# S9-L5

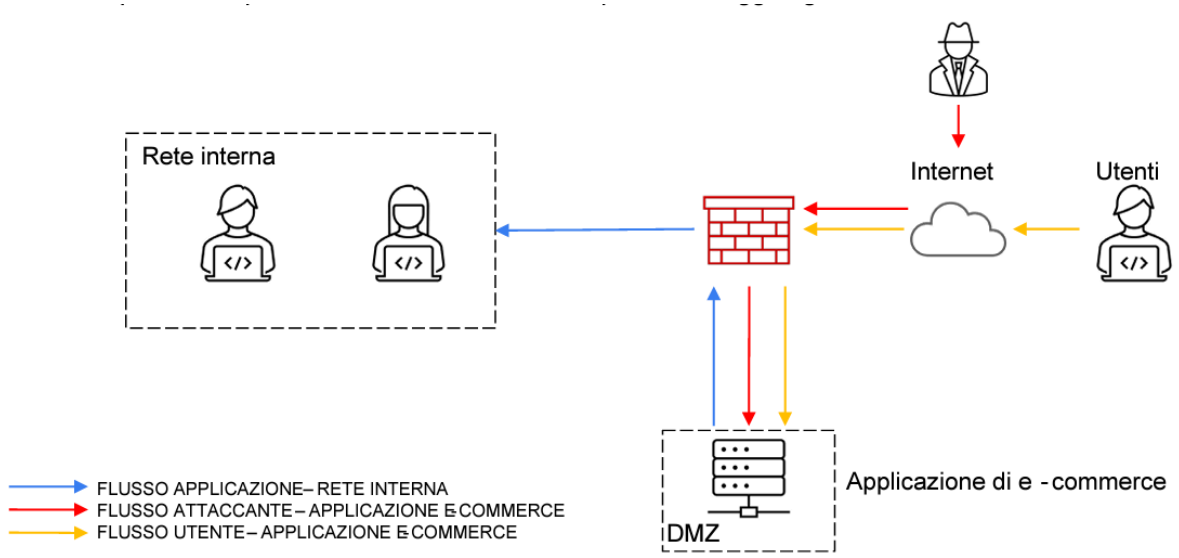
(Bonaldi Cristian)

## Progetto

### Traccia:

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? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica.
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 1.200 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
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 .
4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

## Riferimento in figura:

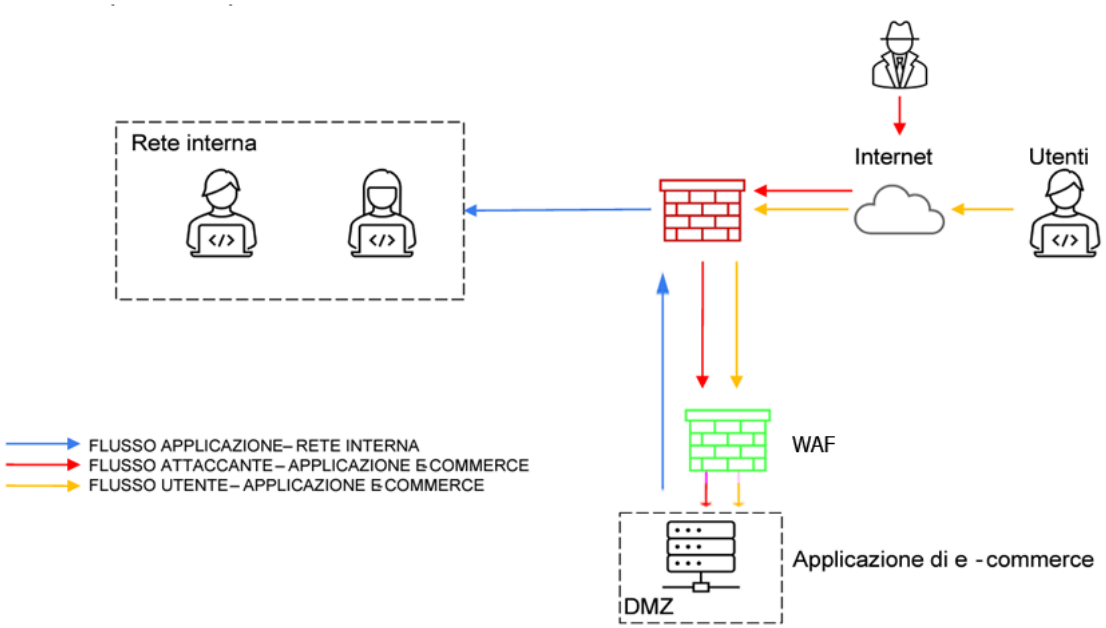



---

## Esercizio e sviluppo:

1.

Partendo dal primo punto, dove vengono richieste delle azioni preventive da implementare per difendere l'applicazione Web da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato, un tipo di soluzione efficace consiste nell'installazione di un WAF (Web Application Firewall):




Infatti un Web Application Firewall (WAF) è uno strumento di sicurezza che protegge le applicazioni web monitorando e filtrando il traffico HTTP/HTTPS in entrata e in uscita. Questo tipo di implementazione applica delle regole predefinite e personalizzate per bloccare attacchi come SQL Injection e XSS. In questo modo, impedisce che il traffico malevolo raggiunga la web application, migliorandone la sicurezza. Come si può notare dalla figura modificata, viene predisposto un WAF per monitorare e proteggere il traffico proveniente da Internet verso la Web Application nella DMZ, mentre la comunicazione con la rete interna resta invariata.

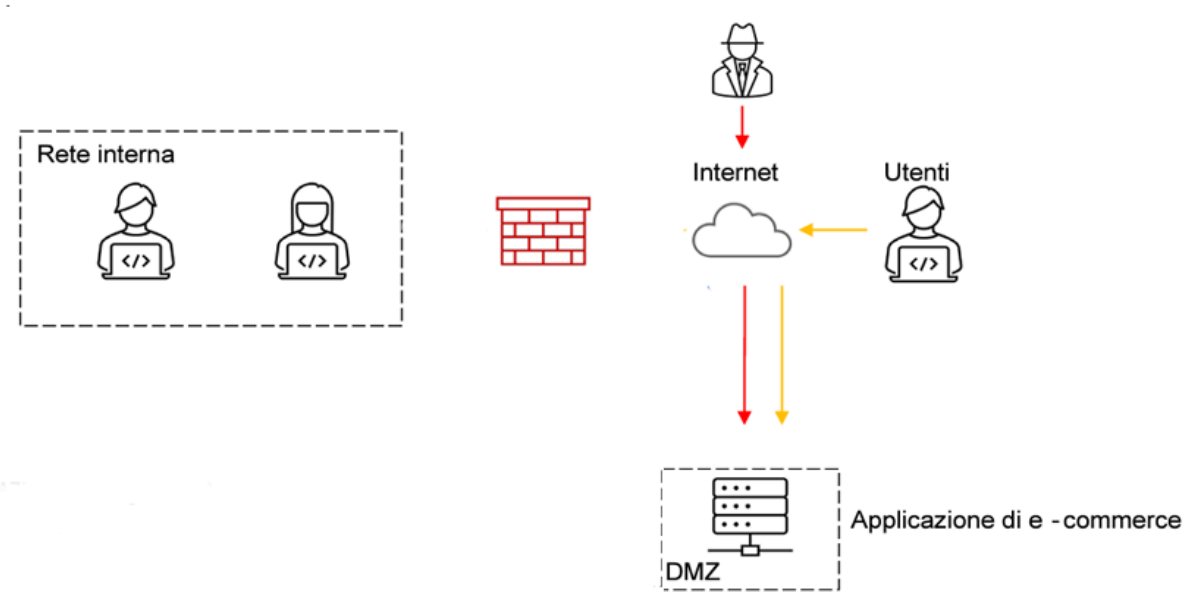
**2.**

Considerando che l'applicazione Web abbia subito un attacco DDoS dall'esterno rendendola non raggiungibile per 10 minuti, e tenendo conto che in media gli utenti spendono 1.200€ ogni minuto sulla piattaforma di e-commerce, si può considerare una perdita economica ai danni dell'azienda di 12.000€ nell'arco di 10 minuti, ovvero durante il periodo di inattività del servizio (1.200€x10m = 12.000€).
Ciò significa che un attacco DDoS può causare significative perdite economiche e interrompere il servizio per un periodo prolungato danneggiando anche la reputazione dell'azienda.
Per questo un'ottima strategia è l'utilizzo di servizi anti-DDoS specializzati (come Cloudflare), in modo da garantire una protezione avanzata bloccando il traffico dannoso prima che raggiunga il sito web, permettendo l'operatività della web app e minimizzando eventuali perdite economiche.

**3.**

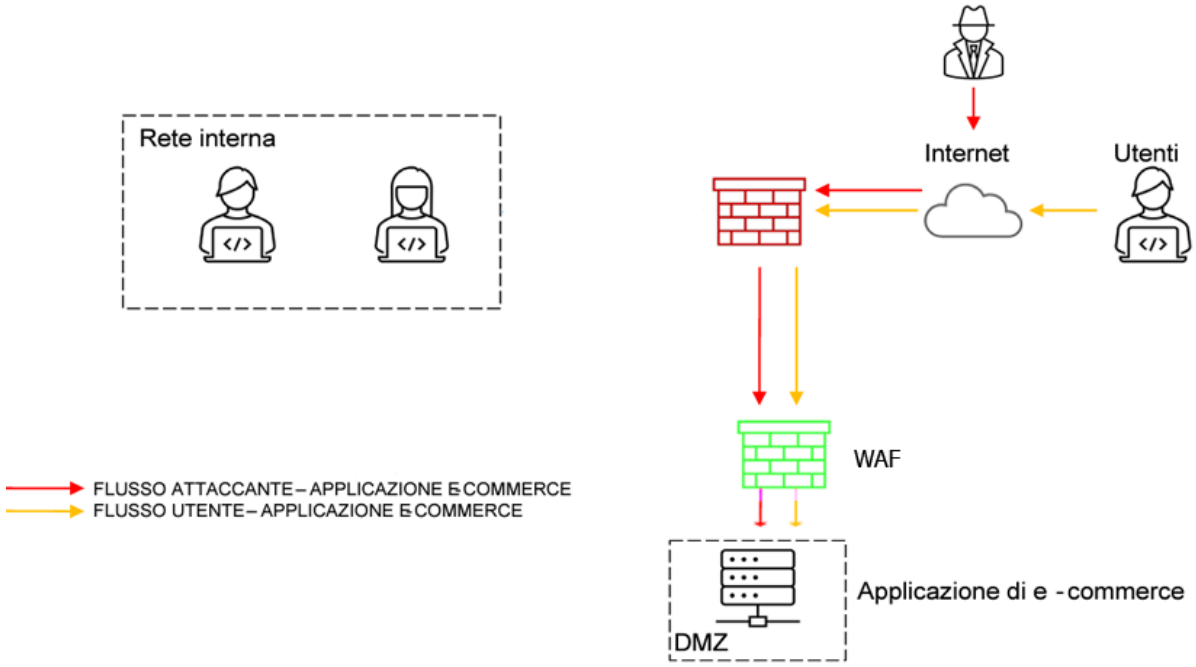
L'applicazione web è infettata da un malware e il nostro obiettivo principale è impedire che il malware si espanda nella rete interna. Per prima cosa, è fondamentale isolare la macchina infetta e di conseguenza la DMZ dalla rete interna per evitare che venga compromessa l'intera infrastruttura. Quindi, manteniamo di fatto la connessione tramite Internet con l'attaccante ma andiamo a

mitigare il danno isolando la macchina dal resto della rete, come mostrato in figura:



4.

Di seguito mostrata la risoluzione del punto 1 e 3:




5.

In questo punto si vanno ad integrare delle soluzioni di sicurezza aggiuntive, considerando un budget tra i 5000-10000€.
Di seguito vengono proposte diverse soluzioni a protezione dell'infrastruttura di rete:

- **Next Generation Firewall**;  garantisce una protezione robusta con ispezione approfondita dei pacchetti, controllo delle applicazioni e prevenzione delle intrusioni.

- **NAS(Network Attached Storage)**: Il NAS protegge i dati con backup regolari aumentando l'affidabilità e la sicurezza delle informazioni aziendali.

- **WAF (Web Application Firewall)**: Il WAF protegge le applicazioni web da attacchi informatici come SQLi e XSS, da exploit noti e sconosciuti, filtrando il traffico HTTP/HTTPS e garantendo la sicurezza e la disponibilità dei servizi web.

- **UPS (Uninterruptible Power Supply)**: l'UPS è fondamentale perché previene la perdita di dati e danni ai dispositivi all'interno di un'azienda, mantenendo operativi i servizi essenziali durante eventuali interruzioni di corrente.

- **Segmentazione di rete**: segmentare correttamente la rete aziendale è importante per  limitare la diffusione di attacchi e migliorare l'efficienza della rete. Questo riduce il rischio di accessi non autorizzati e protezione dei dati sensibili.
- **IDS e IPS**: In ultima analisi si va a consigliare l'applicazione di sistemi di detenzione e prevenzione delle intrusioni, quindi dispositivi per il monitoring del traffico di rete per identificare attività sospette e per la prevenzione di possibili minacce.

Si può valutare una o più delle precedenti proposte in relazione al budget espresso, onde evitare ripercussioni future ancora più gravi in termini economici.