Consegna S9/L5

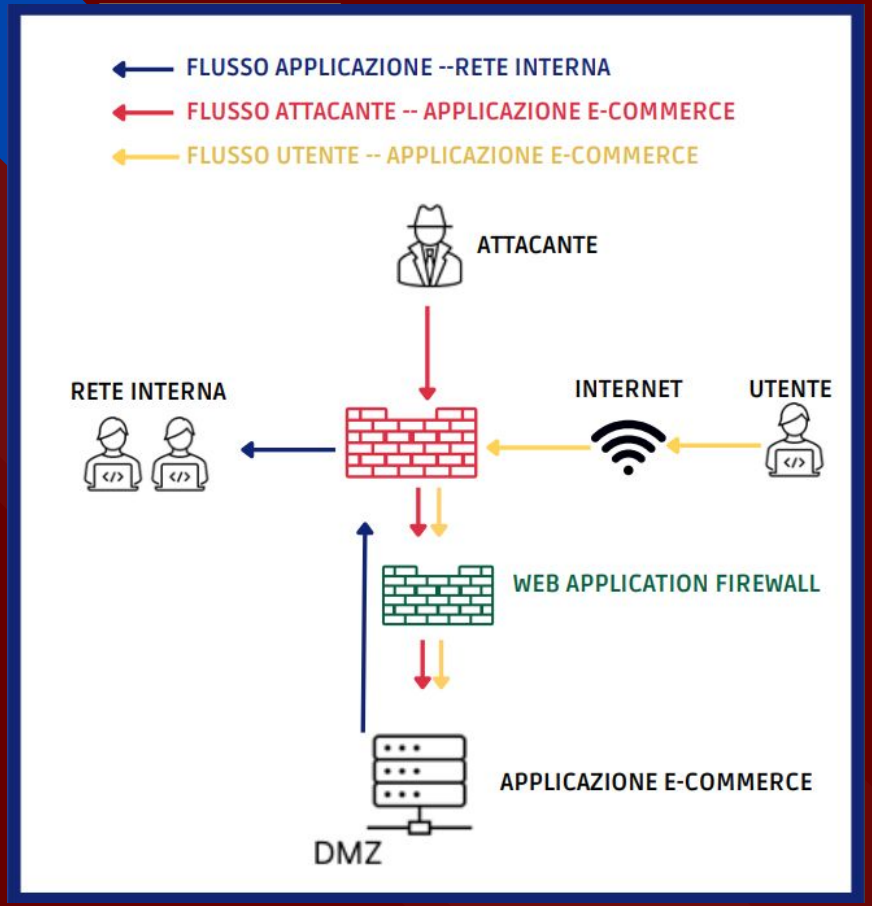
QUESITI

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?

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.

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.

QUESITO 1



Per proteggere la Web App da attacchi di tipo SQLi e XSS si può utilizzare un Web Application Firewall, che serve proprio per la protezione delle Web App da attacchi di questo tipo ed è migliore rispetto a un Firewall Standard. Nella figura a sinistra possiamo notare le modifiche apportate per permettere al Web Application Firewall di proteggere il traffico in entrata.

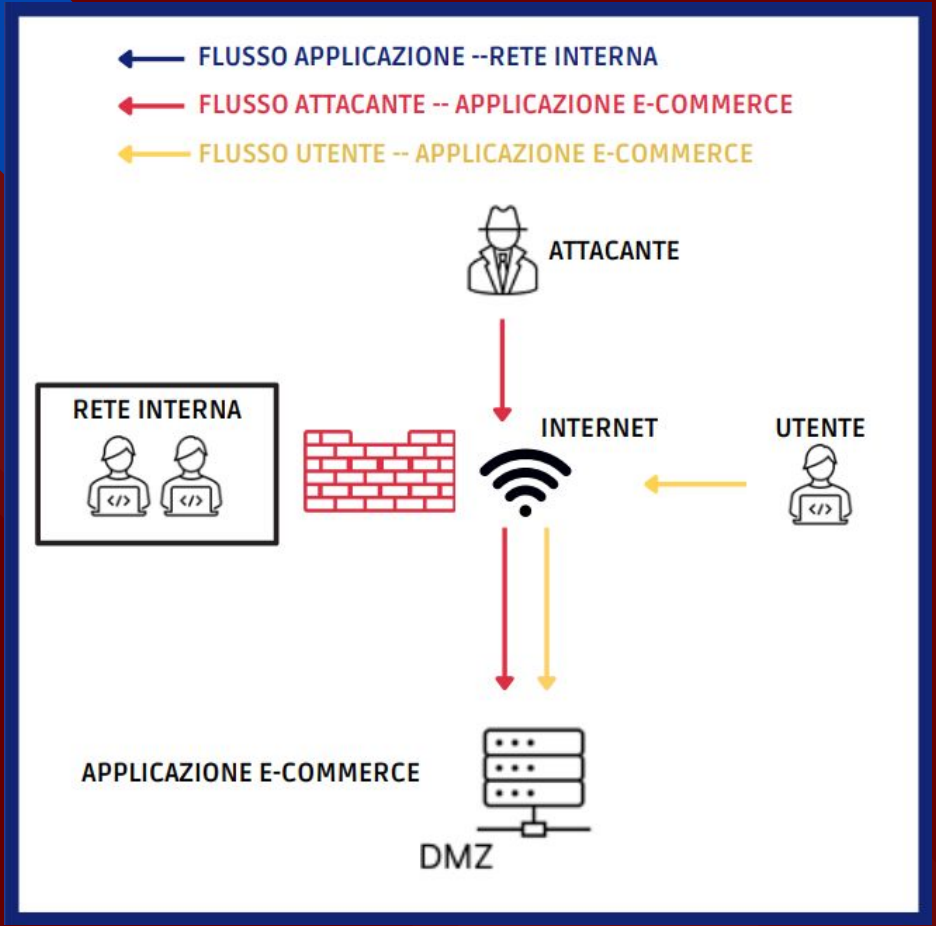
QUESITO 2

A causa dell'attacco Ddos la Web App dell'E-Commerce non è raggiungibile per 10 minuti. Tenendo conto che la spesa è di circa 1.500€ al minuto, per stimare i danni del mancato guadagno basterà moltiplicare la spesa potenziale per i minuti di inattività.

1.500€ x 10 minuti = 15.000 €

Quindi per 10 minuti di indisponibilità l'azienda avrà un potenziale mancato guadagno di 15.000 €.

QUESITO 3



Per risolvere questo problema basterà isolare la macchina infettata. La macchina sarà collegata a Internet e raggiungibile dall'attaccante ma non connessa alla rete interna. Nella figura a sinistra possiamo notare come non ci sia più collegamento tra l'e-commerce e la rete interna.