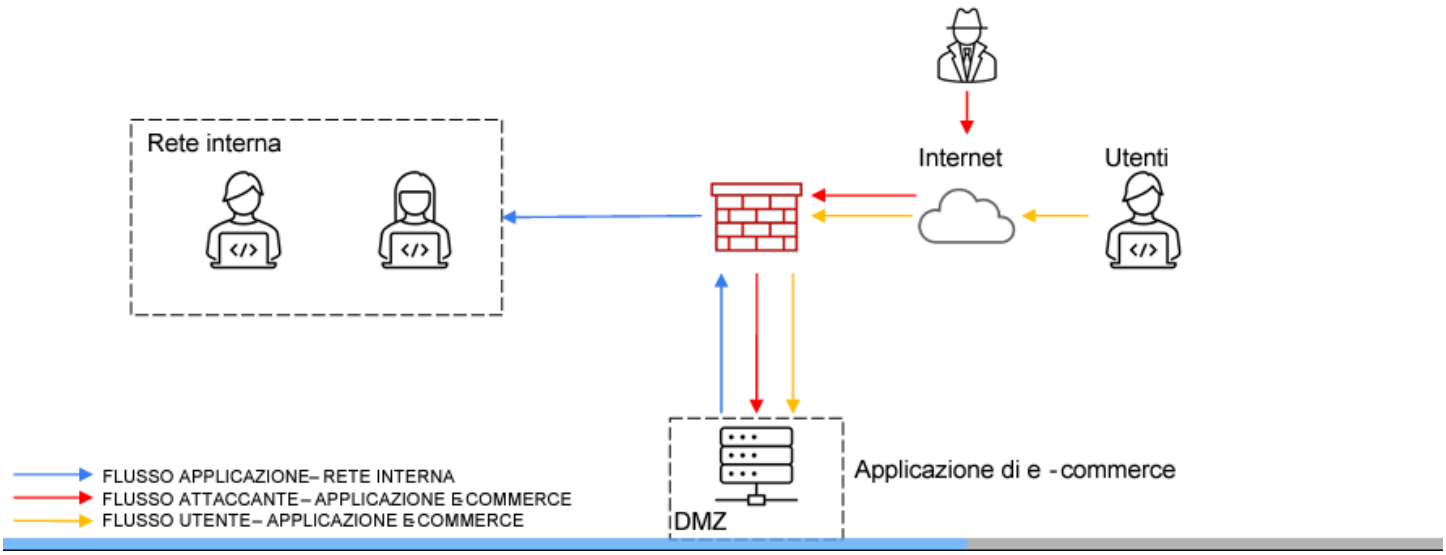
Gestione dei sistemi di sicurezza informatica

Traccia:

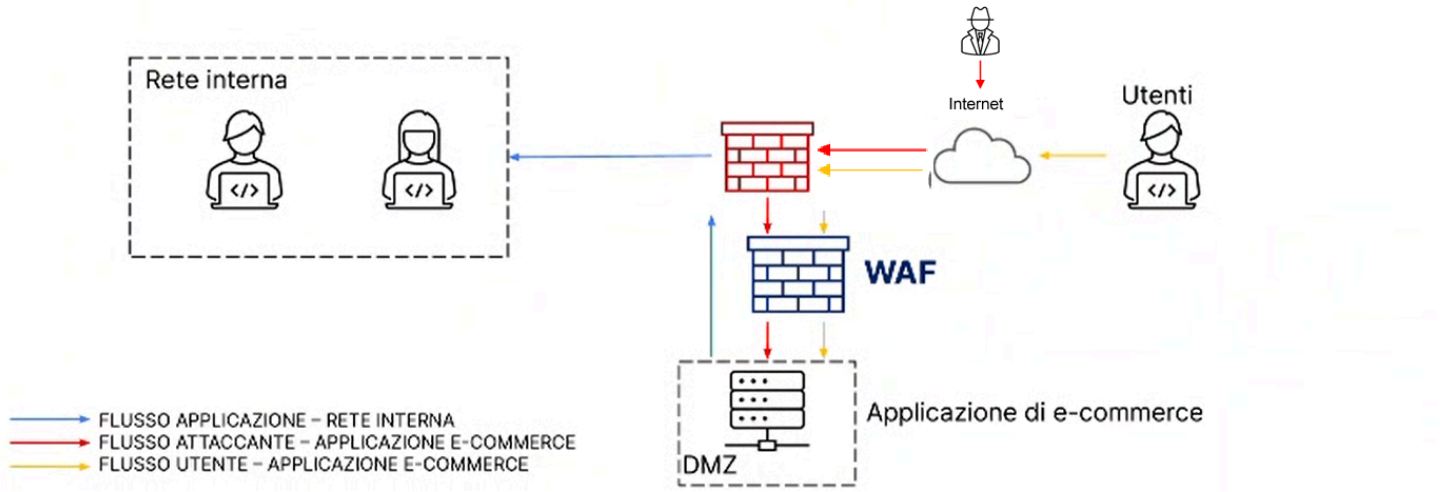
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.
Esercizio Traccia e requisiti
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica
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 gli utenti spendono ogni minuto 1.200 € sulla piattaforma di e-commerce .
Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
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 .
4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5.Modifica << piu' aggressiva >> dell'infrastruttura: integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2) Budget 5000-10000 euro. Eventualmente fare piu' proposte di spesa.

Rete proposta nella traccia:



Possiamo notare che un malintenzionato se utilizza **XSS** o **SQLi** potrebbe accedere al server in

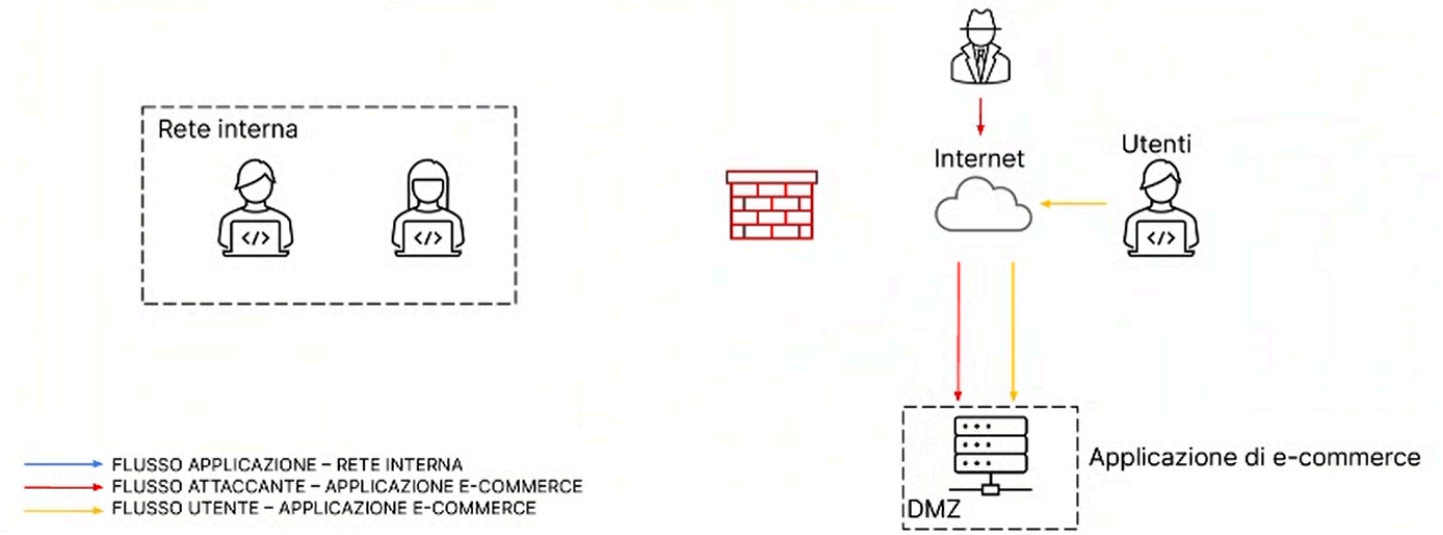
DMZ compromettendo la web app, quindi come primo passaggio bisogna trovare un compromesso per qui tipi di attacchi:
Una possibile soluzione e' l'aggiunta di un **WAF** (**Web Application Firewall**) un firewall apposito per impedire attacchi **XSS** e **SQLi**:



Inoltre consiglierei anche una modifica del codice php per rafforzare la difesa da un attacco SQLi.

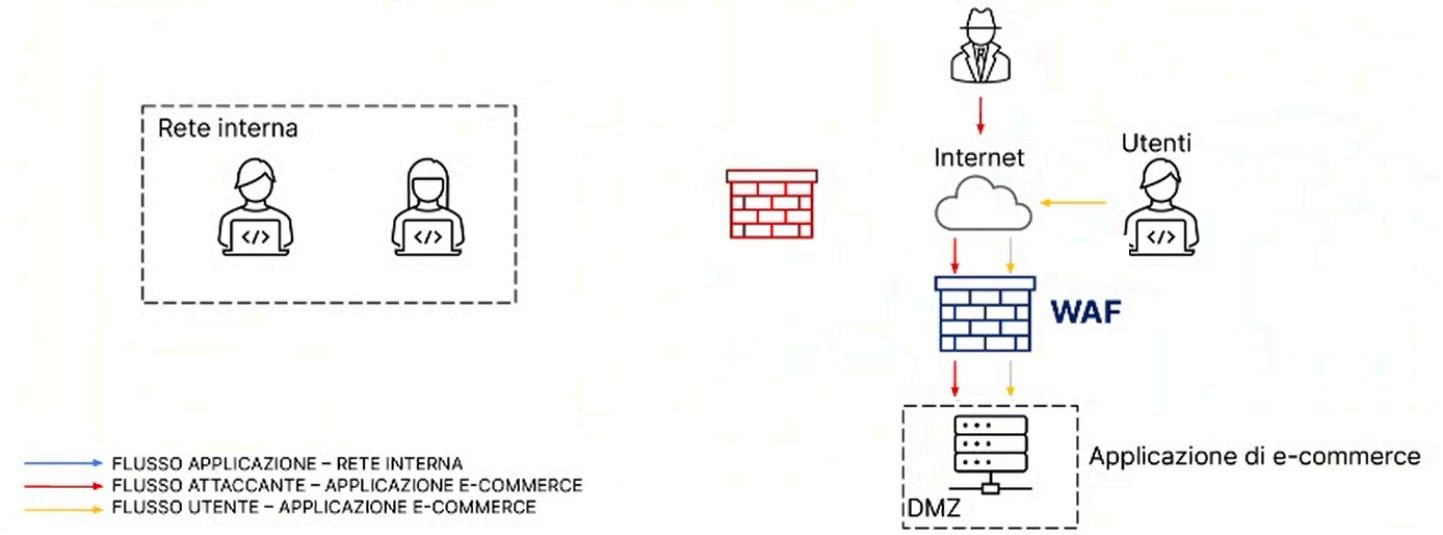
Se invece la **Web App** subisce un attacco **DDoS** (**Distribuited Denial of Service**) per 10 minuti, impedendone l'uso totale, considerando che in media gli utenti spendono ogni minuto 1.200 € sulla piattaforma di e-commerce, possiamo calcolare il danno totale con una semplice proporzione matematica:
1 : 1.200 = 10 : x => x = 1.200 x 10 = 12.000 €
Quindi la compagnia perde un entrata di 12.000 €.

Se la **Web App** viene attaccata da un malware, possiamo gestire l'isolamento della macchina infetta, in questo modo **impediamo** la diffusione del malware nella rete interna.
Questo isolamento non deve essere totale, ma bensi' solo dalla **rete interna**; questo permette al malintenzionato di accedere alla macchina infetta, ma non alla rete interna e in piu' permette delle analisi forense future per scovare il colpevole:



Inoltre e' opportuno gestire al meglio anche i backup, sperando che l'azienda ne abbia fatti alcuni e monitorare il traffico.

Infine possiamo unire le due soluzioni ottenendo questo risultato:



Per una modifica piu' aggressiva, stando in un margine tra 5000-10000 €, possiamo procede nel seguente modo:
1. Aggiungiamo un **EPP (EndPoint Protection)** e un **EDR (Endpoint Detection Response)**, che sono dei software che servono per gestire la sicurezza dei punti finali della rete (Laptop, pc, ecc). In particolare un **EPP** si concentrano sulla prevenzione di possibili attacchi, perfetto per proteggere singolarmente un dispositivo da malware, mentre gli **EDR** si concentrano sulla rilevazione e risposta degli incidenti.
Come prezzo totale, l'utilizzo di entrambi si aggira tra i 2000-4000 €
2. Aggiungiamo la **formazione del personale** per tenerli sempre aggiornati, corsi che potrebbero costare tra i 500-1000€.
3.Aggiungiamo un **penetration testing** periodico per analizzare periodicamente le vulnerabilita', costo tra 1000-2000€.
4.Aggiungiamo un **SIEM (Security Information end Event Menagement)** che e' una soluzione

di sicurezza che unisce la gestione delle informazioni di sicurezza **(SIM)** e la gestione degli eventi di sicurezza **(SEM)**, in altre parole analizza e correla i file log.
I prezzi posso variare da 500-1500€/mese.
5. Non possiamo omettere una **ZTA (Zero Trust Architecture)** che e' un modello di sicurezza informatica che si basa sul principio che nessun utente interno od esterno alla rete aziendale, debba essere automaticamente considerato affidabile. (spettacolare)
I prezzi anche qua si aggirano tra i 500-1000€.
6. Come ultimo ma non per importanza, gestiamo la **segmentazione della rete**, tramite **firewall**, **WAF**, **switch** od altri dispositivi per la sicurezza come poc'anzi visto.
I prezzi di questi dispositivi sono svariati, ma se dobbiamo stare in un margine specifico, restano circa 500-1000€

Conclusione:

Come possiamo notare, i sistemi di sicurezza sono molteplici e lo specifico modello per una data azienda viene poi progettato dal **CISO (Chief Information Security Officer)**; in base al tipo di azienda (sia come dimensioni che come importanza), usera' sistemi piu' o meno sofisticati. Consideriamo che un semplice dispositivo di sicurezza come un firewall ha prezzi che variano da centinaia di euro a decine di migliaia di euro, in base alle esigenze; questo dovrebbe far capire che non esiste uno schema perfetto, ma bensi' esistono schemi ben strutturati nel rapporto qualita'/prezzo e soprattutto basati sulle esigenze aziendali.