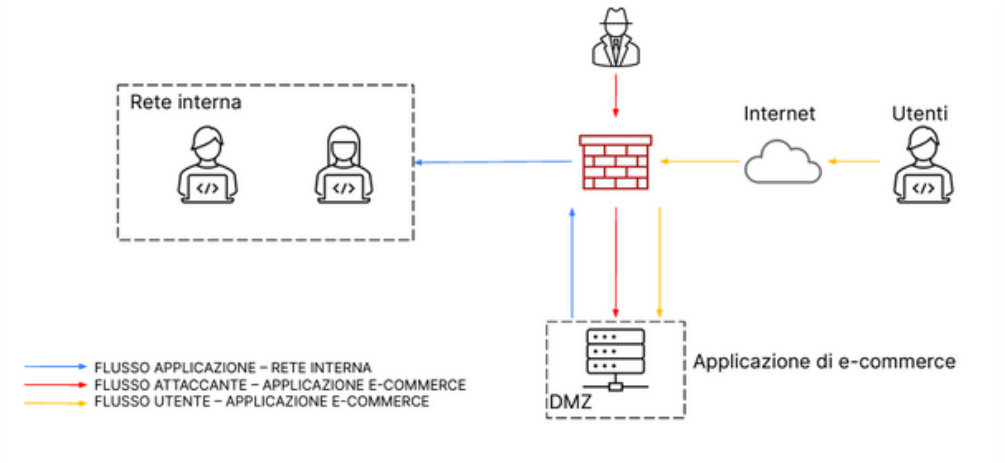
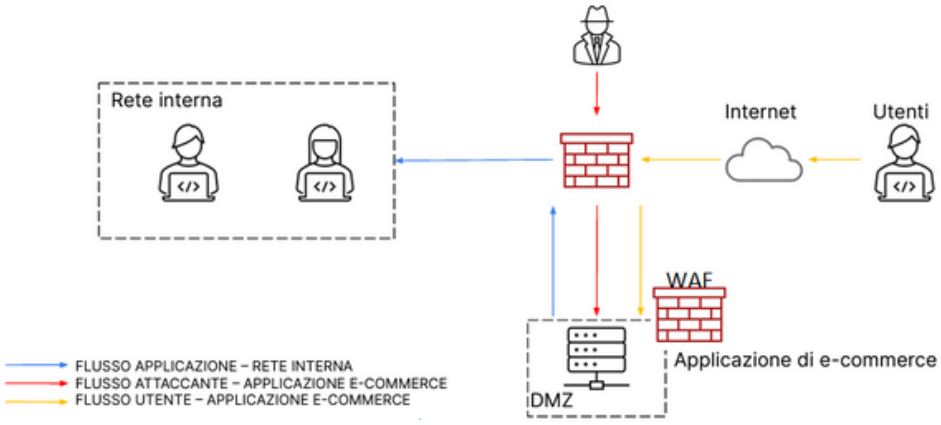
PROGETTO
S9/L5

FERNANDO CATRAMBONE

Con riferimento alla figura sottostante, rispondere ai seguenti quesiti.



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?



Le azioni preventive da applicare per prevenire questo tipo di attacchi sono:

- Impedire l'inserimento diretto di input utente nelle query SQL tramite ad esempio query parametrizzate.
- Validare e sanitizzare tutti gli input dell'utente.
- Mantenere il sistema operativo, il server web e il DBMS aggiornati.
- Eseguire la validazione lato server per garantire che i dati inviati siano conformi alle aspettative.

- Assicurarsi che i caratteri speciali vengano trattati correttamente.
- Evitare l'uso di inline scripting.
- Formare gli sviluppatori sulla sicurezza delle applicazioni web e promuovere le best practices di codifica sicura.

In figura si può notare l'implementazione di un WAF che può identificare e filtrare query dannose o potenzialmente pericolose prima che raggiungano l'applicazione web, e può controllare e validare gli input utente, impedendo l'invio di dati dannosi o potenzialmente pericolosi.

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.

L'impatto sul business è così calcolabile:

Impatto Finanziario = Durata dell'Indisponibilita × Perdita di Guadagno al Minuto

Quindi l'impatto è di 15.000 €.

Le azioni preventive per proteggersi da un attacco Ddos possono essere:

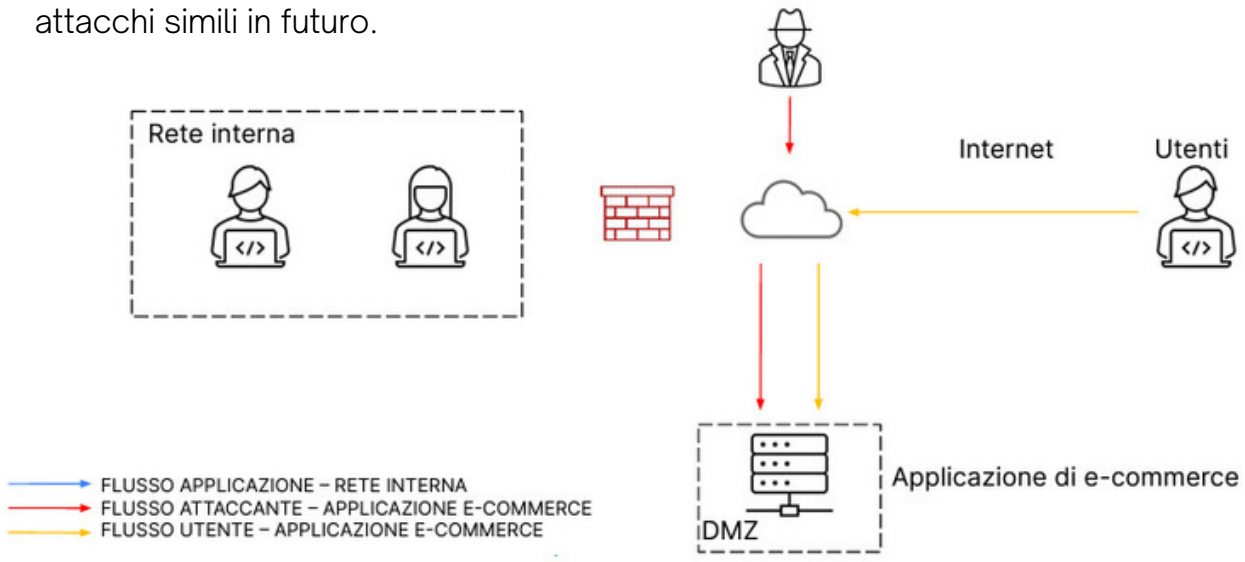
- Configurare correttamente il Firewall per questo tipo di attacchi.
- Utilizzare servizi di mitigazione DDoS offerti da provider specializzati.
- Bilanciamento del carico.
- Monitorare costantemente il traffico per rilevare e rispondere prontamente ad attacchi di questo tipo.
- Filtrare il traffico in modo da limitare l'accesso a indirizzi IP sospetti o noti per partecipare ad attacchi DDoS.
- Considerare l'utilizzo di servizi di protezione DDoS basati su cloud.
- Aggiornare costantemente il sistema.

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.

Nella figura sottostante si può notare come la rete interna sia isolata dalla parte infetta e quindi protetta mentre la DMZ è ancora accessibile all'attaccante e agli utenti.

Le migliori pratiche di response in caso di infezioni mallware sono:

- Isolare immediatamente la macchina infetta, se non spegnerla o rimuoverla del tutto.
- Condurre un'analisi forense per identificare la natura e la portata dell'attacco.
- Ripristinare i sistemi interessati da backup puliti e verificati.
- Identificare e correggere le vulnerabilità.
- Analizzare il malware coinvolto.
- Cambiare tutte le credenziali di accesso compromesse durante l'attacco.
- Potenziare le misure di sicurezza, come l'implementazione di sistemi di rilevamento delle minacce (IDS/IPS).
- Rinforzare la formazione sulla sicurezza informatica tra il personale per ridurre la probabilità di cadere vittima di attacchi simili in futuro.
- Documentare accuratamente l'intero incidente, compresi i dettagli dell'attacco, le risposte adottate e le lezioni apprese. Utile per prevenire attacchi simili in futuro.



GRAZIE

FERNANDO CATRAMBONE