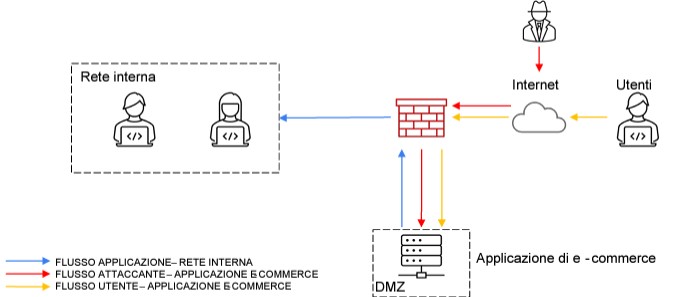
**Progetto settimanale S9L5**

**Grazia Cinzia Coco**

Con riferimento alla figura sottostante, è stato richiesto di rispondere ai quesiti.



**1 Azioni preventive:**

Quali azioni preventive si potrebbero implementare per difendere l’applicazione Web da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato?

Modificate la figura in modo da evidenziare le implementazioni.

Si potrebbe utilizzare un WAF (Web Application Firewall)

**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 1200 euro sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Si stima una perdita di 12000 euro.

Si possono applicare come eventuali azioni preventive: IPS/IDS, penetration testing, logging e monitoring.

**3 Response:**

L’applicazione Web viene infettata da un malware.

La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infettata.

Modificate la figura con la soluzione proposta.

Si potrebbe isolare la parte infetta, mantenendo l’accesso ad internet.

**4 Soluzione completa:**

**5 Modifica “più aggressiva” dell’infrastruttura:**

Integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2).

Budget 5000 - 10000 euro.

Eventualmente fare più proposte di spesa.