PROGETTO S9

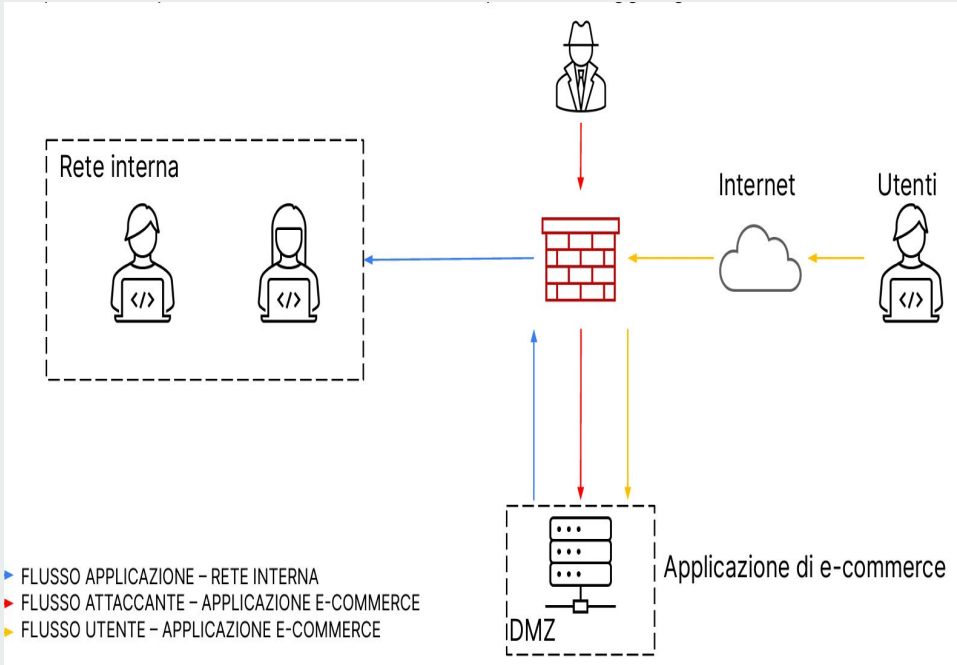
Task 1

La seguente architettura di rete prevede una rete interna raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungerla.

Tale contesto implica diversi rischi derivanti da attacchi SQLi e XSS

- Un attacco SQLi, o injection di SQL, è una tipologia di attacco informatico in cui un aggressore sfrutta le debolezze nei controlli di input di un'applicazione web per inserire istruzioni SQL dannose. L'obiettivo primario di un attacco SQLi è manipolare le query SQL eseguite dal sistema al fine di ottenere un accesso non autorizzato ai dati del database o comprometterne l'integrità.

- Un attacco XSS (Cross-Site Scripting) è una forma di attacco informatico in cui un aggressore introduce script dannosi all'interno di pagine web visualizzate da altri utenti.

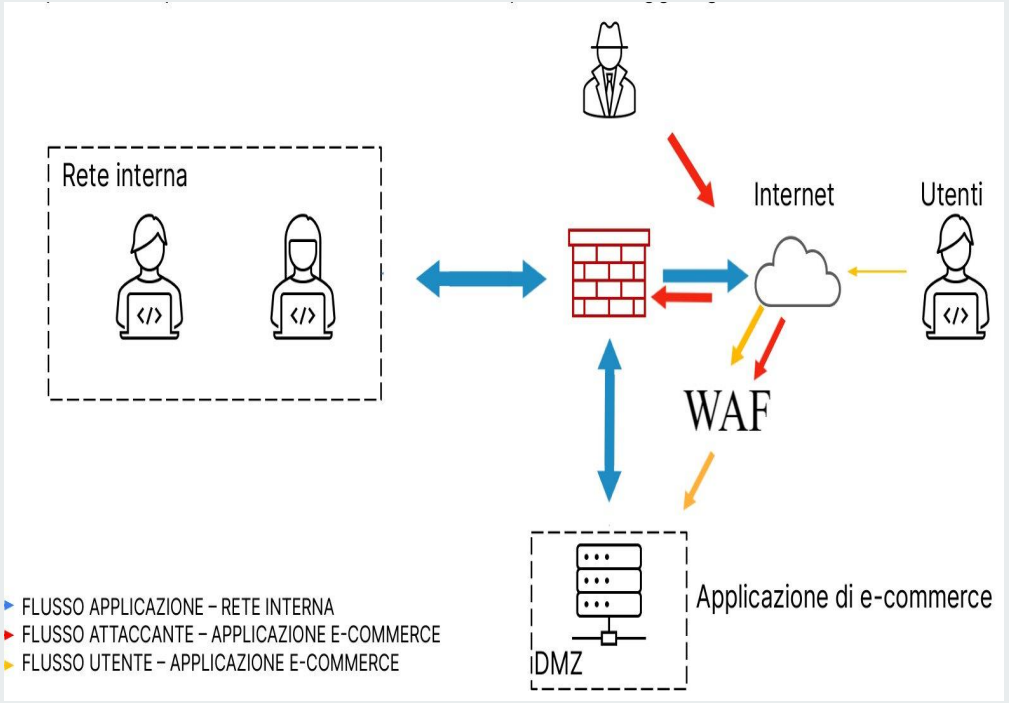


L'implementazione di misure preventive, come l'integrazione di un Web Application Firewall (WAF) e altre pratiche di sicurezza, mira a mitigare i rischi associati agli attacchi SQLi e XSS. Queste azioni sono fondamentali per prevenire eventuali danni derivanti da vulnerabilità nel sistema.

In particolare, la presenza di un WAF contribuisce significativamente alla difesa dell'applicazione web, agendo come una barriera protettiva contro attacchi noti come Cross-Site Scripting (XSS) e SQL injection. Posizionato all'esterno della DMZ, il WAF funge da primo punto di contatto per il traffico in arrivo, filtrando e bloccando potenziali minacce prima che raggiungano la zona demilitarizzata.

Questo approccio preventivo è cruciale per ridurre i rischi e prevenire eventuali conseguenze dannose derivanti da attacchi SQLi e XSS. La configurazione proposta semplifica la gestione del traffico complessivo, consentendo al WAF di fornire una protezione globale per l'intera infrastruttura, dalla DMZ alla rete interna.

Inserendo un Waf ,in quella determinata posizione, verranno filtrate le minacce in ingresso prima di raggiungere la Dmz,



Task 2

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 finanziario = **Durata dell’attacco*Spesa media degli utenti al minuto**

Impatto finanziario = **10 minuti * 1.500€/minuto**

Impatto finanziario = **15.000€**

Approfondimento

Un attacco DDoS, acronimo di Distributed Denial of Service, rappresenta una forma di attacco informatico in cui una vasta rete di computer compromessi, conosciuta come botnet, viene impiegata per sovraccaricare e saturare i server, le reti o le risorse di un obiettivo specifico. L'obiettivo primario di un attacco DDoS è rendere inaccessibile un servizio, un'applicazione o un sito web ai propri utenti legittimi, causando un'interruzione del servizio.

Durante un attacco DDoS, i server vengono sovraccaricati da un considerevole flusso di richieste di traffico, il che può tradursi in un rallentamento delle prestazioni o, nei casi più gravi, in una completa interruzione del servizio. La potenza di un attacco DDoS deriva dalla sua abilità di sfruttare un vasto numero di dispositivi distribuiti geograficamente al fine di generare un traffico che appare legittimo, ma che è eccessivo, sovrastando l'infrastruttura dell'obiettivo prescelto.

TASK 3

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.

Il primo step della terza fase di un piano di risposta agli incidenti è il contenimento del danno causato dall'incidente di sicurezza, che deve iniziare quanto prima possibile una volta terminata la fase di analisi. Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo tale che non possa creare ulteriori danni a reti / sistemi. Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la «segmentazione», che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso.Sebbene la segmentazione riesca a limitare la riproduzione del malware e l'accesso al resto della rete da parte dell'attaccante, spesso non è sufficiente per chiudere la fase di contenimento. In questi casi, quando è necessario un contenimento maggiore, si utilizza la tecnica dell'isolamento. L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.

Quindi l'obbiettivo principale,nel nostro caso, è quello di isolare completamente la Dmz ,ormai infetta ,in modo da evitare ulteriori diffusioni della minaccia alle varie risorse aziendali, mantenendo una connessione internet nella rete interna ma non verso la Dmz