio e rilevamento delle intrusioni specificamente per il server compromesso per analizzare il comportamento dell'attaccante e del malware. Questo aiuta a capire le tecniche usate senza rimuovere l'accesso all'attaccante.

- **Creazione di una Sandbox:**
  Se possibile, creare una copia del server compromesso in un ambiente sandbox isolato per analizzare il malware in sicurezza. Questo permette di studiare il malware senza rischi per la rete aziendale.
- **Rafforzamento della Segregazione di Rete:**
  Rivedere e rafforzare la segregazione tra la DMZ e la rete interna. Implementare un sistema di prevenzione delle intrusioni (IPS) e un firewall di nuova generazione (NGFW) con capacità di ispezione profonda dei pacchetti (DPI) per un controllo più granulare del traffico.
- **Adozione di un Sistema di Risposta agli Incidenti:**
  Sviluppare o migliorare un piano di risposta agli incidenti di sicurezza informatica che includa procedure specifiche per incidenti simili, garantendo tempi di reazione rapidi e azioni efficaci per mitigare i danni.
- **Formazione e Sensibilizzazione:**
  Organizzare sessioni di formazione per il personale IT su come reagire in caso di compromissione del sistema e come prevenire future infezioni.