Progetto S9-L5

Studente: Simone Mininni

Traccia:

Traccia:

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

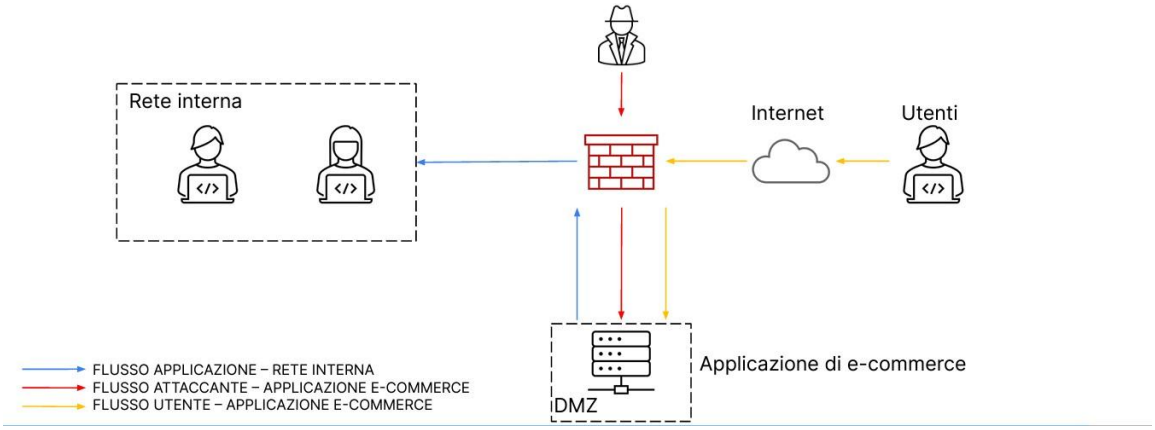
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

1. **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.

1. **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.

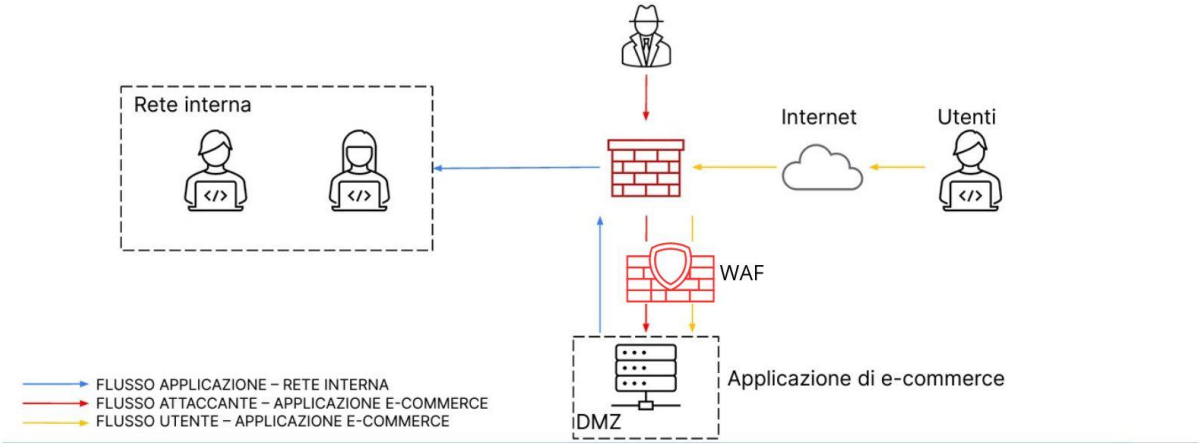
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Quesito 1:

Per proteggere i servizi web si può implementare un Waf(Web Application Firewall). Infatti quest' ultimo andrà ad analizzare il contenuto dei pacchetti in arrivo e se denota qualcosa riconducibile ad un malware, blocca il pacchetto. Al fine di comprendere se si tratta di un malware o meno, esegue un confronto con una tabella che contiene le firme o i nomi dei malware noti.
Oltre a implementare sistemi di sicurezza come i firewall, bisogna mantenere le applicazioni web aggiornate a livello di codice, in modo da mitigare vulnerabilità ad attacchi di tipo "SQLi" e "XSS".

Rappresentazione grafica:



Quesito 2:

Impatto sul business: Tempo del disservizio * fatturato medio nell' unità di tempo(minuti)
10(tempo del disservizio in minuti) * **1500**(spesa degli utenti medi al minuto) **= 15000E**.

Quesito 3:

Nelle operazioni di incident response bisogna seguire un protocollo definito durante la fase di preparazione dove le procedure vengono inserite nei “playbooks”.
Quindi nel nostro caso andremo ad isolare il server web compromesso, quindi scollegarlo dalla rete interna.
Si nota che il servizio rimane ancora accessibile su internet dagli utenti e dall’ attaccante, per policy definite precedentemente a fini economici.

Rappresentazione grafica: