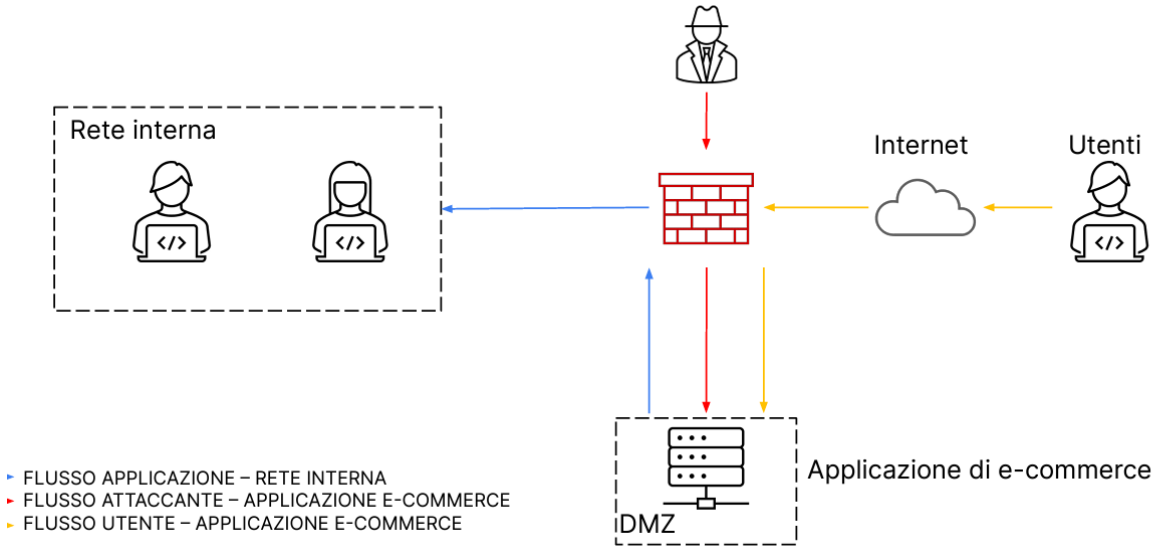
Progetto S9

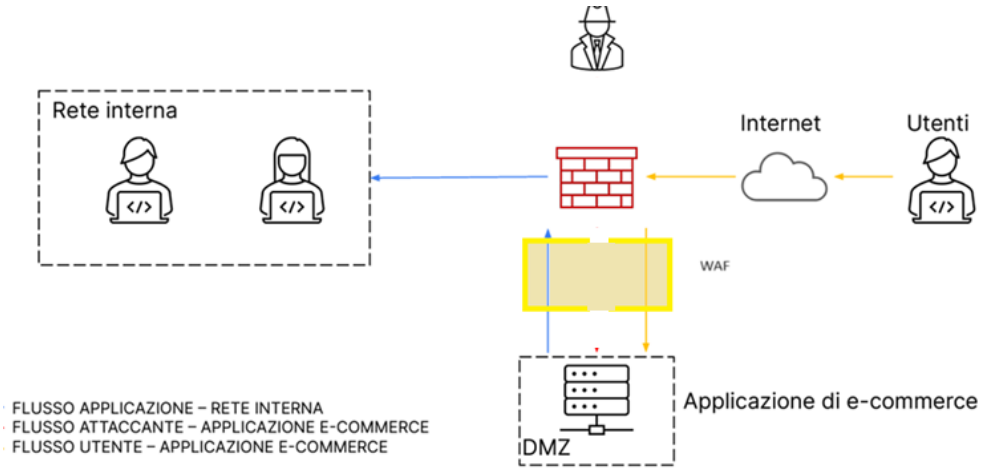
Il progetto di oggi è suddiviso in tre punti:

- 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;
- 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. 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.

Partiamo dal primo punto. Questo è lo schema della nostra rete:



Per implementare la difesa dell'applicazione e-commerce, potremmo aggiungere un WAF (Web application Firewall) tra la dmz e internet. Ricordiamo che il Waf filtra e blocca il traffico HTTP/HTTPS tra l'applicazione web e l'utente finale. Questo tipo di firewall aiuta a proteggere la nostra applicazione di e-commerce da eventuali attacchi XSS e SQL



Il secondo punto, ci chiede l'impatto di un attacco Ddos che rende l'applicazione irraggiungibile per 10 minuti, considerando che ogni minuto l'azienda perde 1500.00€. Il calcolo della perdita totale è molto semplice. Basterà moltiplicare la perdita che l'azienda ha ogni minuto per il tempo totale in cui l'applicazione non è raggiungibile.

Andremo quindi ad eseguire l'operazione 1500 * 10 = 15000.

Quanto questa perdita sia grave per l'azienda, dipenderà poi da quali sono le dimensioni ed il fatturato dell'azienda stessa. Nel caso in cui l'azienda fatturi 10000€ al mese, l'impatto di questo attacco sarà grave, mentre se l'azienda dovesse per esempio fatturare 10.000€ al giorno, l'impatto invece sarà minimo sulla base mensile.

Come ultimo punto, ci viene chiesto di effettuare un'azione di response in quanto la nostra applicazione web è stata infettata. Non vogliamo che l'applicazione sia disconnessa da internet in modo che gli utenti continuino ad avere accesso ad essa. Allo stesso tempo, non vogliamo però che gli altri host della nostra rete interna possano essere infettati. Quello che andremo a fare, pertanto, è isolare la nostra rete interna. Così facendo essa sarà disconnessa da internet e allo stesso tempo dall'applicazione web. Ma facendo così, non rischieremo di avere altri dispositivi infettati e l'attaccante non potrà provare ad accedere ad essi. Una volta che avremo risolto il problema con l'applicazione web, potremo riconnettere la nostra rete interna. Lo schema di rete sarà pertanto il seguente: