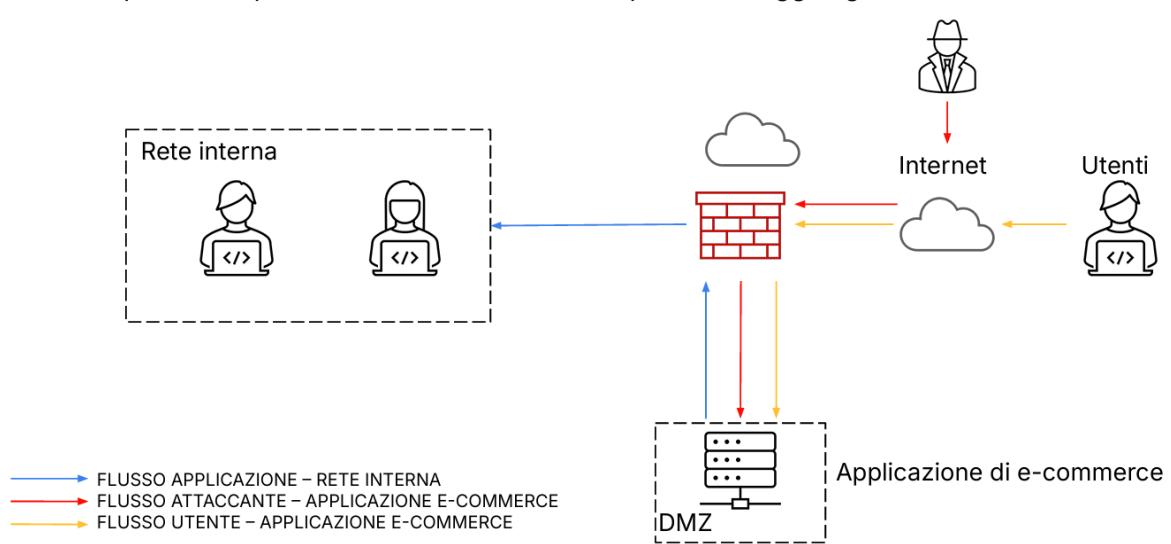


Traccia

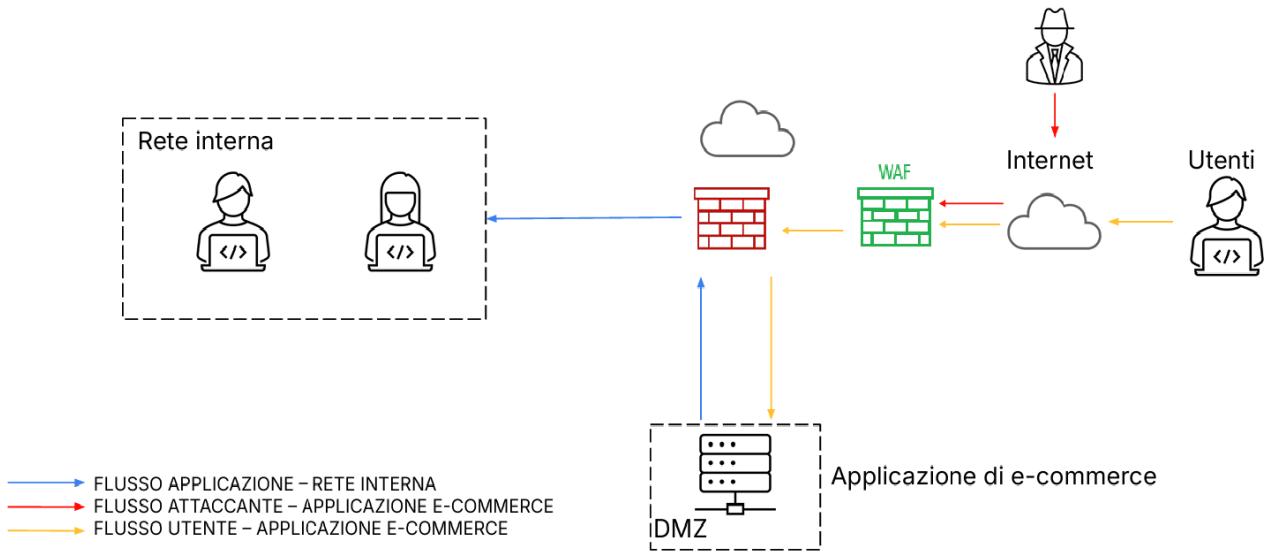
Rispondere ai seguenti quesiti:

1. 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
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
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.



1. Azioni preventive:

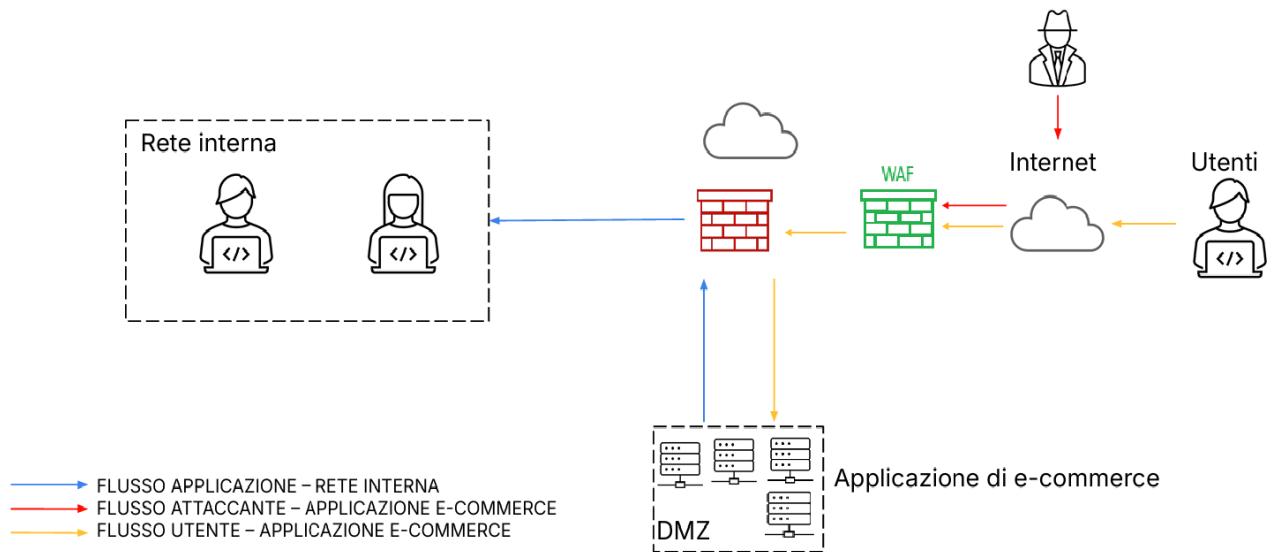
innanzitutto, implementerei un WAF (Web Application Firewall) che ha il compito di prevenire attacchi di tipo SQLi e XSS. Di seguito effettuerei una verifica di codice in input per assicurarci che gli utenti non possano immettere nelle box di testo del codice non filtrato.



2. Impatti sul business:

L'impatto economico è di $1500\text{€} \times 10 = 15.000\text{€}$

Per prevenire questi attacchi si potrebbe utilizzare il WAF implementato in precedenza configurandolo in modo tale che non ci siano troppe richieste da parte di molteplici utenti contemporaneamente. In alternativa si potrebbe creare una rete con più server per gestire l'applicazione di e-commerce così, in caso di troppe richieste, queste ultime avverranno smistate automaticamente e non creeranno coda.



3. Response:

Per me la prima cosa da fare quando si verifica una situazione del genere è individuare ed isolare il server infetto in una rete a parte. In un secondo momento si andrà ad effettuare tutte le analisi del caso.

