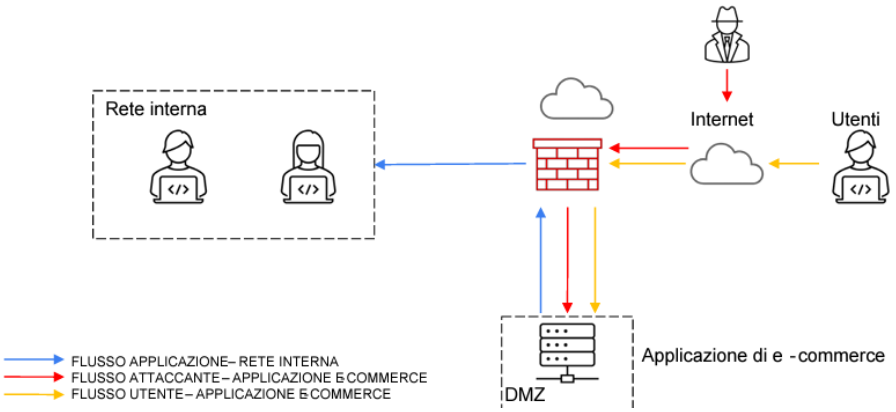
PROGETTO SETTIMANA 9



Seguendo questa architettura di rete bisogna applicare:

1) Protezione contro attacchi SQL injection e XSS.

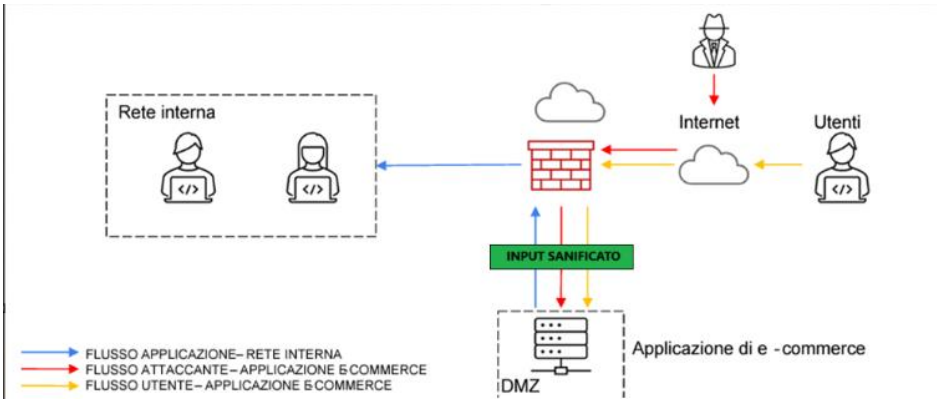
SQL Injection è un tipo di attacco informatico in cui un attaccante inserisce un codice SQL malevolo all'interno delle stringhe di query SQL eseguite da un'applicazione web.

Cross-Site Scripting (XSS) è una vulnerabilità che consente agli attaccanti di inserire script malevoli all'interno delle pagine web che verranno poi visualizzate dagli utenti.

Sono due tipi di attacchi che, se vanno a buon fine permettono all'attaccante di scoprire informazioni riguardanti il database come utenti, password, (SQLi) oppure di rubare informazioni all'utente come i cookie di sessione ed eseguire poi azioni dannose (XSS).

Per difendere l'applicazione web da questi tipi di attacchi occorre validare e verificare tutti gli input dell'utente, sia dal lato client che server, impedendogli di inserire alcuni caratteri come "<", ">", "&", "'" e combinazioni di essi.

Disegno di rete:



2) Impatto sul business

L'applicazione subisce un attacco di DDos dall'esterno che rende l'applicazione non raggiungibile per dieci minuti. Calcolare l'impatto dovuto alla non raggiungibilità del servizio.

Dati:

- Durata dell'attacco = 10 minuti
- Spesa media degli utenti al minuto = 1500€

L'impatto finanziario sarà -> 10 minuti x 1500€/minuto = 15.000€

Come azioni preventive proporrei di aggiungere delle regole nel firewall in modo da bloccare o limitare l'accesso a indirizzi IP sospetti.

Successivamente applicherei delle tecniche di bilanciamento del carico in modo che l'infrastruttura possa gestire carichi elevati di traffico.

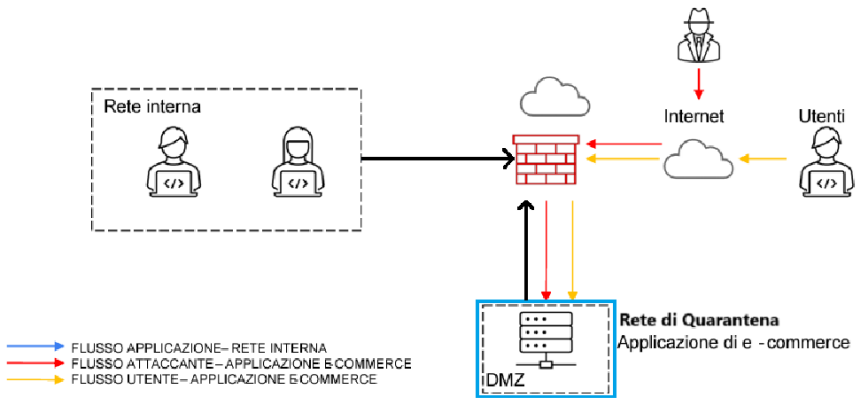
Come ultima azione proporrei di controllare di aver effettuato gli ultimi aggiornamenti.

3) Response

L'applicazione web viene infettata da un malware. La priorità è che il malware non si propaghi sulla rete, non siamo interessati a togliere l'accesso da parte dell'attaccante alla macchina interessata.

In questa circostanza attuerei la tecnica della segmentazione, questa tecnica ci permette di separare l'applicazione di e-commerce dalla rete interna per evitare che il malware si propaghi anche negli altri dispositivi creando una rete separata in cui inserire il sistema infettato. Questa tecnica si attua mettendo il sistema infettato in una rete di quarantena, così facendo l'applicazione di e-commerce si ritrova in una rete creata ad-hoc così come il malware, che non potrà diffondersi.

Disegno di rete:

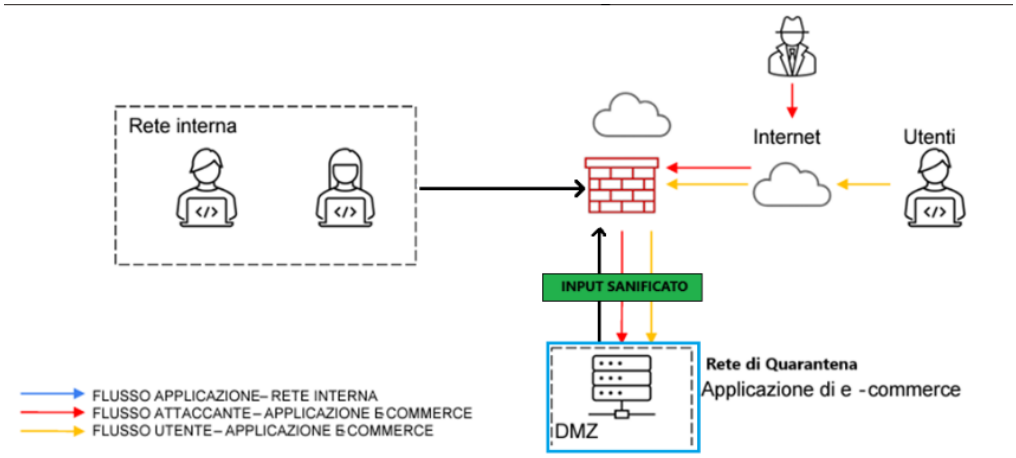


4) Soluzione completa

Questo punto comprende l'unione delle soluzione presentate nel punto 1 e nel punto 3.

In questa soluzione abbiamo sia l'input sanificato per proteggerci da attacchi XSS e SQL injection che l'applicazione web in una zona di quarantena così che in caso di malware, quest'ultimo non si diffonda nella rete interna.

Disegno di rete:



5) Ulteriori misure di sicurezza- Budget 7000€

Come ulteriori modifiche opterei per l'acquisto di un Firewall di nuova generazione (NGFW) in modo da filtrare e gestire il traffico sulla rete. Con un budget così possiamo scegliere un firewall di fascia medio-alta.

Implementerei anche un sistema IDS e IPS in modo da monitorare il traffico e la ricerca di comportamenti sospetti.