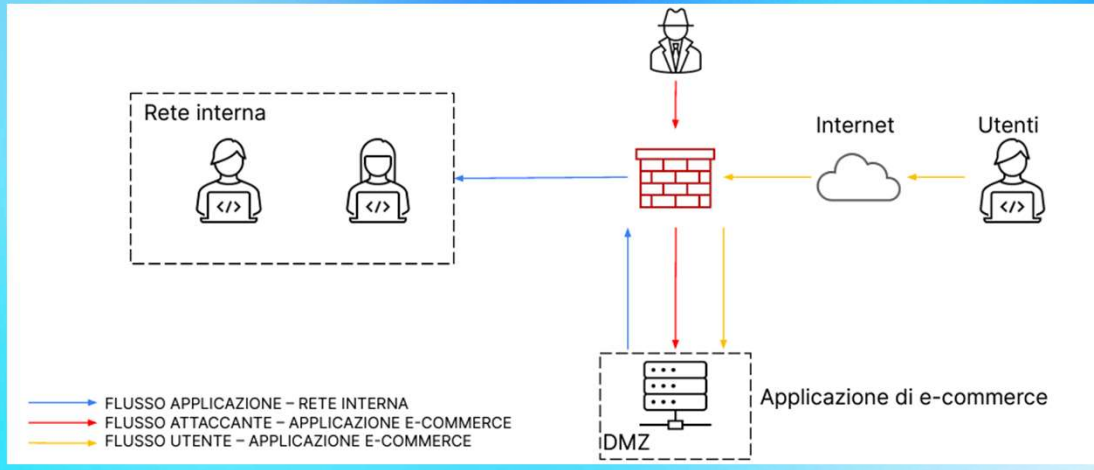
PROGETTO SETTIMANALE

S9/L5

SCOPO DEL PROGETTO

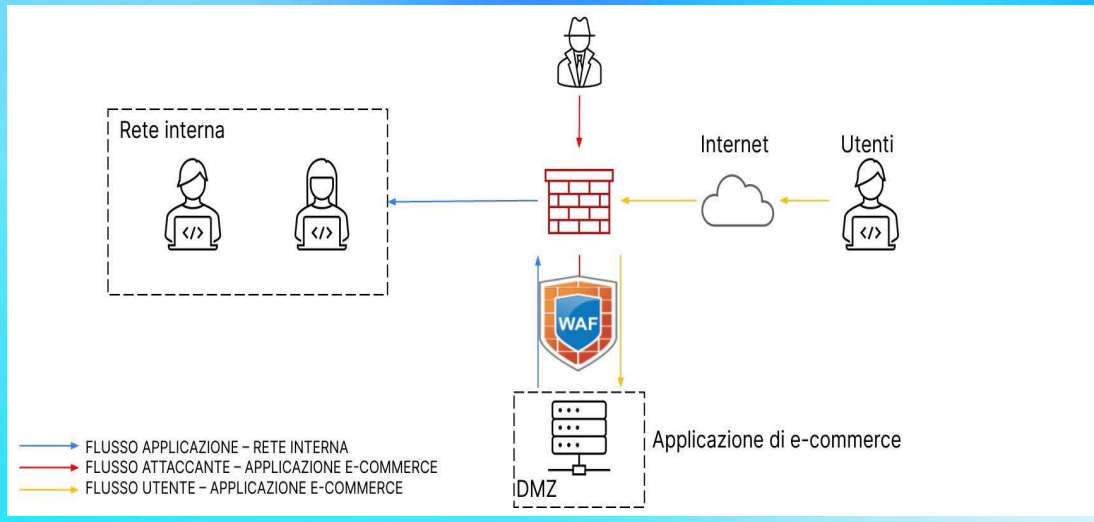
In riferimento all'immagine a destra vado ad eseguire le seguenti azioni:

- **AZIONI PREVENTIVE**: modificare l'immagine in modo da implementare le seguenti azioni per difendere l'applicazione web da attacchi di tipo XSS o SQLi da parte di un attaccante.
- **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.
- **RESPONSE**: l'applicazione Web viene infettata da un malware. Quindi vado a modificare l'immagine affinché la priorità sia quella di non far propagare il malware sulla nostra rete, mentre non dobbiamo rimuovere l'accesso da parte dell'attaccante alla macchina infettata.



AZIONI PREVENTIVE

Per difendere l'applicazione web da attacchi di tipo XSS e SQLi, la soluzione migliore è quella di inserire un WAF (Web Application Firewall). Quest'ultimo legge il contenuto di un pacchetto, lo confronta nel suo database e se è malevolo lo rigetta, in questo modo c'è una maggiore sicurezza per eventuali attacchi provenienti dall'esterno.



IMPATTI SUL BUSINESS

L’applicazione web subisce un attacco DDoS che rende i servizi non disponibili per dieci minuti. In questo lasso di tempo l’applicazione subisce un danno economico pari a 15.000 euro circa in quanto per ogni minuto genera un business pari 1500 euro.
Un attacco DDoS (negazione del servizio), è un attacco informatico in cui un numero elevato di dispositivi connessi in rete vengono coordinati per saturare le risorse di un sistema target, come un sito web o un server.
L'obiettivo principale di un attacco DDoS è rendere il servizio non disponibile agli utenti.
L’attacco sfrutta la potenza di molteplici dispositivi compromessi costituiti molto spesso da una rete di computer chiamati botnet.

RESPONSE

La web application è stata infettata da un malware. La priorità assoluta è quella di non farlo propagare nella rete interna e non dobbiamo rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Quindi la soluzione più efficace è la completa rimozione del sistema dalla rete interna in modo che non abbia più accesso.

Il motivo per cui non rimuoviamo l'accesso da parte dell'attaccante alla macchina infettata è perché economicamente all'azienda non converrebbe bloccare anche l'e-commerce.