Progetto S9/L5 - Analisi dei log

Durante l'esercizio di oggi andremmo a vedere una rete con un Web Server di e-commerce che viene attaccato da un black hat e in riferimento all'immagine di essa risponderemo a questi 3 quesiti:

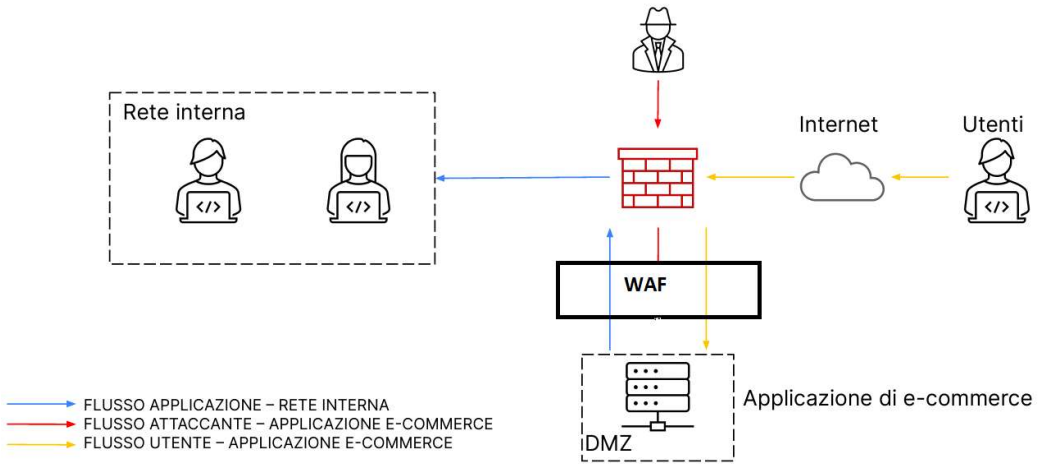
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

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.

1. Azioni preventive

Un azione preventiva che si può attuare per evitare attacchi di tipo SQLi o XSS da parte di un malintenzionato può essere quella di aggiungere il WAF prima del Web Server così da filtrare gli ingressi ed evitare che i malintenzionati iniettino codici malevoli all'interno. Il WAF è un tipo di firewall progettato specificamente per proteggere le applicazioni web da minacce e attacchi informatici. Funziona a livello delle applicazioni, analizzando e filtrando il traffico HTTP tra un'applicazione web e il client, rilevando e mitigando varie forme di attacchi.



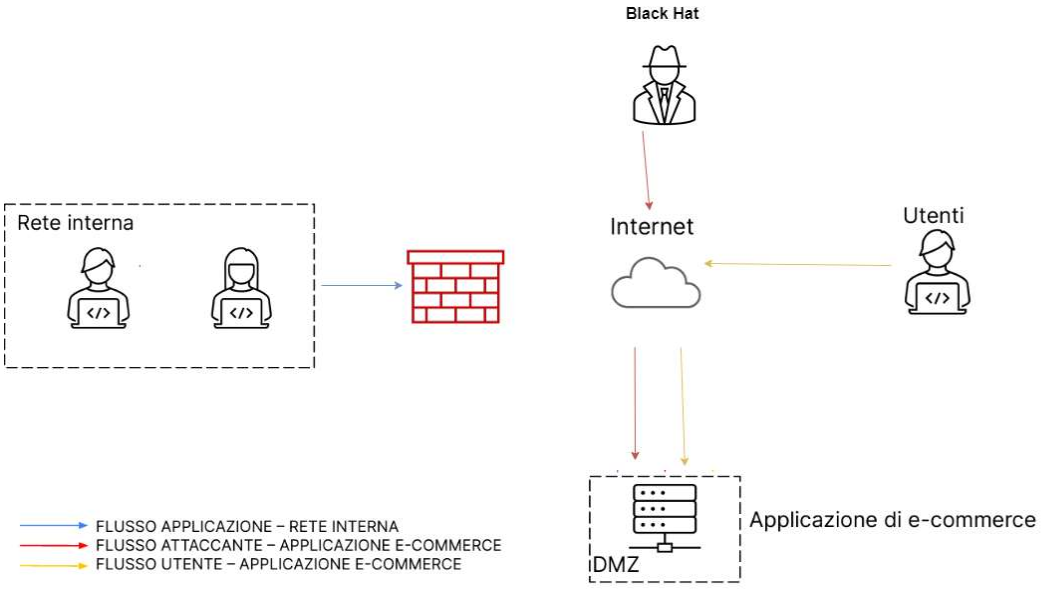
2. Impatti sul business

Il secondo punto chiede di calcolare l'impatto sul business che avrebbe l'azienda in caso che il serve dell'e-commerce andasse in down per 10 minuti sapendo che ogni minuti gli utenti spendono 1.500€. Quindi basta fare un semplice calcolo della spesa al minuto per i minuti del server down, quindi la cifra ammonta a 15.000€.

3. Response

Nel terzo punto ci viene chiesto di evitare la propagazione del malware sulla nostra rete interna, evitando la rimozione dell'accesso del malintenzionato sul web server.

Per fare ciò basta rimuovere la rete interna, compresa del firewall, dalla connessione ad internet così da isolarsi come in figura.



Così facendo andiamo a proteggere la rete interna dal malware però priviamo la connessione alla rete interna ad internet e soprattutto in caso il black hat abbia iniettato un malware attraverso un XSS stored o SQL injection probabilmente gli utenti, ignari della presenza del malware, visitando l'applicazione potrebbero infettarsi.

XSS stored è una categoria di attacchi XSS in cui il payload malevolo viene iniettato e memorizzato su un server web, prontamente restituito agli utenti quando visualizzano una pagina web particolare.

Mentre l'SQL Injection è una vulnerabilità di sicurezza che si verifica quando un'applicazione web consente a un attaccante di inserire o manipolare direttamente comandi SQL, quindi gli utenti che visiteranno il sito infettato potrebbero venire infettati di conseguenza recando molti danni.

Questo a noi come azienda direttamente non reca danni ma indirettamente

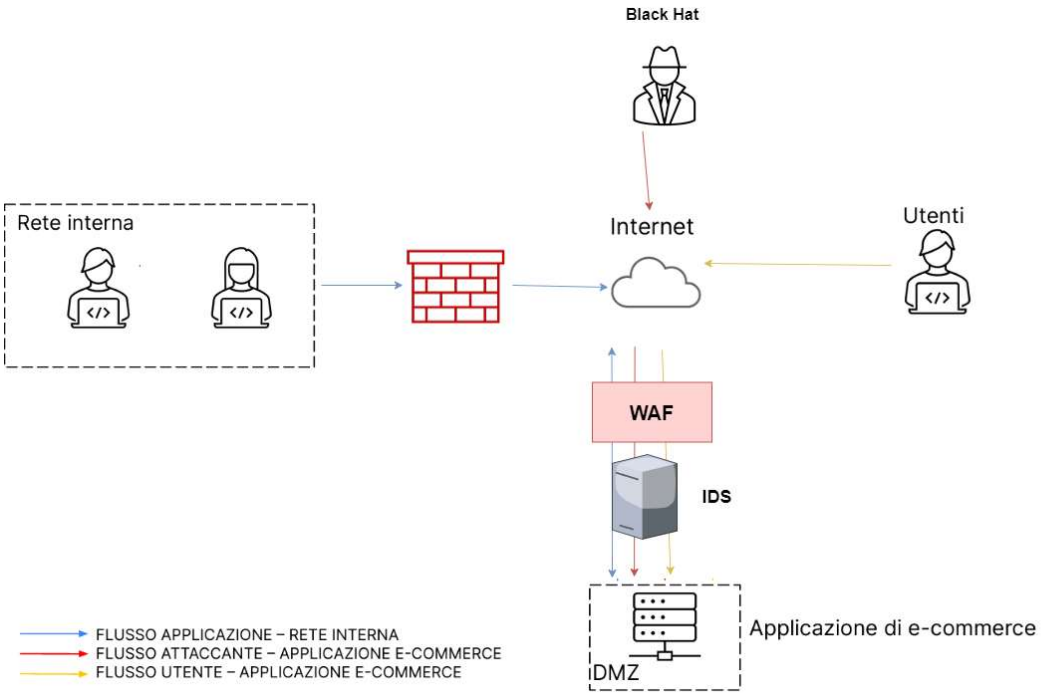
potrebbe recare danni di immagine e di sicurezza.

Portando agli utenti problemi si creerà una brutta pubblicità della nostra piattaforma di e-commerce e di conseguenza l'azienda perderà molti clienti.

Possibile soluzione al problema

Una possibile soluzione a questo problema sarebbe il primis mettere un WAF e un IDS prima della DMZ così da filtrare, come detto prima, gli accessi, sanificare il codice sorgente della web application così da rendere quasi impossibile al black hat l'iniezione di codice malevolo.

Infine in caso il Black Hat riuscisse comunque ad iniettare codice malevolo converrebbe isolare il web server e cercare di "ripulirlo" dal malware, magari attraverso una backup, evitando che gli utenti vengano infettati così da non avere danni d'immagine dell'azienda e quindi creare un piccolo disservizio temporaneo ma non permanente come potrebbe essere quello di perdere la clientela.



Grazie della visione, Caregnato Giacomo