Analisi dei log: caso reale

EPICODE

Cybersecurity Specialist

NOV23

Progetto S9/L5

di Manuel Perelli

Indice

Introduzione

Nel progetto di questa settimana, ci concentreremo sulle azioni preventive all’interno di una rete aziendale di un e-commerce. Valuteremo gli impatti sul business e definiremo le azioni correttive da intraprendere in caso di incidente di sicurezza.

Traccia

STEP 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?

STEP 2

Impatti sul business

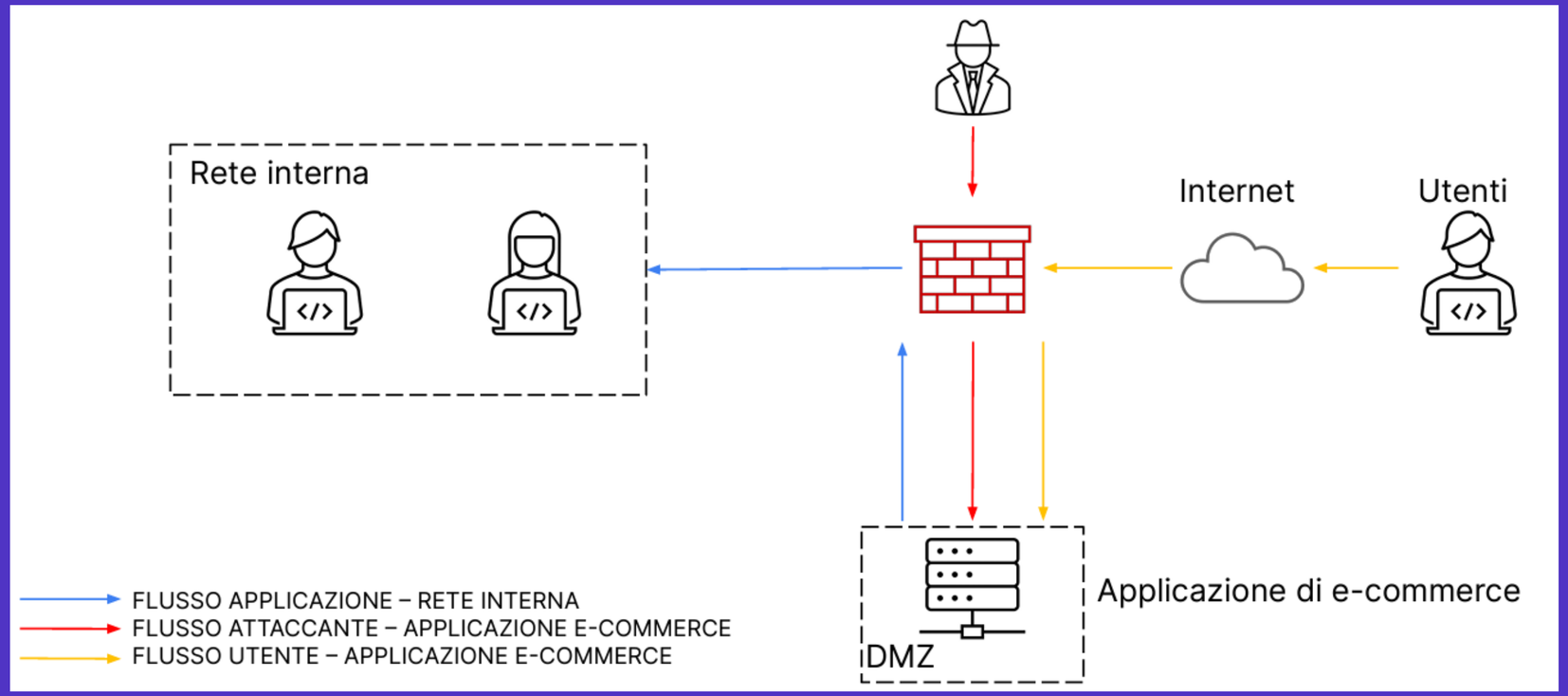
L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

STEP 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.

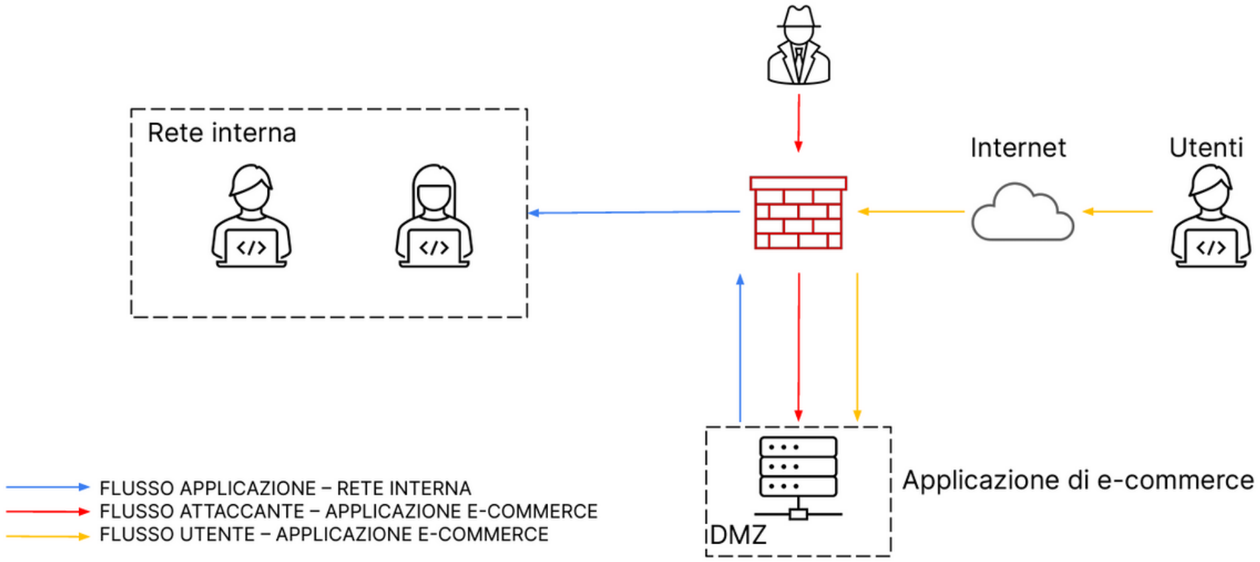
Architettura di rete



L’applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

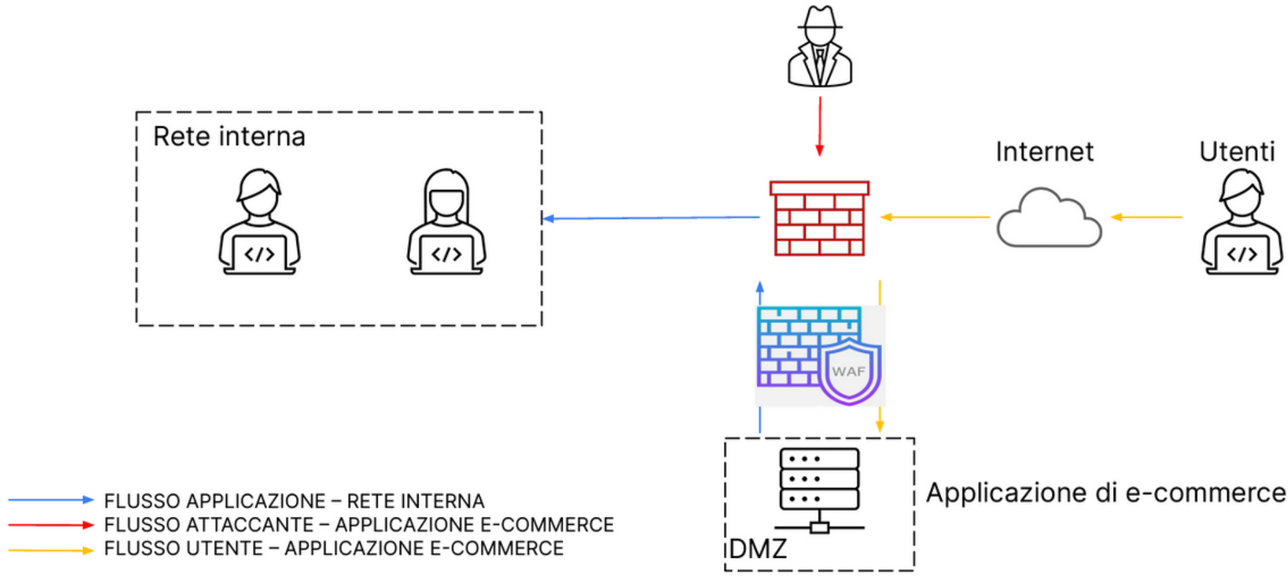
STEP 1: Azioni preventive

Prima



- La rete è dotata soltanto di un comune firewall.

Dopo



- Per una maggiore sicurezza aggiungiamo un Web Application Firewall tra la DMZ e la rete esterna.

Cos‘è un Web Application Firewall?

Un Web Application Firewall (WAF) è uno strumento progettato per proteggere le applicazioni web filtrando e monitorando il traffico HTTP tra l’applicazione web e Internet.
Il WAF opera a livello 7 del modello OSI, filtrando il traffico in ingresso e applicando regole (chiamate policy) per rilevare e bloccare il traffico dannoso. Funziona come un reverse-proxy, proteggendo il server dall’esposizione diretta.

Il WAF protegge le applicazioni web da attacchi dannosi, inclusi:

- Cross-Site Scripting (XSS): iniezione di script malevoli all'interno delle pagine web visualizzate dagli utenti.
- SQL Injection: inserimento di comandi SQL malevoli per compromettere il database dell'applicazione.
- Inclusione di file: tentativi di caricare file dannosi o eseguibili all'interno dell'applicazione.
- Cross-Site Forgery (CSRF): un attacco in cui un utente malintenzionato sfrutta l'autenticazione di un utente legittimo per eseguire azioni non autorizzate.

STEP 2:
Impatti sul business

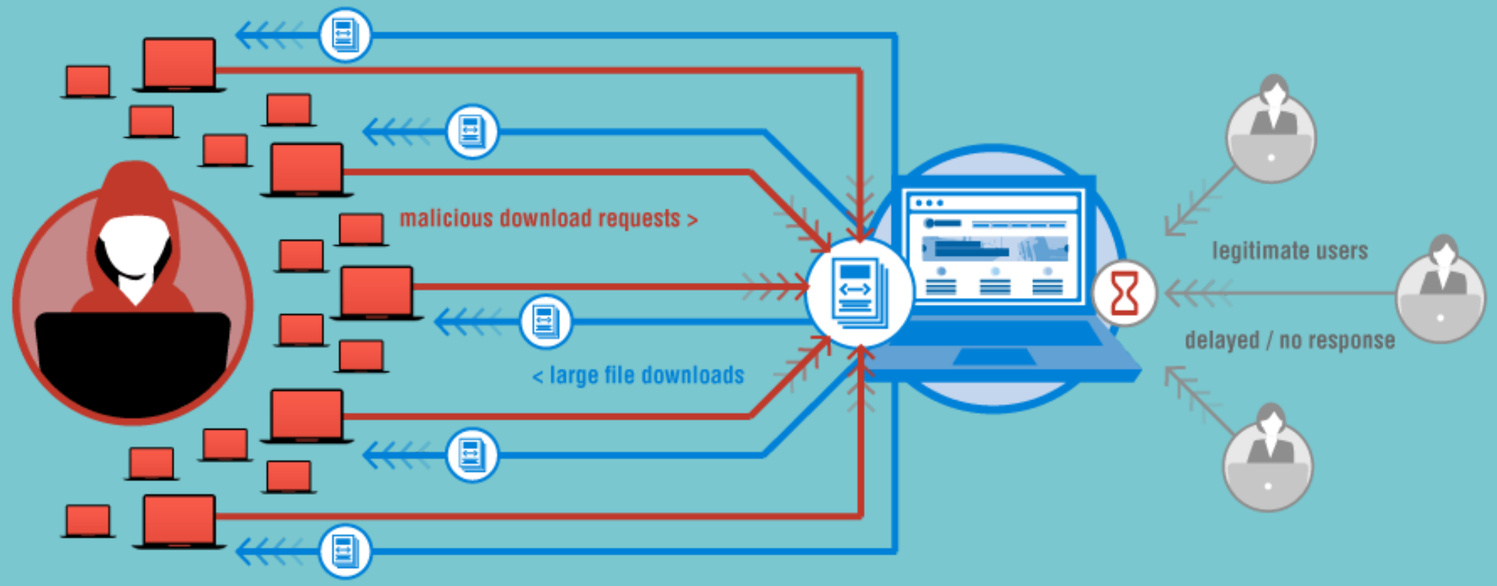
L’applicazione Web subisce un attacco di tipo DDoS dall’esterno che rende l’applicazione non raggiungibile per 10 minuti. In media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

1.500€ X 10 = 15.000€

L’e-commerce perderebbe 15.000€. Se questo avvenisse ogni settimana parleremmo di perdite di fatturato nell’ordine delle centinaia di migliaia di euro.

Cos'è un attacco DDoS?

L'acronimo DDoS sta per "Distributed Denial of Service". In pratica, durante un attacco DDoS, il servizio viene inondato da una grande quantità di richieste fasulle provenienti da molteplici fonti contemporaneamente.
Gli attacchi DDoS saturano le risorse del sistema bersaglio, impedendo ai legittimi utenti di accedere al servizio. Questo avviene attraverso l'invio di un elevato volume di traffico, che può essere generato da botnet o altre risorse distribuite.

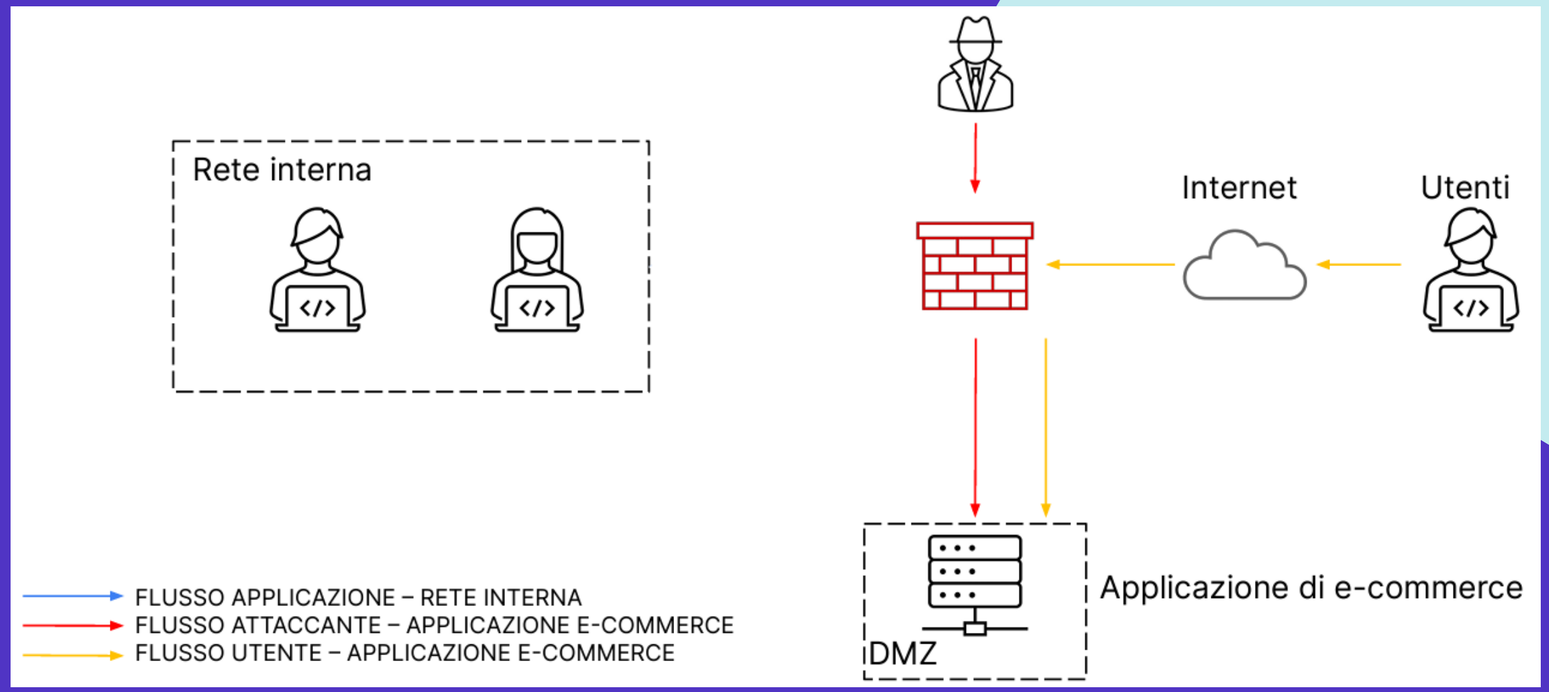


☂ Come possiamo proteggere l'applicazione web da attacchi DDos?

Un Web Application Firewall (WAF) può contribuire a mitigare gli attacchi DDoS. Ecco come:

- Filtraggio del traffico: un WAF può rilevare e filtrare il traffico sospetto o anomalo proveniente da indirizzi IP noti per essere parte di una rete di bot DDoS.
- Rate limiting: il WAF può limitare il numero di richieste da un singolo indirizzo IP in un determinato intervallo di tempo. Questo rallenta gli attacchi DDoS che dipendono da un alto volume di richieste.
- CAPTCHA: "Completely Automated Public Turing test to tell Computers and Humans Apart" che verifica che chi interagisce con il sito web sia umano o bot

STEP 3: Response



Grazie ad un processo di segmentazione separiamo il server dell'applicazione web dalla rete interna. Questo non permetterà al malware di propagarsi e bloccherà l'accesso all'hacker alla rete interna. L'applicazione resterà comunque accessibile e fruibile dalla rete internet per non impattare il business dell'e-commerce

Conclusioni

La sicurezza di un’applicazione web richiede un approccio multilivello che include misure preventive, una risposta efficace agli attacchi e una comprensione dell’impatto potenziale degli attacchi sul business.
Implementando queste strategie, si può migliorare notevolmente la resilienza dell’applicazione web agli attacchi.