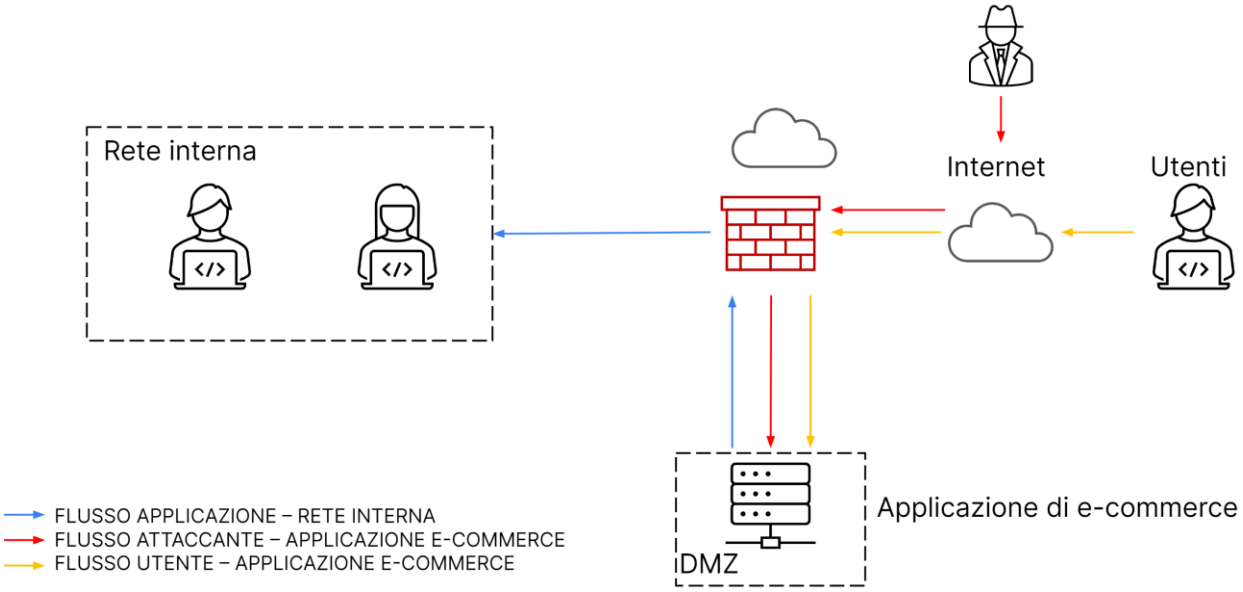
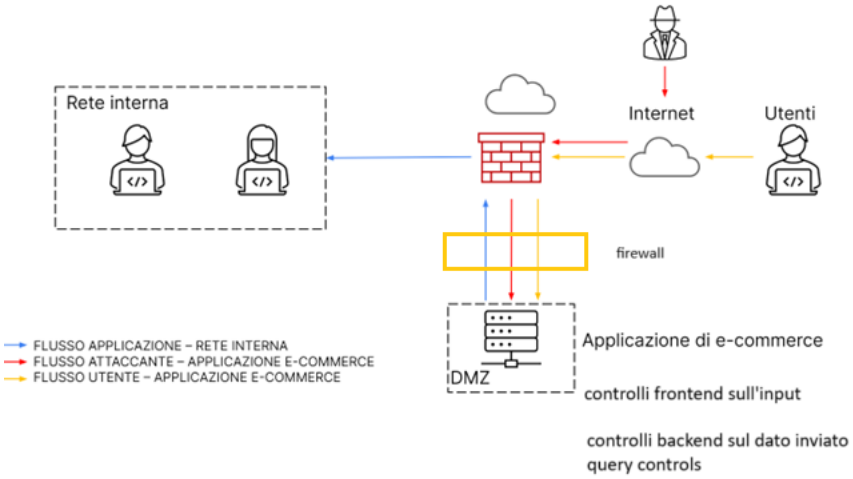


1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

- Limitare i privilegi di ogni utenza, così da non permettere l'esecuzione di query o script da utenti non autorizzati
- Usare query parametrizzate, che usano variabili, non costanti
- Sanitizzazione input a più livelli di codice (non solo controllando a livello codice il contenuto dell'input, ma anche livello api accettando application/json e non text/html)
- Firewall
- Autenticazione per ogni utenza
- Aggiornamento sui vari canali OSINT (alienvault, ciscoTools, …) su nuove vulnerabilità che permettono SQLi o XSS di qualunque tipo
- test periodico contino sulle vulnerabilità per testarne la resilienza



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

- tenere un server di riserva sempre attivo in grado di sostituirsi al server vittima, probabilmente dispendioso rispetto ad altre soluzioni
- accendere/affittare un server e reinstallare/avviare i vari servizi per l'eCommerce nel momento del disastro, meno dispendioso, ma si perdono minuti nel riavviare i vari servizi
- avere una copia dei dati di backup immediatamente accessibile è quasi fondamentale nei casi di incidenti per diminuire il tempo di down service, si consiglia quindi di adottare una buona strategia di backup utilizzabile nel momento in cui il problema sorgesse per una corruzione di dati

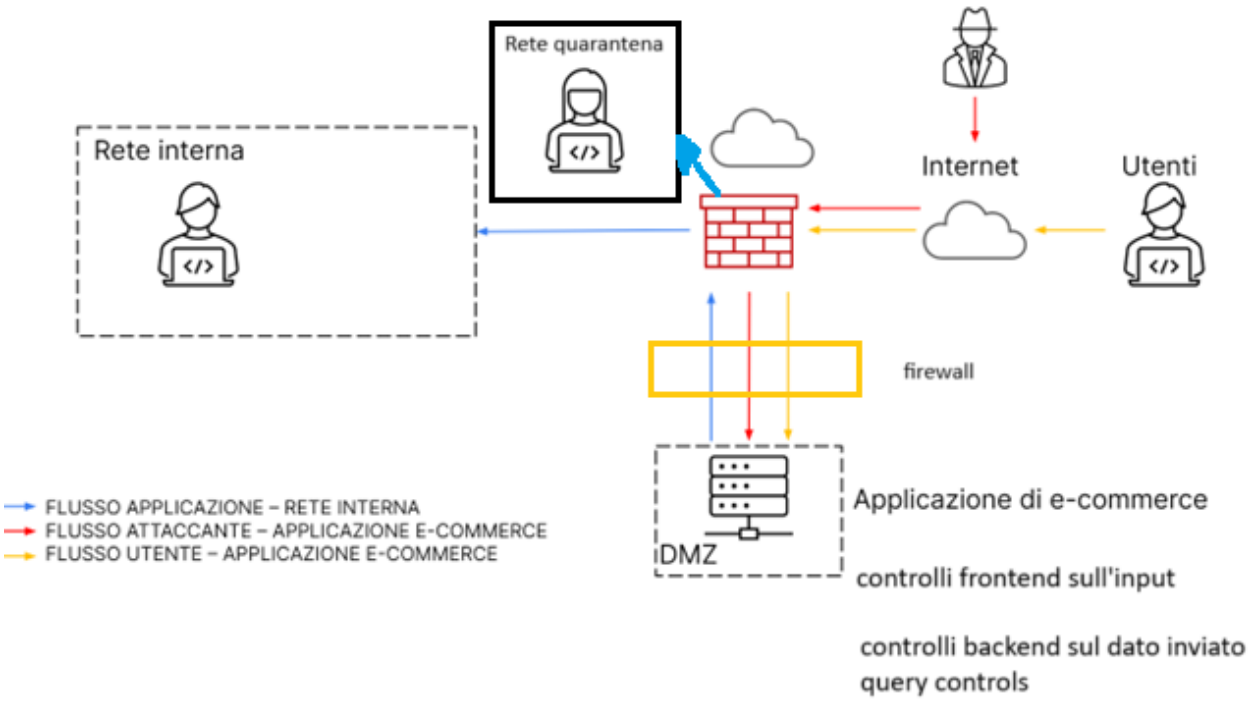
3. Response: l'applicazione Web viene infettata da un malware.

La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a

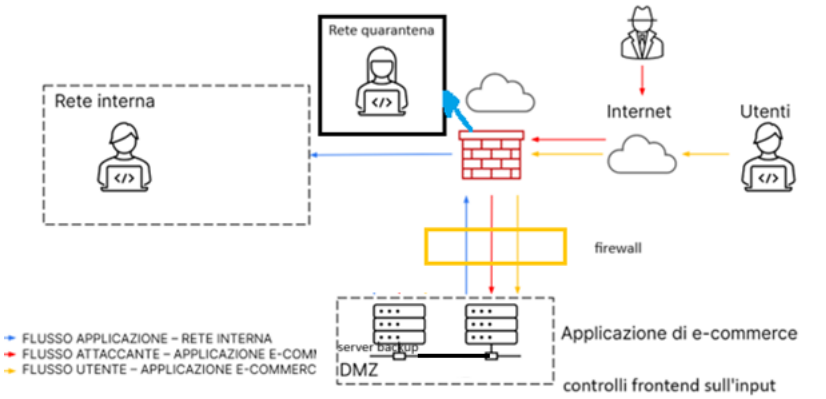
rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

- Dati i requisiti, la soluzione è separare il sistema infetto in una rete di quarantena con la tecnica di segmentazione così da non far propagare il malware nella rete

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



5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)



Applicazione di e-commerce

controlli frontend sull'input

controlli backend sul dato inviato
query controls