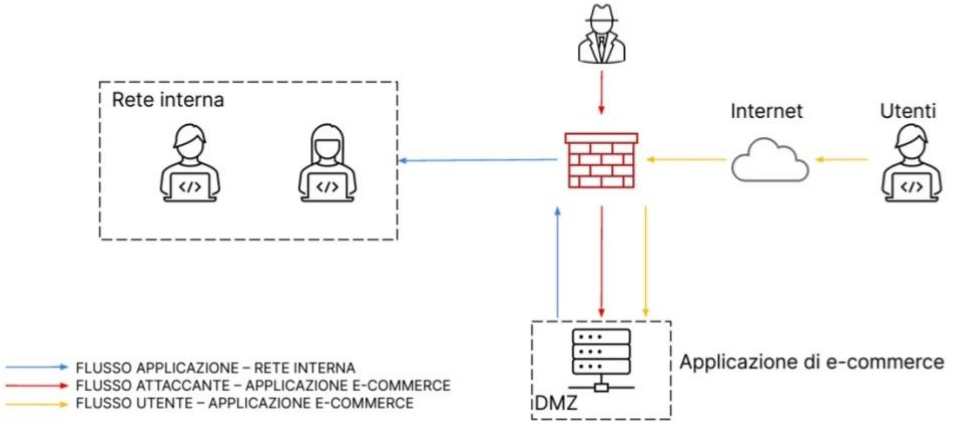
Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



3

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 in slide 2 con la soluzione proposta.

Azioni preventive:

Per proteggere l'applicazione Web dalle minacce XSS e SQL injection si può utilizzare un Firewall per bloccare eventuali intrusioni codice malevolo.

Un Firewall è come un muro che lascia passare solo l'invio di dati autorizzato.

Impatti sul business:

L'attacco viene utilizzato Ddos per mandare in tilt i computer e non far più funzionare un determinato sito.

In questo caso specifico se gli utenti del sito di e-commerce spendono € 1500 al minuto, 10 minuti senza poter utilizzare il sito equivalrebbero all'incirca a €15.000 di perdita stimata.

Response:

Considerando che il malware ha già infettato il sito di e-commerce e si sta cercando di limitare i danni la soluzione migliore da adottare sarebbe una strategia basata sull'isolamento del computer infetto; in particolar modo suggerisco di lasciare il computer ancora collegato ad internet ma isolato dalla rete interna.