PROGETTO S9 L5

1. ***AZIONI PREVENTIVE***
2. ***IMPATTI SUL BUSINESS***
3. ***RESPONSE***

1. AZIONI PREVENTIVE

Alcune azioni preventive che possono essere poste a tutela delle applicazioni web, come l'e-commerce, sono l'inserimento di un ***Web Application Firewall*** tra il firewall e la DMZ, così da tutelare i servizi forniti.
Viene preferito un WAF rispetto ad altre soluzioni in quanto è il firewall per eccellenza a tutela delle Web Application, permette di proteggere la DMZ da attacchi di tipo SQLi e XSS.

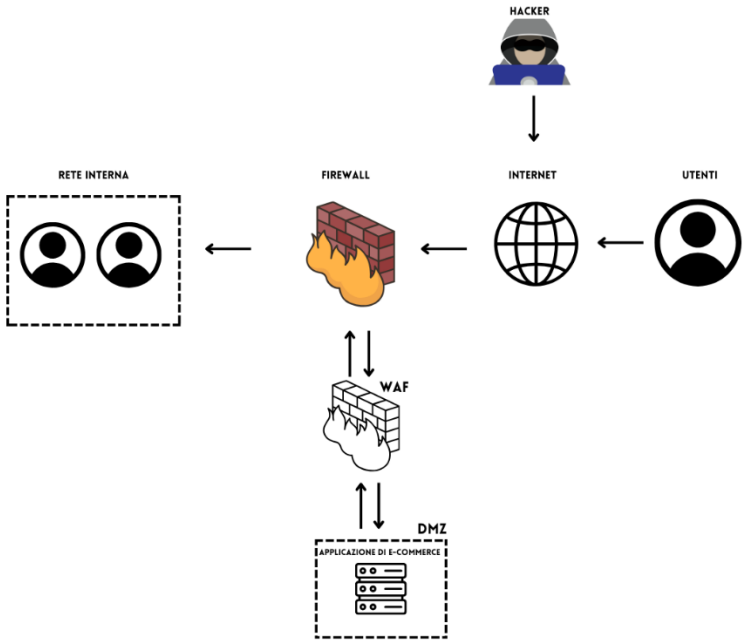
L'SQL Injection è una forma di attacco informatico che sfrutta vulnerabilità nelle applicazioni web. L'attaccante inserisce o manipola codice SQL malevolo all'interno di campi di input o parametri dell'applicazione, con l'obiettivo di alterare le query SQL eseguite dal sistema. Tipicamente, ciò avviene quando l'input dell'utente non viene validato in modo adeguato, permettendo agli aggressori di eseguire operazioni non autorizzate sul database sottostante.
Nel contesto di un modulo di accesso, un attaccante potrebbe inserire del codice SQL inappropriato nel campo dell'username, alterando la query originale. Se l'applicazione non tratta

correttamente questi dati di input, l'attaccante potrebbe ottenere accesso non autorizzato, estrarre informazioni sensibili o manipolare i dati.

Il **Cross-Site Scripting (XSS)** rappresenta una vulnerabilità comune nelle applicazioni web, in cui gli attaccanti inseriscono script dannosi che vengono successivamente eseguiti sul lato del client, generalmente all'interno del browser dell'utente. Questo tipo di attacco può assumere diverse forme, tra cui:

- Stored XSS, in cui gli script pericolosi sono memorizzati su un server e restituiti agli utenti quando accedono a una pagina specifica
- Reflected XSS, in cui gli script dannosi sono inclusi direttamente nelle URL e restituiti immediatamente nella risposta del server.

Gli attacchi XSS consentono agli aggressori di compromettere la sicurezza dell'applicazione, rubare informazioni sensibili come cookie di sessione ed eseguire azioni dannose a nome dell'utente.



2. IMPATTI SUL BUSINESS

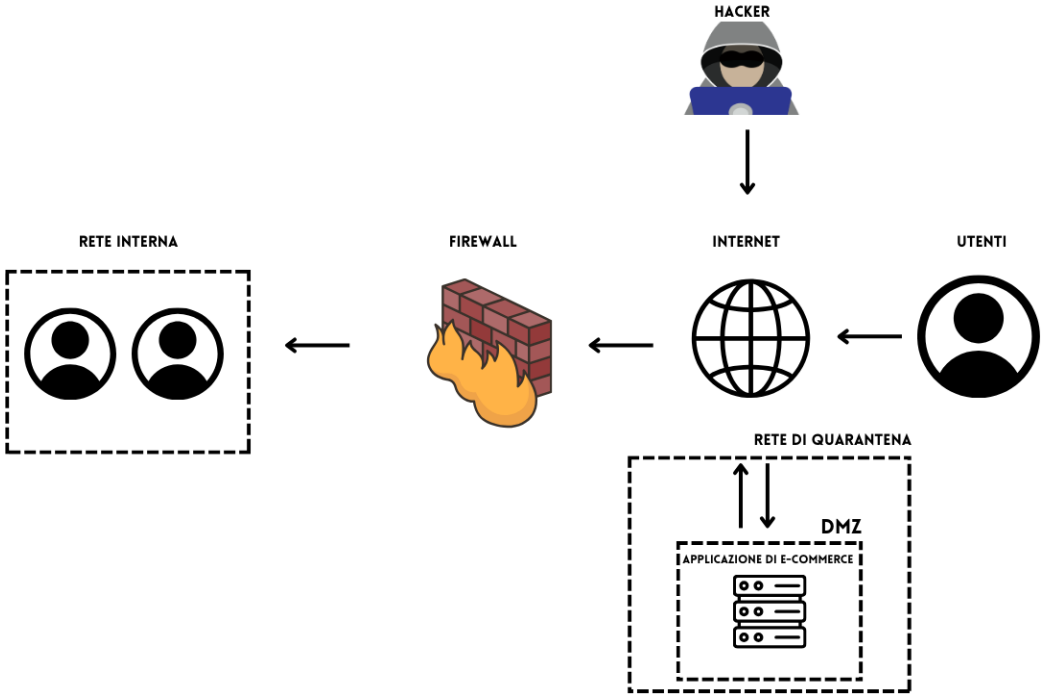
Nel caso in cui ci fosse un attacco di tipo Ddos dall'esterno, che rende l'applicazione non raggiungibile per 10 minuti, considerando che in media ogni minuto si effettuano acquisti di circa € 1500, possiamo calcolare l'impatto del business in maniera abbastanza rapida: 1500 x 10 = 15000.

Un tipo di attacco del genere, che rende inutilizzabile l'ecommerce genererebbe una perdita ipotetica di € **15000**

3. RESPONSE

l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra 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.

Nel caso in cui l'applicazione Web venga infettata da un malware e non siamo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infetta, possiamo trovare una soluzione simile a quella proposta.



La DMZ viene posta in una sottorete, chiamata ***Rete di Quarantena***, che isola i componenti infetti dalla rete interna, così da non permettere la diffusione del malware al resto dei dispositivi. Potrebbe sembrare una soluzione non completa, in realtà ha una funziona ben specifica, in quanto non taglia la connessione al potenziale attaccante, così come al resto degli utenti, continuando a fornire i servizi essenziali, e al contempo permette di effettuare ulteriori analisi del tipo di attacco senza esporre a ulteriori rischi la rete interna aziendale.