Progetto S9/L5

Traccia:
Con riferimento alla figura 1, 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 1 con la soluzione proposta.

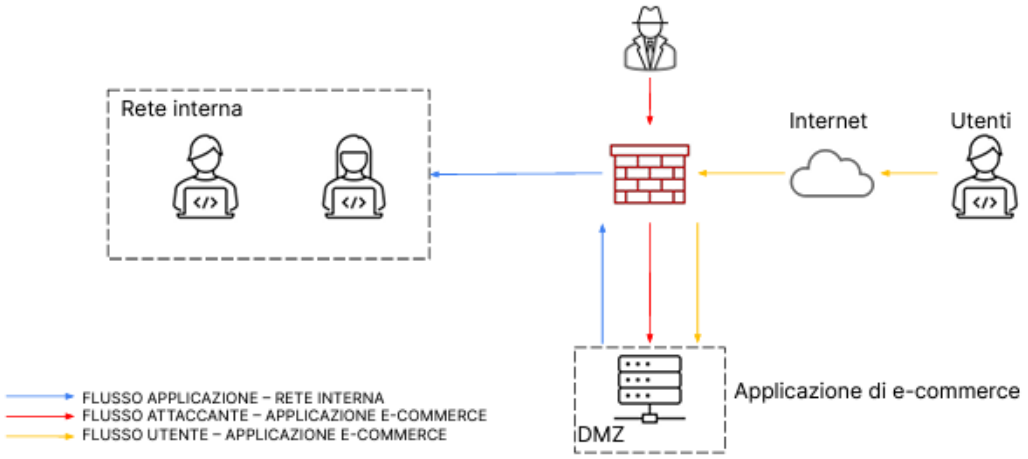

Figura 1

1) Soluzione es 1

1. Azioni preventive: quali azioni preventive implementeremo 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

Per garantire una protezione completa della Web App contro minacce come XSS e SQLi, si adotta una soluzione integrata che include un Web Application Firewall (WAF) affiancato da sistemi di rilevamento e prevenzione delle intrusioni (IPS/IDS). Nella figura iniziale, la figura 2 riflette una configurazione avanzata in cui il WAF, posizionato per proteggere il traffico in entrata dalla rete Internet, è supportato da IPS e IDS. Gli IPS sono collocati tra il WAF e la Web App stessa, monitorando e prevenendo attacchi nel traffico diretto alla Web App. Contestualmente, gli IDS sono disposti strategicamente all'interno della rete, nelle vicinanze dei server del database e ai punti di ingresso/uscita della rete, contribuendo a rilevare e mitigare attacchi in diverse fasi dell'infrastruttura. Questa combinazione di WAF, IPS e IDS crea un sistema di difesa multistrato, fornendo una protezione completa contro le varie minacce che potrebbero compromettere la sicurezza della Web App.

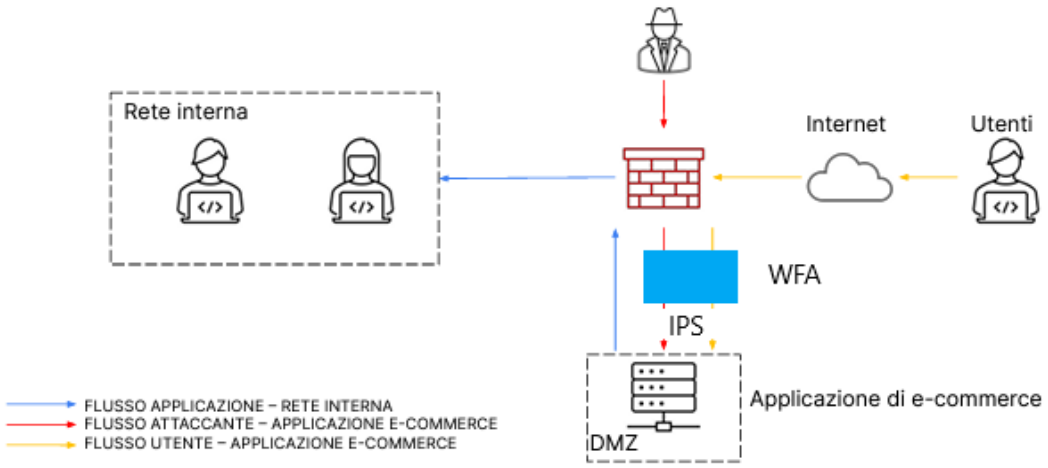

Figura 2

2) Soluzione es 2

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.

L'attacco di tipo DDoS ha provocato un'interruzione della piattaforma di e-commerce per un periodo di 10 minuti. Considerando che gli utenti spendono approssimativamente 1.500€ al minuto, è possibile stimare i danni causati dal mancato guadagno moltiplicando la spesa potenziale degli utenti per il periodo di indisponibilità del servizio. Pertanto, l'impatto sul business può essere calcolato come segue:

$$\text{Impatto sul business} = 1.500€ \times 10 \text{ minuti} = 15.000€$$

In altre parole, la compagnia ha subito una perdita di 15.000€ in acquisti potenziali a causa dei 10 minuti di indisponibilità della piattaforma.

3) Soluzione es 3

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 con le evidenze delle implementazioni.

Data l'alta priorità assegnata alla questione, si può implementare una strategia focalizzata sull'isolamento della macchina infettata. In tale scenario, la macchina in questione sarà direttamente connessa a Internet e al firewall , rendendola accessibile all'attaccante ma disconnessa dalla rete interna. La figura nella successiva slide illustra la soluzione basata sulla strategia di isolamento della macchina infetta. Si evidenzia chiaramente l'assenza di comunicazione tra l'applicazione Web e la rete interna, rafforzando così la sicurezza e limitando l'espansione di possibili minacce attraverso la disconnessione della macchina compromessa dalla rete principale.