PREVENZIONE, IMPLEMENTAZIONE DI SICUREZZA E RESPONSE

Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

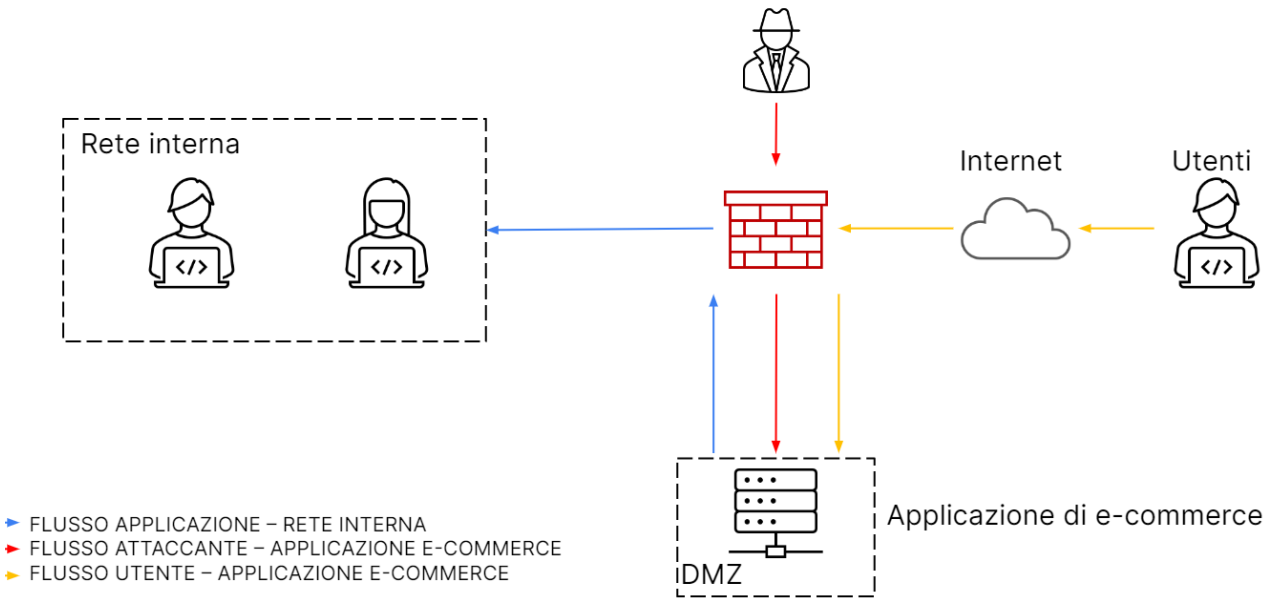
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni

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.

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

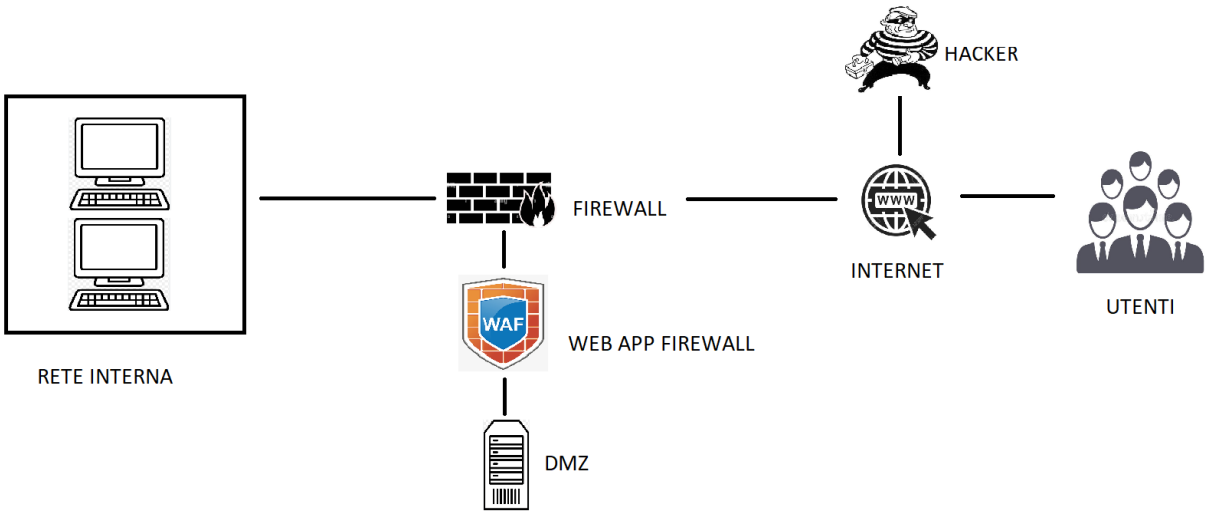
5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo)**



1. Azioni preventive contro SQLinjection o XSS:

Il metodo più efficace per prevenire questi 2 tipi di attacchi su una Web Application è quello di aggiungere un Web Application Firewall che permette, in modo molto semplificato, di intercettare e analizzare traffico HTTP, operando quindi al livello applicativo a differenza di un normale firewall che lavora a livello di pacchetti; sarebbe più opportuno utilizzare WAF 3.0 che proteggono da attacchi 0-day (gli attacchi maggiormente usati tra gli hacker per via proprio della mancanza di misure di controllo, essendo vulnerabilità ancora sconosciute agli sviluppatori) che localizza e identifica le vulnerabilità.

Di seguito il link da cui ho preso queste informazioni:
https://www.zerounoweb.it/cloud-computing/waf-significa-web-application-firewall-che-cos-e-come-funziona-e-a-cosa-serve/



2. **Impatto sul business attacco DDoS**

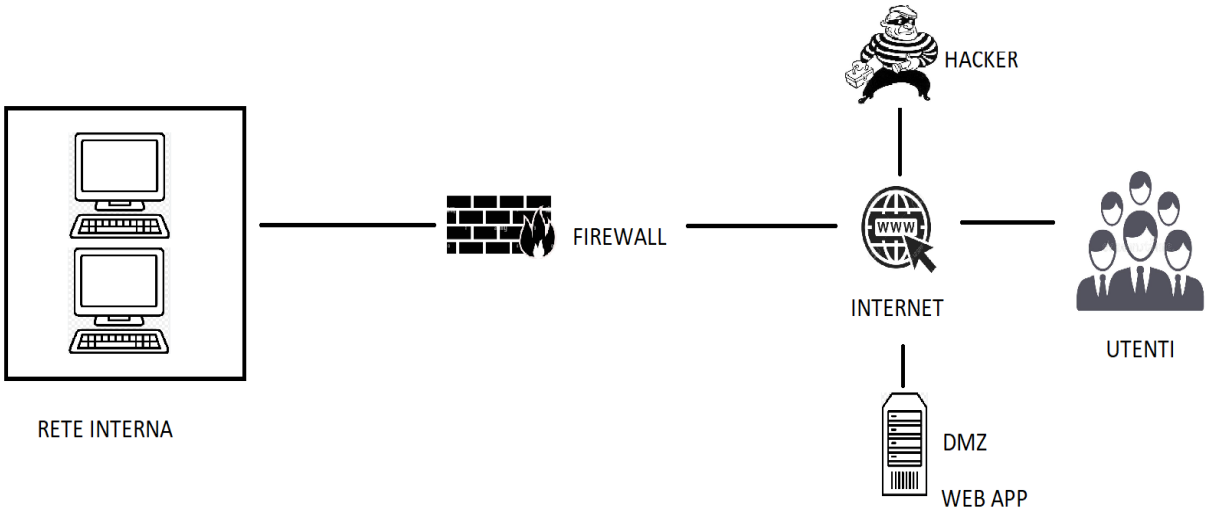
Avendo subito un attacco DDoS, ovvero distributed denial of service, invio di molteplici pacchetti verso un server da più pc (botnet) in modo da esaurire le sue risorse fino a renderlo inaccessibile per un determinato periodo di tempo, la web app è rimasta irraggiungibile per 10 minuti; secondo un'accurata stima, gli utenti in media spendono sul nostro sito e-commerce 1500 € ogni minuto, quindi la perdita economica a causa del DDoS sarà di 15000 € (1500x10).

3. **Incident Response**

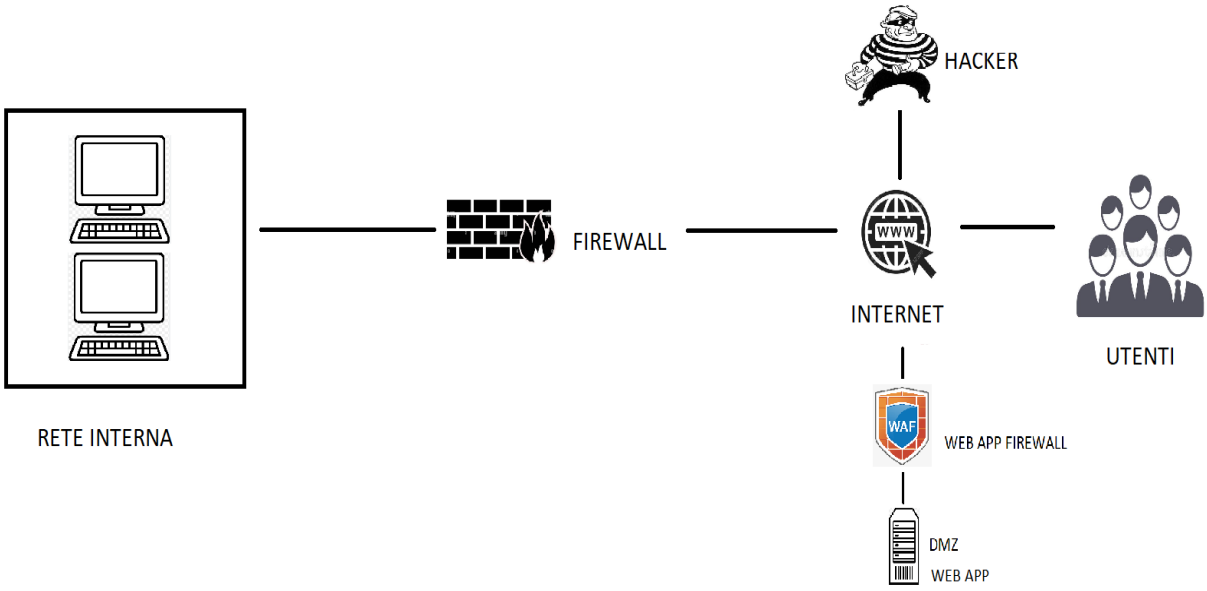
La nostra Web App è stata infettata da un malware e il nostro scopo è quello di non farlo propagare verso la nostra rete interna, senza però eliminare il collegamento verso internet e verso l'attaccante.

Il modo migliore per operare in questo caso è la tecnica di **isolamento**, cioè disconnettere completamente il sistema infetto dalla rete interna, lasciando solamente la comunicazione con internet; questo permette comunque all'attaccante di rimanere collegato col sistema infetto, ma anche agli utenti di

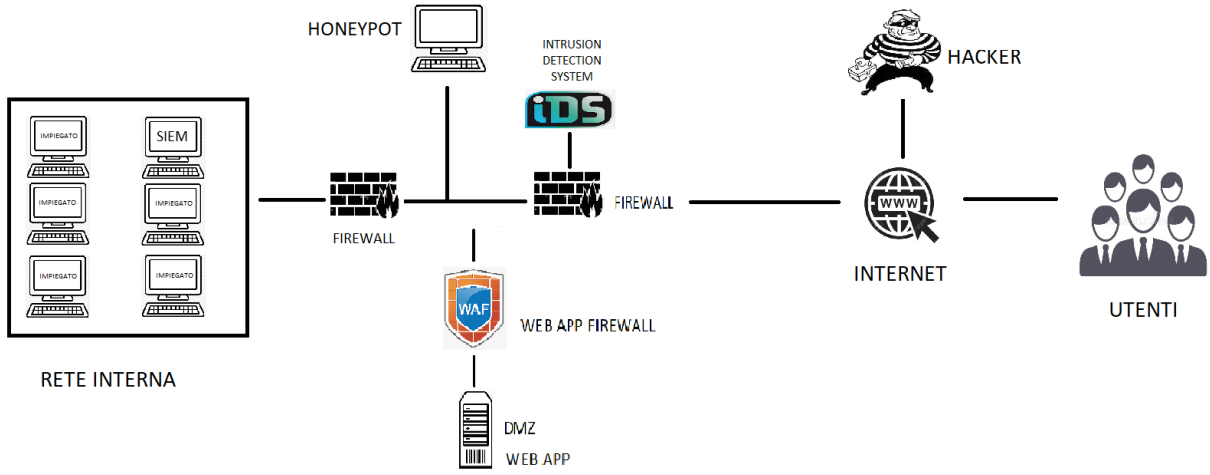
continuare ad effettuare operazioni sulla web app.



4. **Soluzione completa, prevenzione e response**



5. **Infrastruttura con sistemi di sicurezza avanzati**



Per proteggere ulteriormente la rete, si potrebbe aggiungere un IDS (magari integrato al primo firewall) che ci permette di rilevare pacchetti a livello di rete, trasporto e applicativo potenzialmente pericolosi;

proteggere la Web App nella DMZ con un WAF 3.0 che, come già detto nel punto 1, filtra il traffico HTTP, oltre che identifica e localizza le vulnerabilità ed è molto efficace nel contrastare attacchi SQLi e XSS che sono tra i più pericolosi per un sito web di e-commerce;

si potrebbe anche aggiungere un honeypot, computer esca che sembra essere parte della rete, ma che in realtà non contiene informazioni preziose ed è isolato dal resto del network interno (nel nostro caso, come si può vedere dall'immagine, è delimitato da 2 firewall e un WAF);

consiglierei di aggiungere un ulteriore firewall a protezione della rete interna che filtrerebbe sia il traffico in entrata che in uscita, in modo da proteggere ulteriormente la rete interna;

il tutto collegato ad un SIEM, log collector che permette al SOC, security operation center, di monitorare tutti gli eventi che accadono nella rete in questione; al SIEM infatti, saranno mandati i log di tutti gli apparati di rete connessi ad essa.