M5W20D4

Security Operation

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

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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

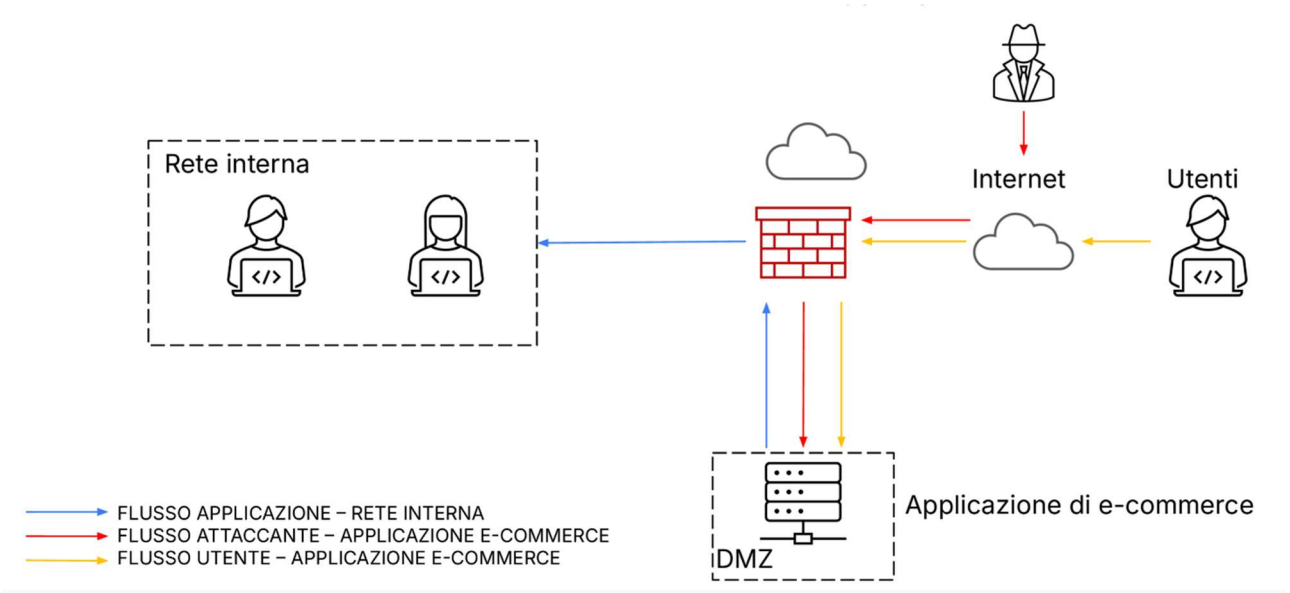
3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

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.



1. Riguardo alle *azioni preventive* si potrebbe adottare l'uso di un WAF (Web Application Firewall) che sono spesso centrati per contenere le minacce come SQL Injection o Cross Site Scripting (XSS) che si interponga tra il firewall e l'applicazione di e-commerce oltre all'inserimento di un SIEM (Security Information and Event Management) che possa ricevere tutte le informazioni da tutte le fonti. Il SIEM difatti è per la raccolta di log e monitoraggio delle minacce in tempo reale generando dei report di conseguenza mentre il WAF blocca gli attacchi impedendo la loro esecuzione.
2. Gli *impatti sul business* sono che, tenendo conto che al minuto vengono persi 1500€ al minuto, in un totale di 10 minuti vengono "persi" 15'000€, si intendono persi i soldi che l'Azienda avrebbero potuto guadagnare dagli acquisti dei commercianti sulla piattaforma.
3. *Response*: è chiaro che se viene attaccata l'applicazione di e-commerce bisogna isolare la macchina scollegando il Flusso Applicazione – Rete interna dal Firewall a Rete Interna così come dal Firewall alla DMZ.
4. Soluzione completa: