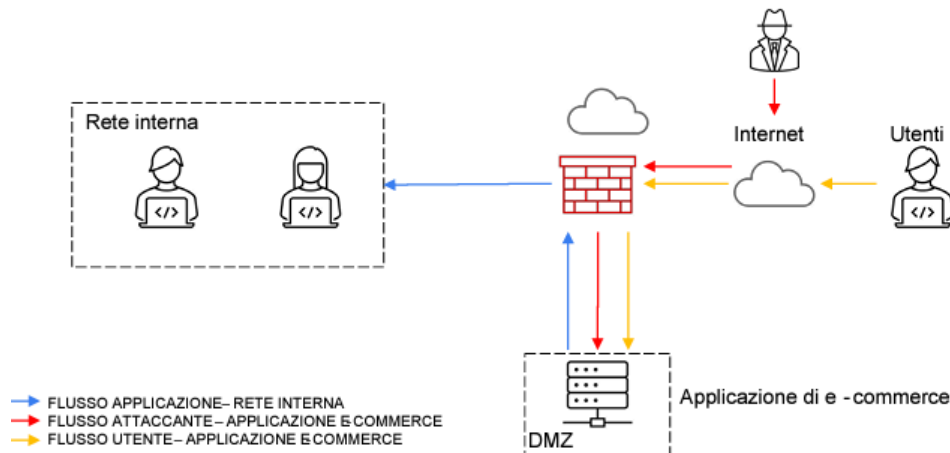
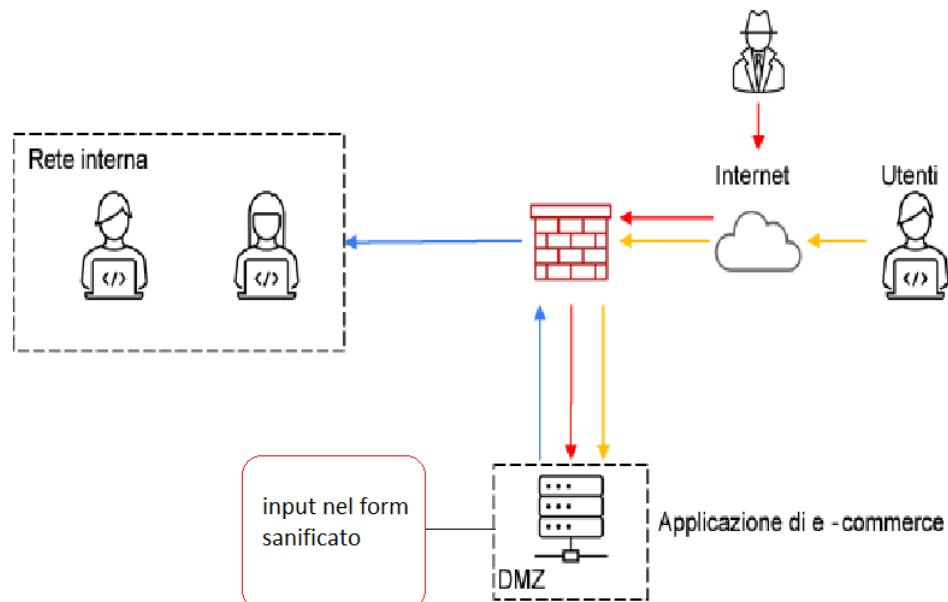


PROGETTO SETTIMANA 9

quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?



SOLUZIONE



Implemento un input sanificato nell'applicazione e-commerce, in modo tale da mitigare entrambi le vulnerabilità (xss, sqli).

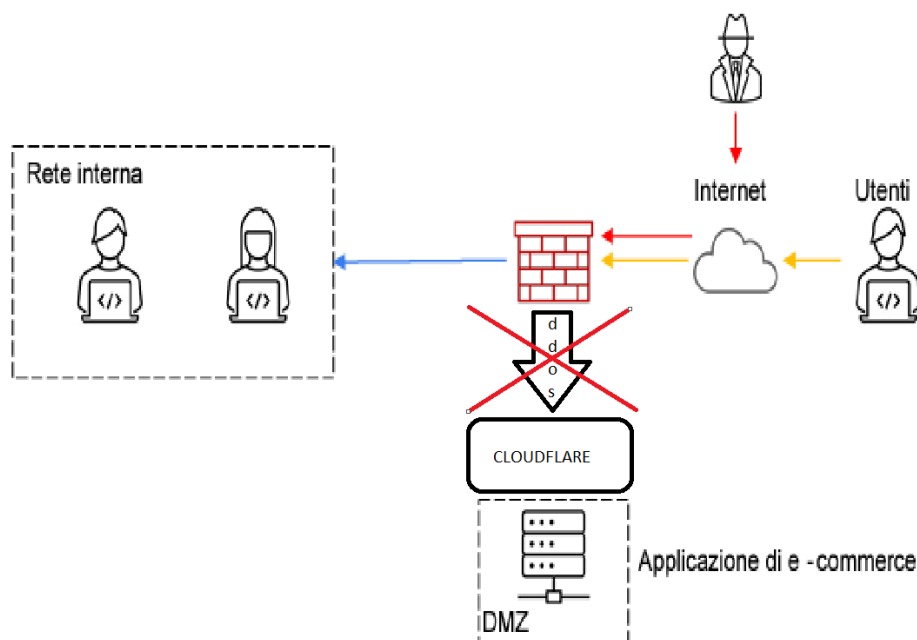
2

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.

SOLUZIONE

Impatto totale sul business dell'azienda=15.000€

Andiamo ad aggiungere un servizio di protezione a questo tipo di attacco utilizzando **cloudflare**, quest'ultimo monitora in tempo reale il traffico di rete sull'applicazione web e in caso di eventuale attacco DDOS/DOS attiva un sistema di protezione in modo da mitigare il problema e mantenere l'applicazione web **online**.

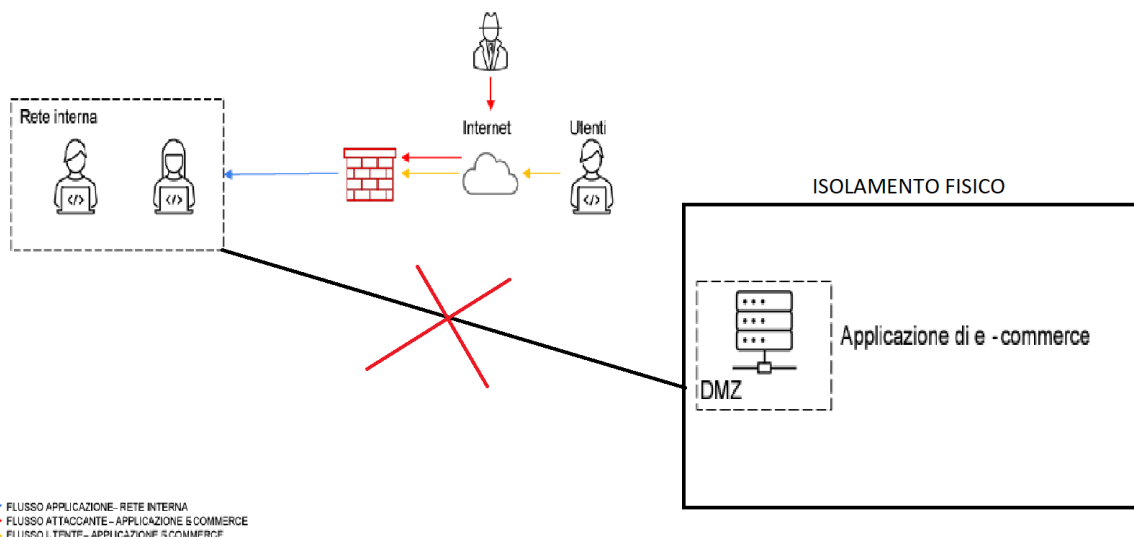


3

L'applicazione Web viene infettata da un malware.
La vostra priorità è che il malware non si propaghi sulla vostra rete.

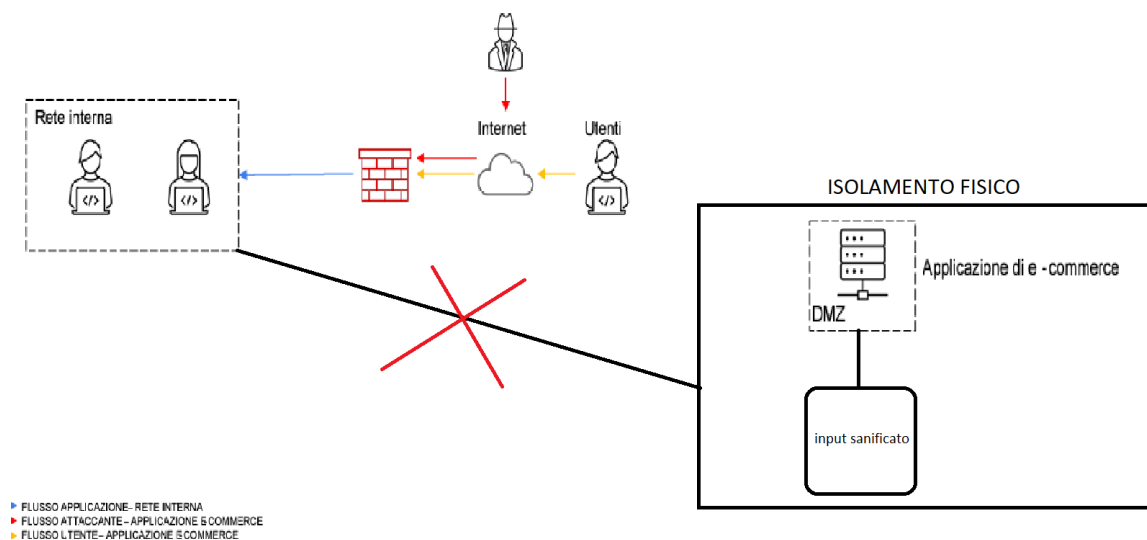
SOLUZIONE

In caso si identifichi un malware all'interno della nostra applicazione web, andiamo in maniera immediata a isolare la nostra web-app (*mettendola offline*) in modo da essere sicuri che il **malware** rimanga solo all'interno di essa e non comporti problemi alla rete interna.



SOLUZIONE COMPLETA

Unire i disegni dell'azione preventiva e della response



Possibile integrazione di elementi di sicurezza per la nostra struttura di rete



possiamo aggiungere un ips in modo da monitorare e bloccare eventuali minacce.

Prezzo=2700€(Cisco ASA5515-IPS-K9)

Inoltre possiamo integrare anche un firewall NGFW di nuova generazione, anche quest'ultimo ci fornisce ulteriore sicurezza per mitigare ad esempio attacchi dos/ddos



Prezzo=3000€(Sophos XGS 2100 Appliance)

Integrando entrambi gli hardware possiamo avere un'ottima sicurezza di rete.

**ATTENZIONE:NON POSSIAMO MAI OTTENERE UNA
SICUREZZA COMPLETA ED ESSERE IMMUNI DA ATTACCHI
INFORMATICI!**