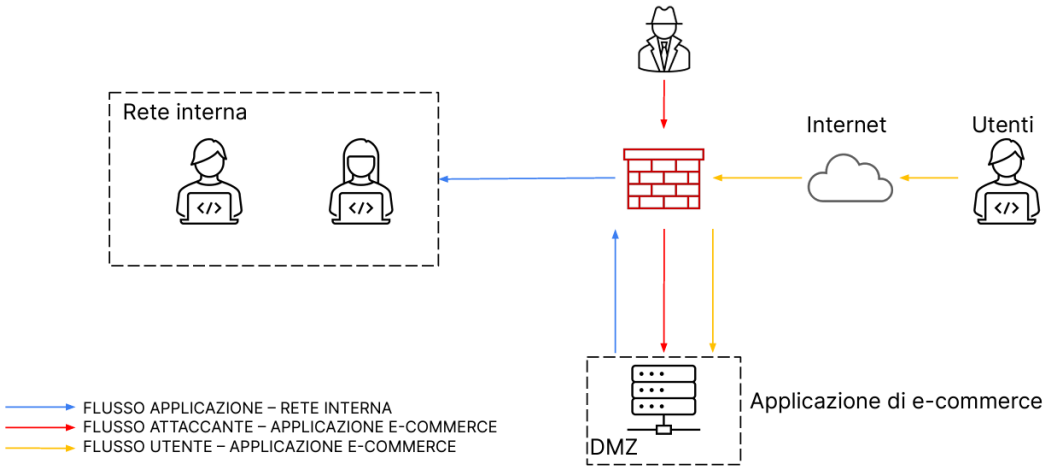
S9/L5

Davide Diglio



Traccia

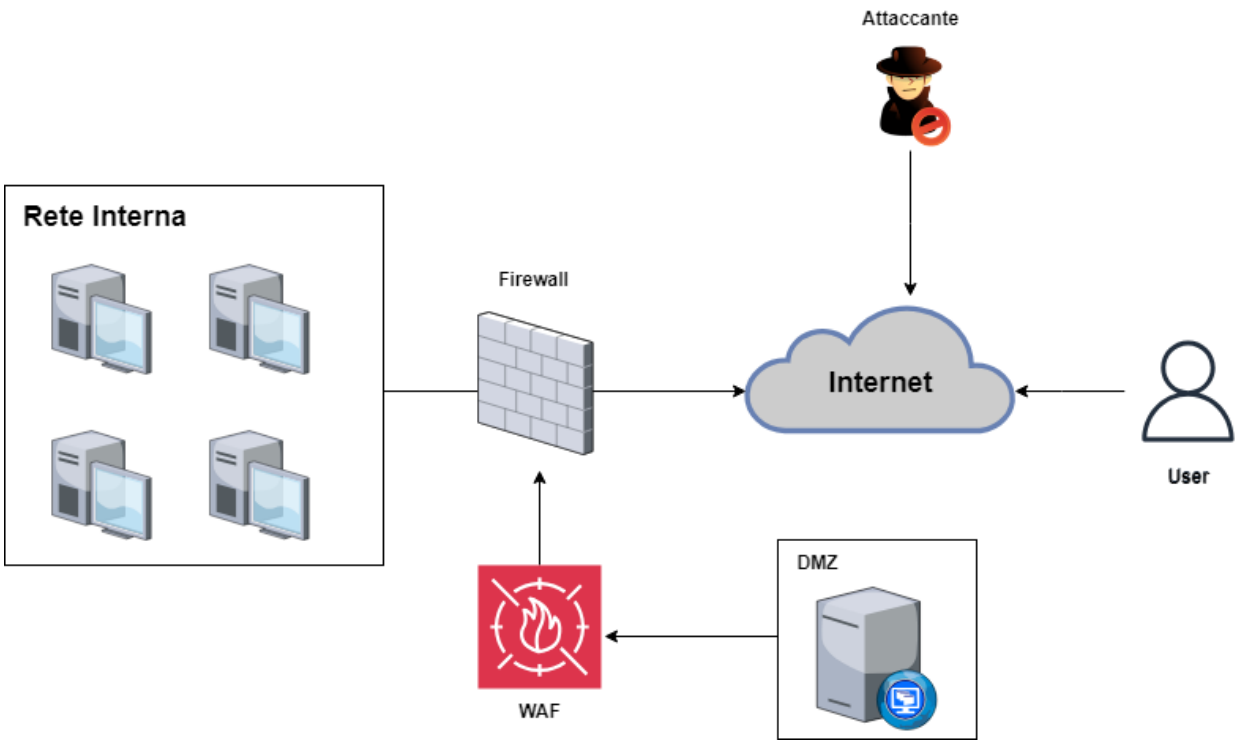
Rispondere ai seguenti quesiti:

- 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?
- 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.
- 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.

Svolgimento

Parte I: Azioni preventive

Per difendere l'applicazione Web da attacchi SQLi o XSS, si posso implementare varie difese. Ad esempio, utilizzando un dispositivo di sicurezza come il WAF, che la sua funzione è quella di filtrare e monitorare il traffico, bloccando eventuali attacchi.



Si consiglia anche di mantenere i server DMZ sempre aggiornati le patch di sicurezza, eseguire i backup dei dati, per garantire al sicuro i dati.

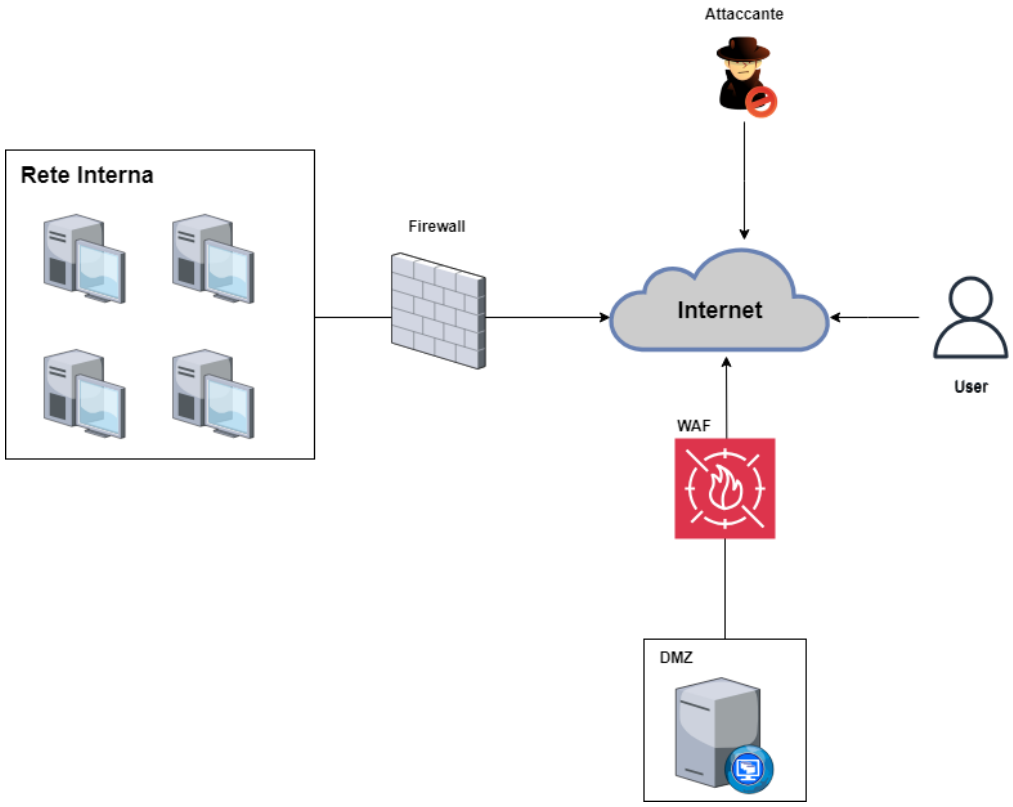
Parte II: Impatti sul business

L'applicazione Web non è raggiungibile per 10 minuti per colpa di un attacco Ddos. L'impatto sul business dovuto alla non raggiungibilità del servizio è di 1.500 euro ogni minuto. Calcolando si arriva a 15.000 euro di danni sulla piattaforma e-commerce, per prevenire questa perdita si possono adottare delle soluzioni, ad esempio utilizzando server

di backup o servizi tipo quelli di ridondanza. Si può anche limitare l'accesso ai servizi necessari e utilizzare una buona sicurezza, utilizzando un firewall per gli attacchi DDos.

Parte III: Response

Per non far propagare il malware sulla rete si può isolare e-commerce dalla rete interna per evitare la diffusione del malware.



In questo modo l'attaccante potrà attaccare e-commerce protetto dal WAF, e se nel caso lo superasse, non potrà andare nella rete interna perchè è stata isolata.