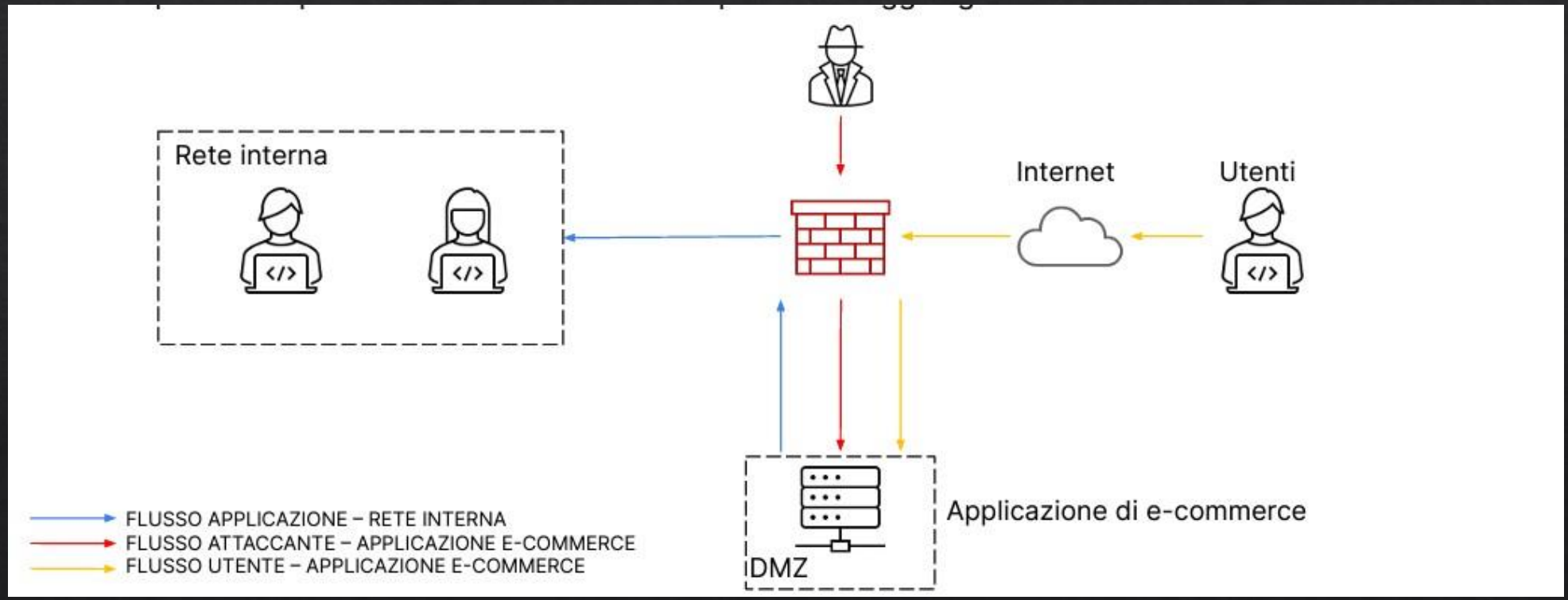
S9L5

La traccia di oggi con riferimento alla figura in slide 2, ci chiede di trovare le soluzioni dei seguenti problemi

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.
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 con la soluzione proposta.

L'architettura di rete prevede che l'applicazione di e-commerce sia accessibile agli utenti tramite internet per effettuare acquisti sulla piattaforma. La rete interna è accessibile dalla DMZ grazie alle configurazioni delle policy sul firewall. Di conseguenza, nel caso in cui il server nella DMZ venga compromesso, c'è il rischio potenziale che un attaccante possa penetrare nella rete interna.



IMPATTO SUL BUSINESS

Per stimare l'impatto finanziario causato dalla indisponibilità del servizio a causa di un attacco ddos, prendiamo in considerazione i seguenti aspetti:

- Periodo di tempo in cui il servizio non è accessibile: 10 minuti
- Reddito medio generato per ogni minuto dagli utenti sulla piattaforma di e-commerce: 1.500 €

Per calcolare il totale dell'impatto finanziario sull'attività, moltiplichiamo la durata della indisponibilità del servizio per il guadagno medio per minuto per utente:

Impatto finanziario = durata di indisponibilità del servizio (minuti) * guadagno medio per minuto per utente

Impatto finanziario = 10 minuti * 1.500 €/minuto

Impatto finanziario = 15.000 €

Date le circostanze di emergenza, è possibile adottare una strategia focalizzata sull'isolamento della macchina infetta. In questa situazione, la macchina verrà direttamente collegata a internet, rendendola accessibile all'attaccante, ma interrompendo la connessione con la rete interna. La figura nella presentazione illustra chiaramente la strategia di isolamento della macchina infetta. È importante notare che non vi è più alcuna comunicazione tra l'applicazione web e la rete interna.