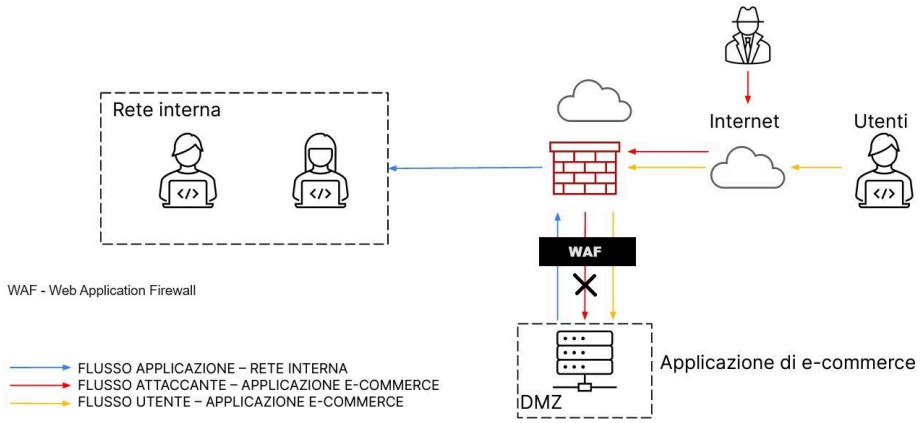
PROGETTO 5 - ROBERTO ROSSI

1- 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 di sotto in modo da evidenziare le implementazioni.

Le soluzioni per limitare attacchi SQLi e XSS possono essere varie.
Inizierei con l'assicurarmi che in fase di programmazione gli sviluppatori abbiano inserito dei controlli di valutazione e sanificazione dell'input immesso dagli utenti e che quindi vengano gestiti correttamente dal sistema. Un'altra soluzione, in aggiunta a quella appena citata, è l'utilizzo di un WAF – Web application Firewall, il cui funzionamento è quello di monitorare, filtrare o bloccare il traffico dati proteggendo le Web App da possibili minacce.

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



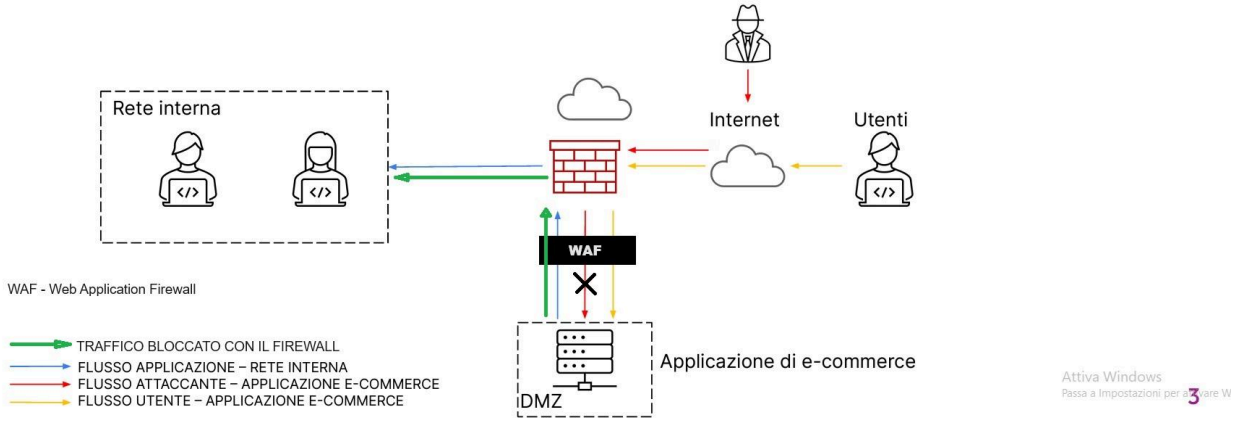
2- Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Per fare un'analisi riduttiva e immediata calcoliamo il danno con una semplice moltiplicazione tra il danno di ogni minuto, 1500 euro, per i 10 minuti in cui il sito sarà irraggiungibile che equivale a 15 mila euro di danno.

Per limitare le perdite e scongiurare attacchi futuri, è consigliata l'installazione di un Next Generation Firewall configurato a dovere e proporrei un server separato con il full backup dell'intera applicazione, un cloud esterno e/o un sito di back up da utilizzare nel caso il danno sia più grave dell'esempio, tale da subentrare al sito principale e non perdere neanche un minuto di danno e garantire ai clienti il continuo servizio.

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



3- 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.

Blocchiamo con il firewall il traffico in uscita dalla webapp alla rete interna, in modo da isolare la rete dai dati della webapp, senza staccare la webapp da internet in modo che l'attaccante abbia ancora accesso alla stessa.

4.5- Modifica più aggressiva dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.