CASO DI ATTACCO REALE

TASK 1 = Azioni preventive da implementare per difendere l'applicazione Web da attacchi SQLi e XSS da parte di un potenziale attaccante.

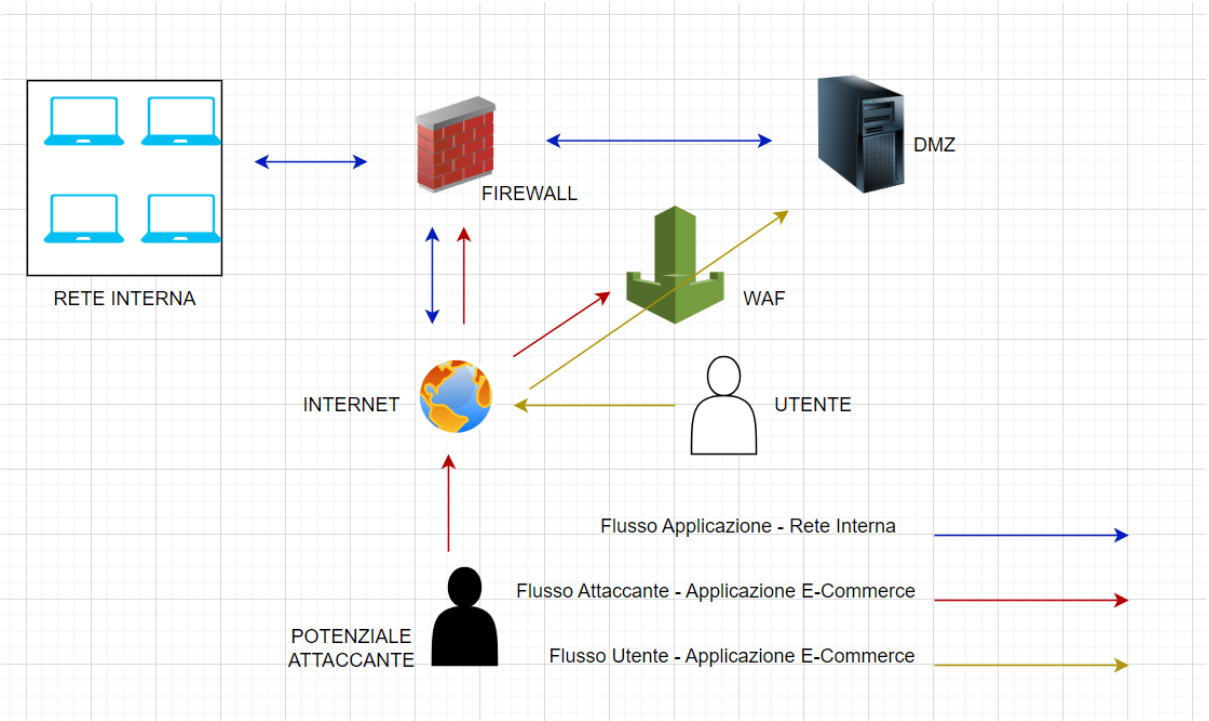
I servizi di Security Operations sono basati sulla gestione degli incidenti di sicurezza, ai quali si va incontro quando si verificano violazioni o minacce imminenti ai sistemi informativi. Gli incidenti di sicurezza possono includere la perdita o la divulgazione di dati sensibili, intrusioni nei sistemi interni da parte di utenti malintenzionati o attacchi malware.

Attenendoci alla task, focalizziamo il nostro interesse sulle azioni preventive, le quali vengono intraprese prima che si verifichi un incidente di sicurezza al fine di ridurre i rischi di eventi negativi. Ciò può comportare l'implementazione di misure di sicurezza, come firewall, sistemi di rilevamento delle intrusioni, politiche di accesso controllato e formazione del personale sulla sicurezza informatica.

Dunque, implementiamo delle misure preventive per difendere l'applicazione Web da attacchi SQLi e XSS da parte di un potenziale attaccante. Per far ciò, è possibile aggiungere un WAF (Web Application Firewall), il quale agisce come una barriera di protezione tra le applicazioni web e gli utenti esterni, rilevando e bloccando attacchi noti come Cross-Site Scripting (XSS) e SQL injection.

Di seguito un disegno dell'interfaccia di rete proposta con l'aggiunta di un WAF, posizionato all'esterno della DMZ, poiché in questo modo agirà come un punto di ingresso aggiuntivo per il traffico in arrivo dall'esterno e filtrerà le potenziali minacce prima che raggiungano la DMZ .

Questa configurazione può semplificare la gestione del traffico e consentire al WAF di fornire una protezione globale per l'intera infrastruttura, compresa la DMZ e la rete interna.



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€

TASK 3 = Ci concentriamo sulla fase del processo di incident response, affrontando una situazione in cui un attaccante ha infettato una web application tramite malware. Il primo passo di questa fase è il contenimento del danno causato dall'incidente, che deve essere effettuato il più rapidamente possibile per evitare la diffusione della minaccia ad altri sistemi e risorse aziendali. L'obiettivo principale del processo di contenimento è isolare l'incidente, evitando ulteriori danni alle reti e ai sistemi colpiti, riducendo l'impatto generale dell'incidente. Le tecniche utilizzate per raggiungere questo obiettivo includono la segmentazione, l'isolamento e la rimozione.

Ci sono situazioni in cui l'isolamento non è sufficiente e si richiede una misura di contenimento più rigorosa, che è la completa RIMOZIONE del sistema dalla rete interna e da Internet. In questo scenario, l'attaccante non avrà accesso né alla rete interna né alla macchina infetta. Questa strategia estrema viene adottata quando l'attaccante rappresenta una minaccia critica e non si possono rischiare ulteriori compromissioni dei sistemi aziendali. A tal proposito, la rimozione completa del sistema dalla rete garantisce un isolamento totale e protegge l'azienda da ulteriori danni, fornendo una protezione più robusta.

In questo caso Isoleremo la DMZ dalla nostra rete interna mantenendo una connessione ad internet da parte nostra ma non ci sarà connessione di alcun tipo dalla nostra rete interna verso la DMZ e viceversa.