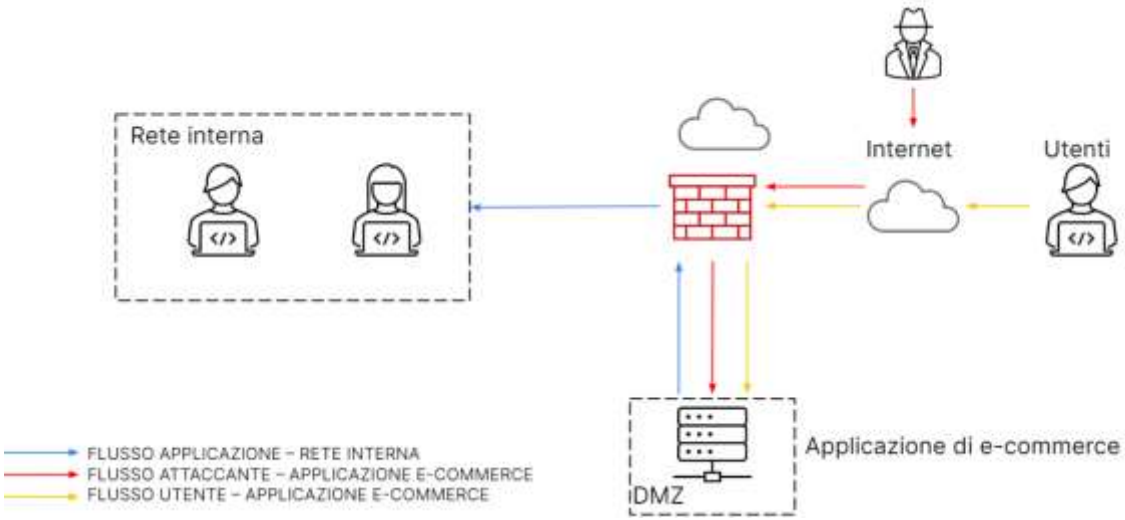


Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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

Le vulnerabilità di tipo SQLi sono quelle in cui l'autore di un attacco utilizza parte di un codice SQL per manipolare un database e accedere ad informazioni potenzialmente preziose. Può essere utilizzato contro qualsiasi applicazione web o sito web che utilizzi un database basato su SQL. Anche in un attacco XSS Cross Site Scripting l'autore prende il controllo di una web app e sulle sue componenti.

Le azioni preventive possono essere le seguenti:

Formazione del personale sui rischi derivanti da questi attacchi, dunque dare loro la giusta formazione;

Tenere sotto controllo l'input degli utenti fino a quando non viene verificato. Assegnare solo i privilegi minimi necessari per agli account che si connettono al database. Filtrare/sanitizzare;

Tenere sempre aggiornate le versioni degli asset attraverso software e patch di sicurezza più recenti;

Eseguire la scansione delle web app. Pentesting;

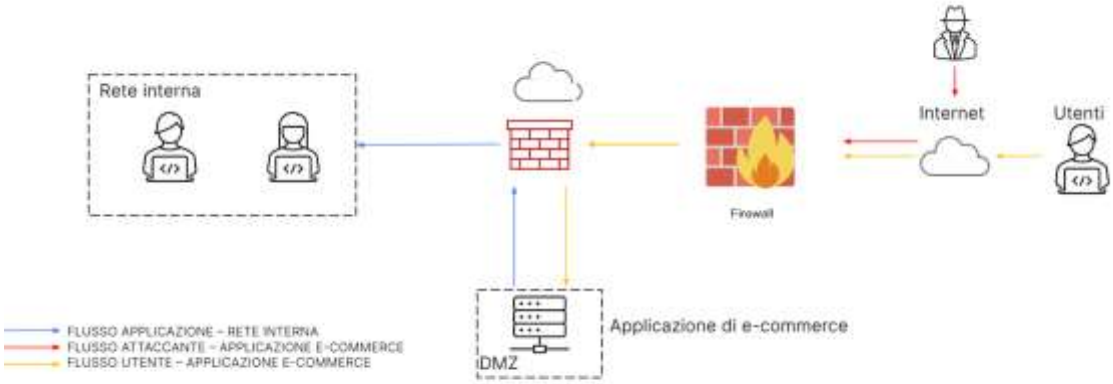
Utilizzare un firewall WAF;

Segmentare la rete;

IPS/IDS;

Controllare gli end point;

Group Policy.

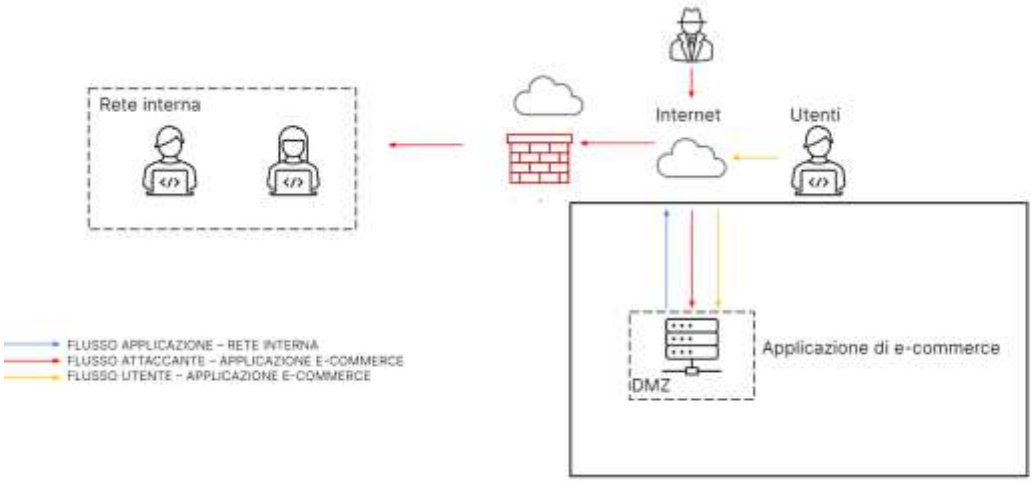


2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti**.
   Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** sulla piattaforma di e-commerce. **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**

Attraverso il **BIA Business Impact Analysis** si possono identificare le risorse critiche di una compagnia e le potenziali minacce alle quali sono esposte. Il BIA ha inoltre lo scopo di misurare la probabilità che tali minacce possano verificarsi e l'impatto sul business. Il primo passo è quello di **identificare le priorità** del business e calcolare: il valore del **Maximum Tolerate Downtime (MTD)** cioè il limite massimo di tempo durante il quale un business può non essere operativo senza causare danni irreparabili e il Recovery Time Objective (RTO), ovvero l'ammontare di tempo necessario a recuperare un sistema o una funzionalità in caso di disastro. Una volta completata la fase di identificazione delle priorità si passa a quella di **identificazione dei rischi**, in seguito a quella della **valutazione delle probabilità** infine una **valutazione degli impatti.** In questo caso l'impatto è Alto in quanto la compagnia non riesce ad erogare i servizi critici per tutti gli utenti che in quei 10 minuti avrebbero speso in media 15.000 euro.

Attraverso il thread modeling vengono presi in esame i diversi fattori al fine di capire i veri rischi dell'organizzazione. I componenti del TI attraverso sorgenti pubbliche o fonti a pagamento possono recuperare info sulle minacce (feed). Sarebbe opportuno anche creare dei backup per non perdere i dati o utilizzare un cloud. Fare dei Controlli Network: NAC (Network Access Control) che consentono di controllare gli accessi alla propria rete limitando l'accesso solo agli utenti autorizzati e assicurando che i sistemi che accedono alla rete soddisfino determinati requisiti di sicurezza. Utilizzare un Firewall per filtrare i pacchetti e monitorarli. Vedi sopra.

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 2 con la soluzione proposta.



La web app viene isolata.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)