PROGETTO SETTIMANALE UNIT 3 WEEK 1

Cuore Andrea

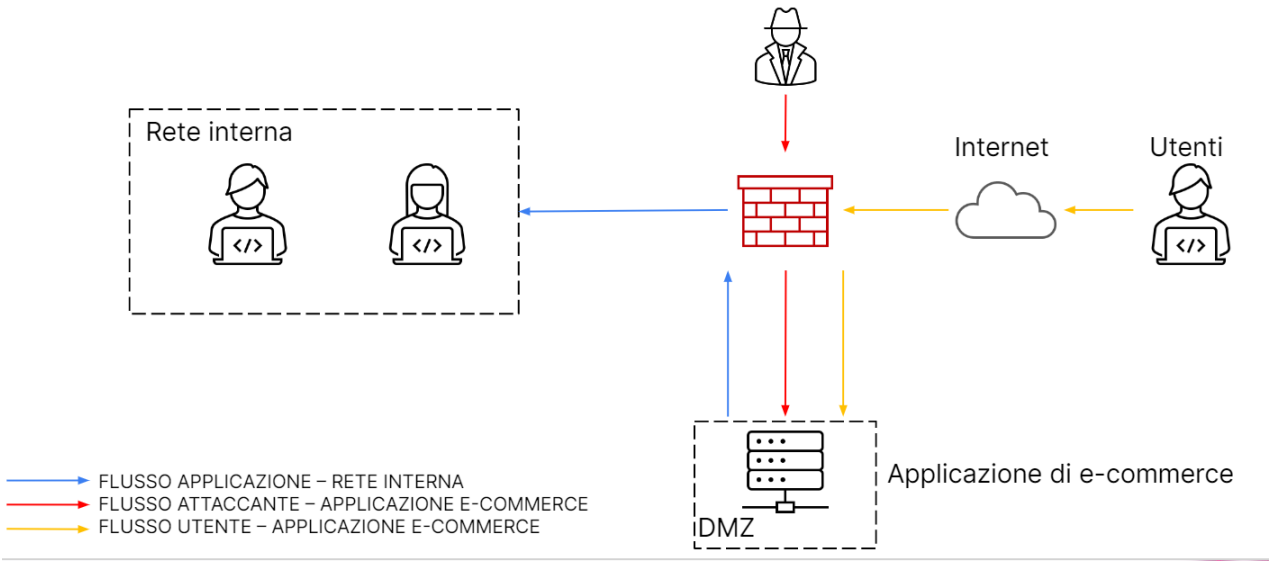
23/12/2022

TRACCIA:

In un'architettura di rete per un e-commerce ci troviamo davanti a diverse casistiche

1) Azioni preventive in caso di attacco XSS/SQLi
2) Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio per 10 minuti, a seguito di un attacco DDoS, sapendo che in media gli utenti spendono 1.500€ ogni minuto sulla piattaforma di E-commerce.
3) Azioni di response: L'applicazione web viene infettata da un malware
    a. Evitare che il malware si propaghi sulla rete
    b. Rendere accessibile il sito
    c. Non rimuovere l'accesso, ma monitorare l'attaccante
4) Soluzione completa: unire le soluzioni di prevenzione e di response
5) Modifica dell'architettura di rete

Architettura iniziale:



Azioni di prevenzione in caso di attacco XSS/SQLi

Come ben sappiamo, la tipologia di attacchi XSS/SQLi usano come vulnerabilità il mancato controllo da parte dell'input utente. Per ovviare a questo problema utilizziamo il WAF. Questo strumento infatti può controllare l'input utente e verificare che non vi siano azioni di tipo XSS/SQLi, di base i WAF hanno già un gruppo di regole preinstallate che copre sia il reparto SQLi che XSS.

Regole WAF SQLi:

- SQLiExtendedPatterns_QUERYARGUMENTS
- SQLi_QUERYARGUMENTS
- SQLi_Body
- SQLi_COOKIE
- SQLi_URIPATH

REGOLE WAF XSS:

-CrossSiteScripting_COOKIE

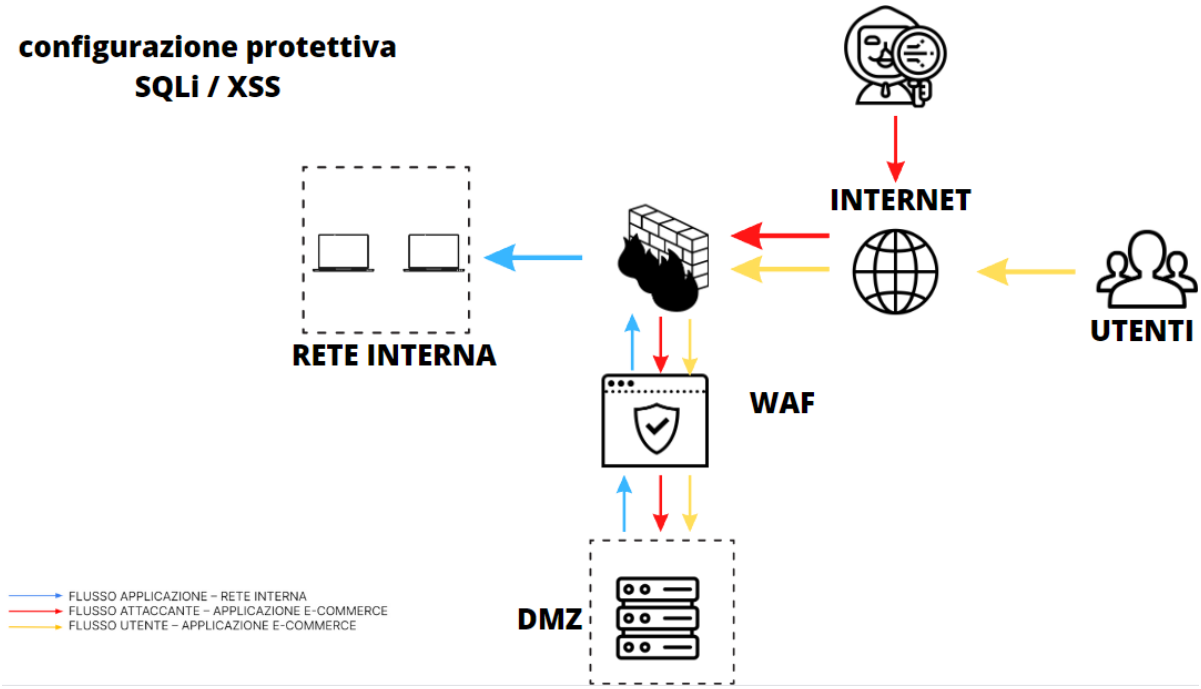
-CrossSiteScripting_QUERYARGUMENTS

-CrossSiteScripting_BODY

-CrossSiteScripting_URIPATH

Fonte: Regola AWS WAF per impedire SQLi e XSS (amazon.com)

N.B: Le regole scritte con questa formattazione appartengono al WAF di Amazon, in altri WAF potrebbero avere una formattazione diversa.



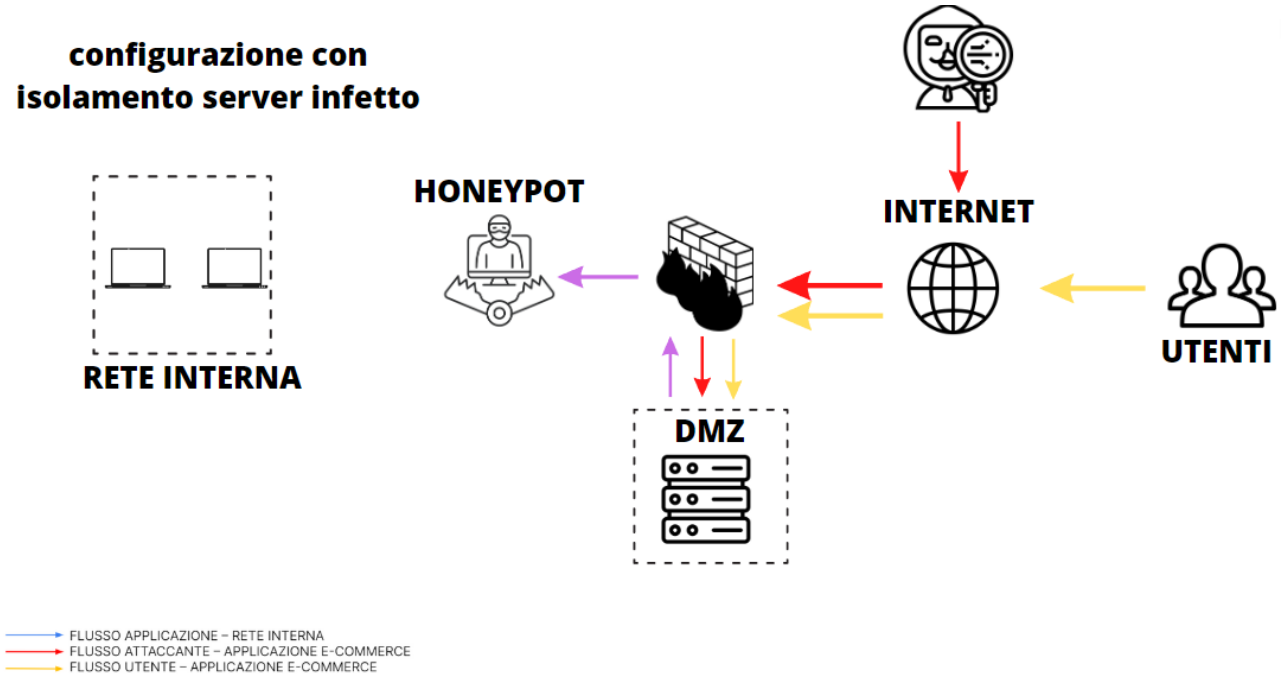
Impatti sul business:

Con i dati a nostra disposizione possiamo stimare che l'impatto sul business, in caso di sito down a causa di un DDoS, può essere circa di 15.000€.

Se calcoliamo che il sito guadagna dagli utenti circa 1.500€ al minuto e lo moltiplichiamo per i minuti in cui il server è down (10) possiamo arrivare alla cifra stimata. (1.500€ x 10 = 15.000€).

Azioni di response a seguito di Web App infetta:

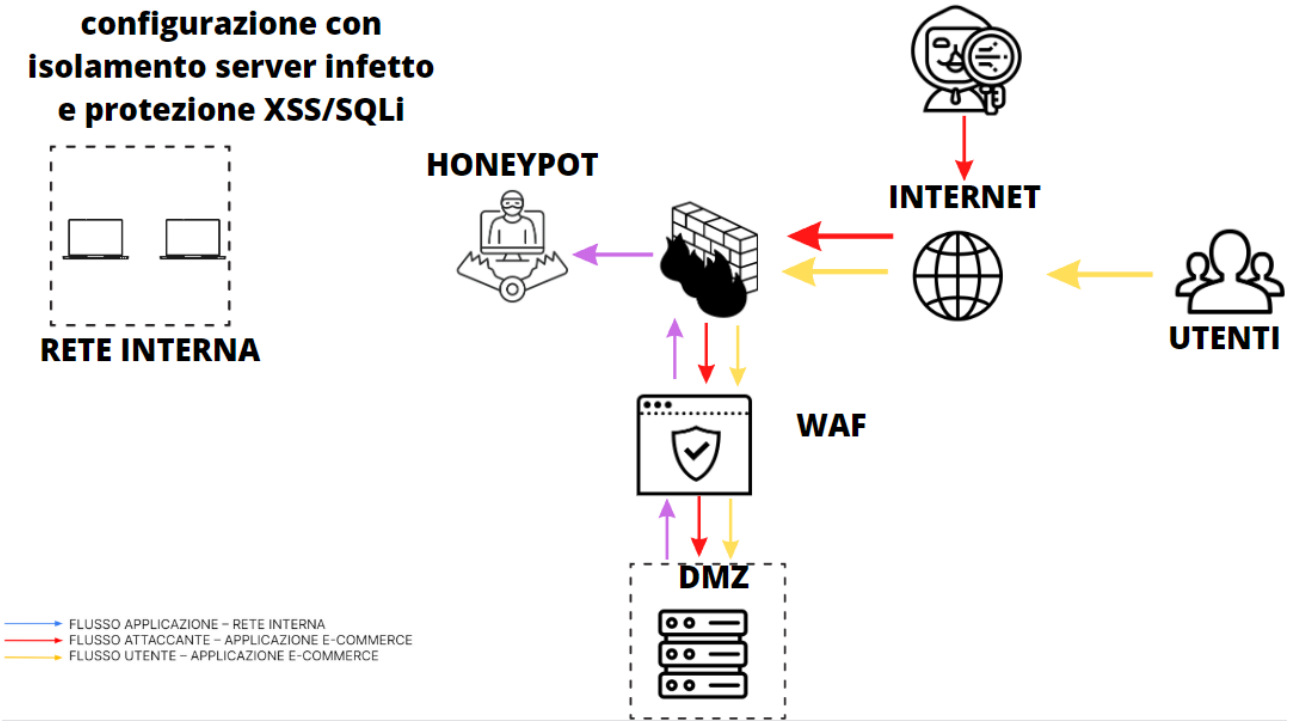
Come possiamo notare nella figura di architettura iniziale, il server della Web App comunica direttamente (passando per il firewall) con la rete interna. A seguito di un malware che infetta il nostro server si incorre nel rischio di infettare tutta la rete interna, dunque come azione di risposta è necessario staccare il collegamento tra Web App e rete interna, adottando una politica di Isolamento. Per monitorare l'attaccante e per garantire l'utilizzo dell'e-commerce agli utenti, abbiamo lasciato il Server collegato ma è stato inserito, come nodo di uscita un collegamento verso un honeypot, che ci permetterà di ricevere quante più informazioni possibili sull'attaccante qual ora dovesse riuscire ad entrarci.



Azione preventiva e di response:

Le azioni delle singole tecniche sono state spiegate precedentemente ma l'unione di queste ultime va a ricoprire un ultimo ma importantissimo parametro, ovvero ricopriamo la sicurezza utente. Difatti staccando la rete interna ed applicando un WAF al webserver non solo mettiamo in sicurezza la nostra rete interna ma evitiamo

che gli utenti incappino in un XSS persistente, e che si vedano i loro dati sensibili (credenziali, informazioni sensibili, informazioni bancarie) rubati.



Architettura rivisitata:

La mia architettura di rete rivisitata ha un impronta un po' più aggressiva per salvaguardare l'integrità degli utenti, del server e della rete interna.

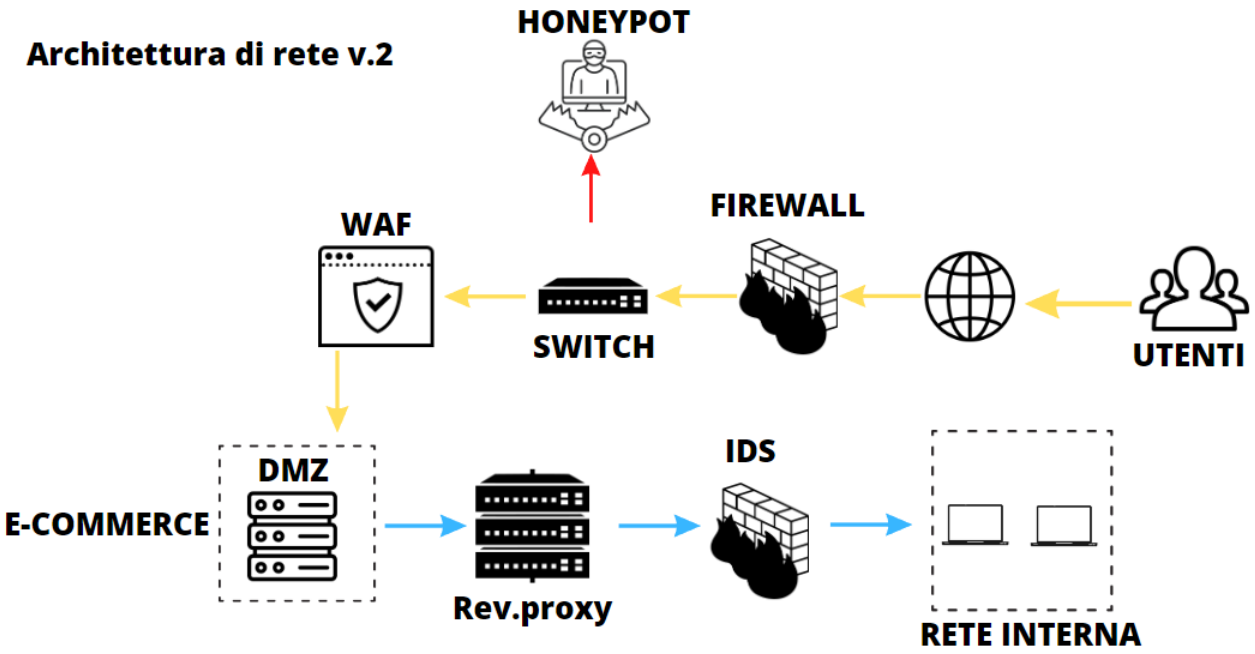
Come primo elemento vediamo un firewall che servirà per filtrare i pacchetti ed avere un primo giro di controllo, successivamente si passerà allo switch che sarà collegato sia al waf che ad un honeypot, questo è stato fatto per far incappare l'attaccante in una "trappola" e farci rendere conto di un attacco ancor prima che questo accada.

Il waf sarà collegato al web server come detto prima per evitare attacchi di XSS ed SQLi.

N.B: Il rev.proxy in immagine non è da intendersi come un proxy server ma come modulo di un secondo firewall.

Successivamente il waf per comunicare con la rete interna dovrà passare un secondo firewall, dove vi è applicato il modulo di reverse proxy. Questo modulo può operare come un **port forwarding,** inoltrando sulla rete interna le richieste che provengono dall'esterno operando però con il Controllo sulla sintassi del protocollo per filtrare attacchi o richieste.

Ed infine come ultima protezione della nostra rete interna abbiamo un IDS.


Architettura di rete v.2
HONEYPOT
WAF
FIREWALL
SWITCH
UTENTI
DMZ
E-COMMERCE
Rev.proxy
IDS
RETE INTERNA