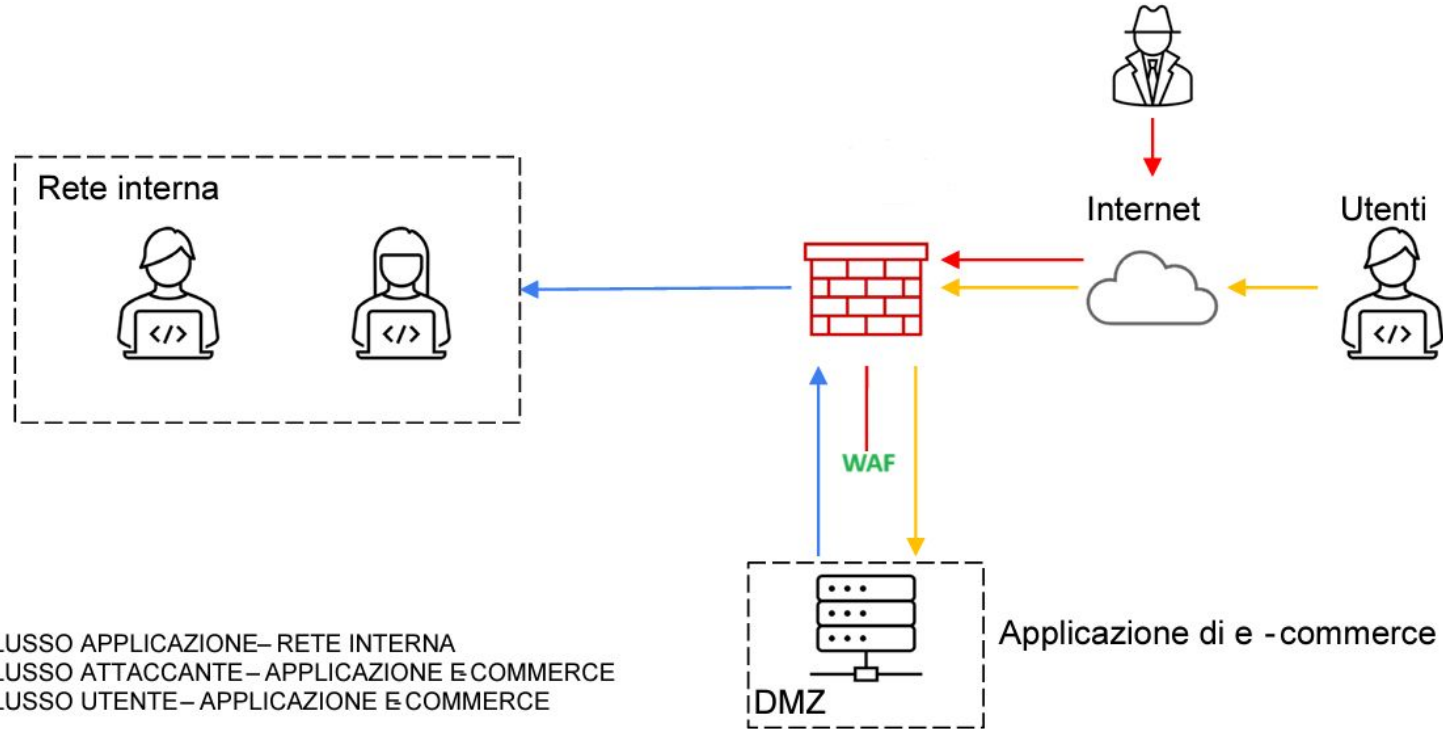


1) Per difendere un'applicazione web da attacchi di tipo SQLi (SQL Injection) e XSS (Cross-Site Scripting) da parte di utenti malintenzionati, una delle soluzioni comuni è l'implementazione di un Web Application Firewall (WAF). Un WAF è un'applicazione firewall che opera a livello di applicazione per filtrare e monitorare il traffico HTTP tra un'applicazione web e l'utente finale. Esso può essere configurato per identificare e bloccare gli attacchi di tipo SQLi e XSS, oltre a fornire altre funzionalità di sicurezza.

Protezione con il WAF






Calcolo dell'impatto finanziario causato da un DDoS

2) Per calcolare l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS, dobbiamo moltiplicare il numero di minuti di indisponibilità per il valore medio generato dagli utenti sulla piattaforma di e-commerce per minuto. Quindi, per calcolare l'impatto finanziario della non raggiungibilità del servizio per 10 minuti, possiamo usare la seguente formula: $\text{Impatto finanziario} = 1.500 \text{ €/min} * 10 \text{ min} = 15.000 \text{ €}$ (Impatto finanziario = Valore per minuto * Minuti di indisponibilità).

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa dell'attacco DDoS è di 15.000 €



Eventuali valutazioni di azioni preventive che si possono applicare in questa situazione

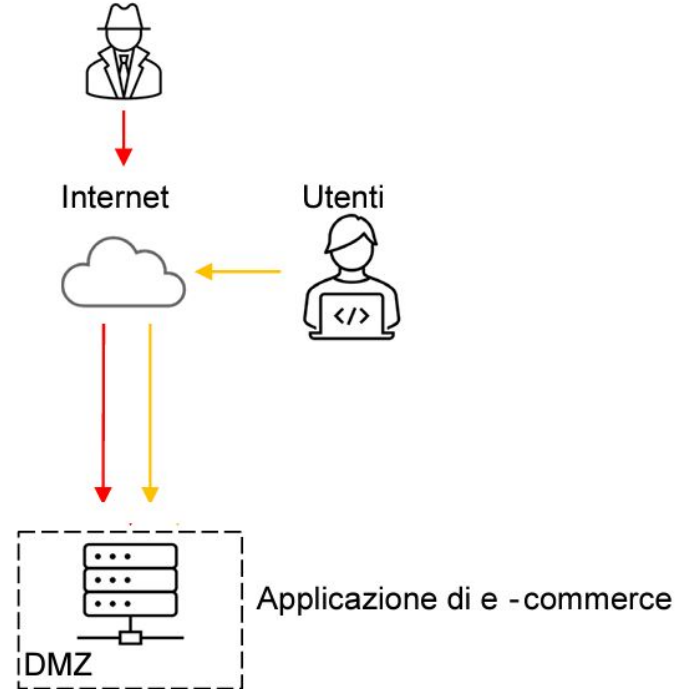
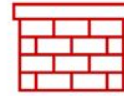
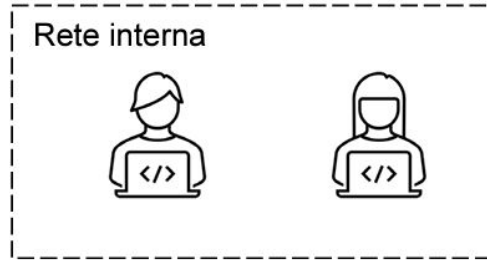
Per prevenire o mitigare gli attacchi DDoS e ridurre l'impatto finanziario della non raggiungibilità del servizio, è possibile adottare diverse azioni preventive: implementazione di un sistema di mitigazione DDoS, bilanciamento del carico, utilizzo di servizi di protezione DDoS, monitoraggio del traffico, configurazione di limiti di traffico, utilizzo di servizi di mitigazione DNS, test e ottimizzazione della rete, Pianificazione della risposta agli incidenti, formazione del personale.



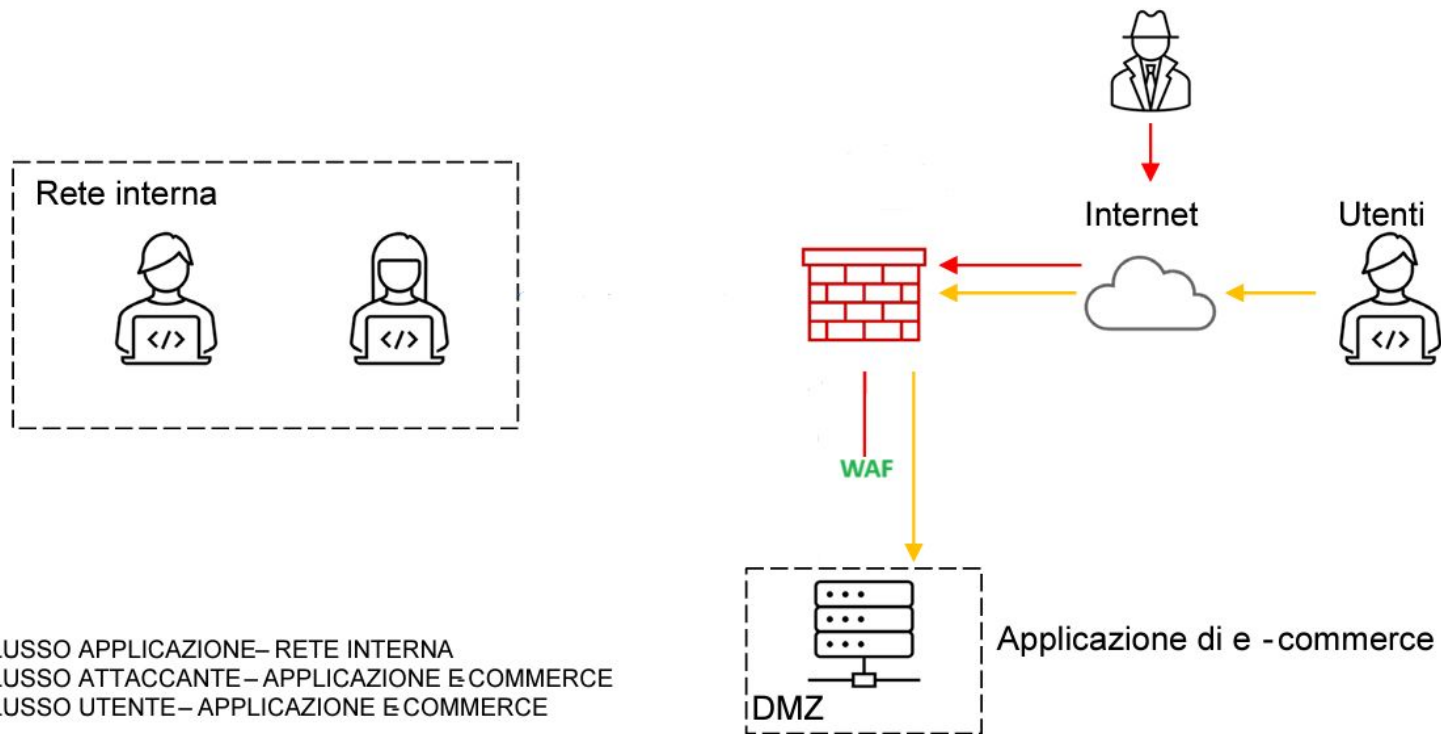
Isolamento

3) Per affrontare questa situazione, la priorità è impedire la propagazione del malware sulla rete senza rimuovere l'accesso dell'attaccante alla macchina infetta. Ecco una possibile soluzione sarebbe l'isolamento della macchina infetta: isolare la macchina infetta dal resto della rete utilizzando VLAN (Virtual LAN) o segmenti di rete separati. In questo modo, si impedisce al malware di diffondersi ad altri dispositivi sulla rete.

Isolamento



Unione dell'azione preventiva e response





Modifica <<più aggressiva>> dell'infrastruttura

Per una modifica <<più aggressiva>> dell'infrastruttura, per affrontare l'infezione da malware senza rimuovere l'accesso dell'attaccante alla macchina infetta, è possibile integrare ulteriori elementi di sicurezza per rafforzare le difese. Ecco alcuni elementi: sandboxing, honeypots, analisi comportamentale, deception technology, endpoint detection and response (EDR), segmentazione della rete, machine learning e intelligenza artificiale, autenticazione a più fattori (MFA), backup e ripristino dei dati, test di penetrazione. Questi elementi aiutano a creare un perimetro di sicurezza più robusto e ad aumentare le possibilità di rilevare e mitigare gli attacchi avanzati.