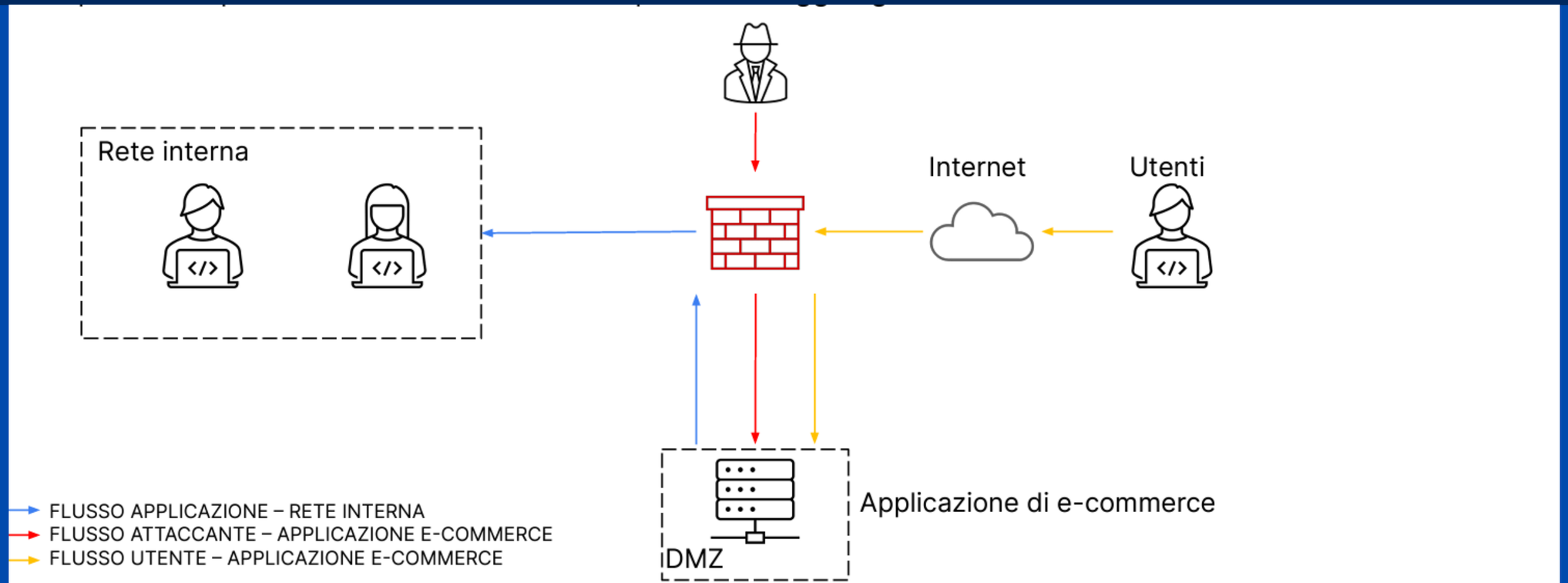
Progetto S9/L5

Traccia: Con riferimento alla figura , 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
1. **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.
1. **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 con la soluzione proposta.



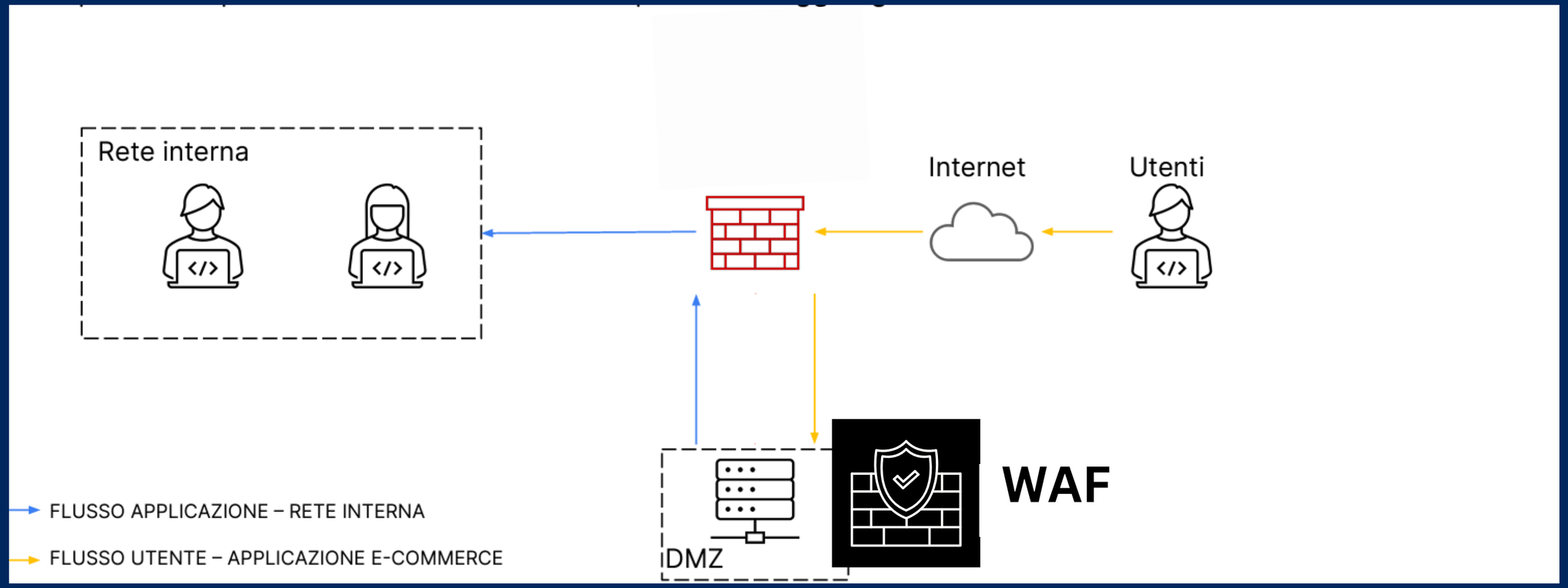
Sviluppo Azioni Preventive

Proteggere un'applicazione web da attacchi di tipo SQL injection (SQLi) e cross-site scripting (XSS) è fondamentale per garantire la sicurezza dei dati e degli utenti. Ecco alcune azioni preventive che si possono implementare:

- **Validazione e Sanitizzazione degli Input**
- **Least Privilege Principle**
- **Monitoraggio e Registrazione degli Eventi di Sicurezza**
- **Configurare un firewall per filtrare il traffico di rete.**
- **Segmentazione di Rete**
- **Monitoraggio del Traffico di Rete**
- **Controllo degli Accessi**
- **Backup e Ripristino**
- **Aggiornamenti del Sistema**
- **Formazione e Consapevolezza**

Modifica Alla Rete

Andiamo ad aggiungere un WAF. Un WAF è un tipo di firewall che si concentra specificamente sulla protezione delle applicazioni web e infatti lo andiamo a posizionare tra l’internet e la nostra DMZ. L'implementazione di un WAF è una pratica consigliata per migliorare la sicurezza delle applicazioni web ma va vistra nell’ottica di una delle tante contromisure necessarie infatti è spesso parte integrante di una strategia di sicurezza informatica più ampia, che include anche altre misure preventive a livello di rete e applicazione.



Impatti sul business

Per calcolare l'impatto finanziario dovuto alla non raggiungibilità del servizio a causa di un attacco DDoS, si utilizza la seguente formula:

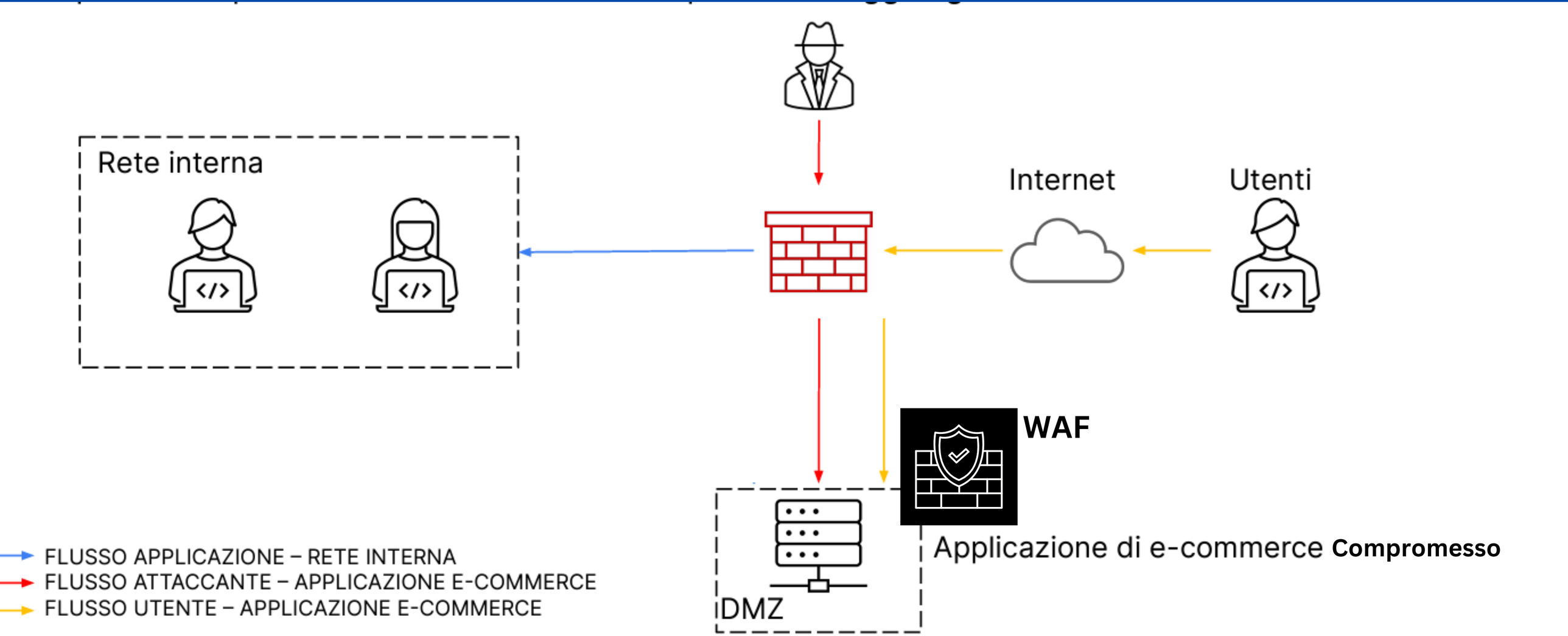
Impatto Finanziario=Perdita di guadagno per minuto (1500€)×Durata dell’indisponibilità in minuti(10).

Quindi, in questo scenario, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa dell'attacco DDoS è di 15.000 €. Questo rappresenta la perdita potenziale di guadagno durante il periodo di indisponibilità del servizio.

Response

Nella situazione in cui l'applicazione web è stata infettata da un malware e la priorità è evitare la propagazione del malware sulla rete senza interrompere l'accesso dell'attaccante alla macchina infettata, è utile adottare una strategia di contenimento. Isolare immediatamente la macchina infettata dalla rete principale. Questo può essere fatto mettendo la macchina in una subnet separata o in una VLAN dedicata. Andremo a lavorare sullo nodo che collega la rete interna alla DMZ, negando le connessioni verso la rete interna ma lasciando l'applicazione online.
Questo comporta una serie di valutazioni sotto diversi punti di vista, andiamo ad analizzarne qualcuno.
Se da un lato è vero che esponiamo chi visita il sito di e-commerce al rischio di essere infettati dal malware d'altro canto questa scelta ci da la possibilità di indagare a fondo sulle tecniche utilizzate dall'attaccante e analizzarne il comportamento, potremmo essere al day 0 di una nuova minaccia e la raccolta di informazioni è un'arma importante per un eventuale risoluzione delle minacce.
Il passo successivo è indubbiamente la rimozione del malware, (ma che non andremo a vedere in queste slide) in modo che i clienti che accedano al nostro sito lo possano fare in totale sicurezza(buona reputazione per l'azienda).

Response


Rete interna
Internet
Utenti
WAF
DMZ
Applicazione di e-commerce **Compromesso**
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

FINE

Grazie
Massimo Cinquegrana