**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.**

**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?**

Per difendere un’applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS) si possono adottare diverse metodologie.

Una delle più consigliate è sicuramente il Web Application Firewall (WAF). Può essere particolarmente efficace nella prevenzione di attacchi tramite:

* **Filtraggio delle richieste e delle risposte:** è in grado di filtrare il traffico http in ingresso e uscita, consentendo il passaggio solo alle richieste e risposte che rispettano le regole settate.
* **Protezione delle vulnerabilità conosciute:** I WAF contengono spesso delle regole specifiche per la rilevazione dei modelli noti associati a degli attacchi noti.
* **Analisi del comportamento:** I WAF avanzati sono in grado di analizzare il comportamento per identificare attacchi, tramite la corrispondenza a modelli noti.

E’ importante notare come il WAF **NON** deve essere la sola misura di sicurezza adottata.

Infatti, altre metodologie da utilizzare in concomitanza sono:

* **Escaping delle stringhe:** Per prevenire attacchi di tipo XSS, bisogna utilizzare funzioni appropriate di escape -come htmlspecialchars in PHP-, prima di visualizzare dati dinamici sulle pagine Web. In questo modo si renderanno inoffensivi gli input.
* **Validazione dei dati in input:** Implementando una validazione dei dati in input, come moduli, parametri URL e cookie. Rifiuterà i dati che non soddisfano i requisiti.
* **Penetration test:** Eseguire test regolari in maniera tale da identificare ed eventualmente correggere le vulnerabilità.
* **Content Security Policy (CSP):** Implementando una CSP possiamo limitare quali risorse esterne possono caricare e quali script possono essere eseguiti.
* **Isolamento DMZ:** Assicurarsi che la DMZ sia completamente isolata dalla rete interna, permettendo solo ai servizi necessari di essere esposti. Quindi, limitando l’accesso solo ai server e ai servizi autorizzati.

**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 docuto alla non raggiungibilità del servizio, considerando con in media ongi minuto gli utenti spendono 1.500$ sulla piattaforma di e-commerce.**

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

Il calcolo da applicare in caso di DDoS al nostro e-commerce, tenendo in considerazione il tutto è:

* **Calcolo dell’importo che gli utenti spendono in 1 minuto:** Importo medio speso dagli utenti in 1 minuto = $1.500
* **Calcolo dell’importo totale perso in 10 minuti:** Importo totale perso in 10 minuti = Importo medio al minuto X 10

Importo totale perso in 10 minuti = $1.500 x 10 = $15.000

Calcolo Analisi del Valore (AV) e Esposizione al Rischio (EF):

* **Impatto finanziario (IF):** $1.500 (importo perso in 10 minuti)
* **Probabilità di accadimento (PA):** Questo è un valore che rappresenta la probabilità che un attacco DDoS si verifichi in un periodo. Questo dato si assegna in base a vari fattori, come:
  + Tipologia applicazione
  + Profilo di minacce
  + Misure preventive adottate

Ciò comporta una stima in base al contesto specifico. In questo caso farò un esempio di probabilità al 5% (0,05)

* **AV (Analisi del Valore):** AV è il prodotto di IF e PA.
  + AV = IF\*PA
  + AV = $15.000 \*0,05
  + AV = $750

Quindi, l’AV dell’attacco DDoS è di $750

**EF (Esposizione al Rischio):** rappresenta il potenziale impatto finanziario totale nell’arco di un periodo di tempo. Non si conterà più solo il singolo evento ma si metterà in conto un mese intero con una possibilità mensile (ad esempio) del 2% di subire attacchi DDoS. Il calcolo sarà così composto:

* + EF = AV \* Numero di eventi previsti
  + EF = $750 \* (30 giorni al mese \* 24 ore al gg) / (10 minuti per evento)
  + EF = $750 \*432
  + EF = $324.000

Questo è il potenziale impatto finanziario relativo agli attacchi DDoS durante un mese considerando una probabilità del 5%.

Per quanto riguarda le possibili azioni preventive, abbiamo:

* **Distribuzione Geografica:** Utilizzare una distribuzione geografica dei server e dei servizi, in maniera tale da distribuire il traffico e garantire che un possibile attacco non colpisca tutti i server in contemporanea.
* **Backup e ripristino:** Mantenere le procedure di backup regolari, soprattutto dei dati critici, così che -qualora un attacco facesse ingenti danni- da avere sempre un rapido rispristino a portata di mano.
* **Test di resilienza:** Eseguire molti test di resilienza e simulazioni di attacchi DDoS per valutare come il sistema reagisce, apportando le dovute modifiche.
* **Scalabilità automatica:** Configurare l’ambiente in maniera tale da avere risorse aggiuntive in caso di attacco DDoS. Facendo ciò, la capacità del server può essere aumentata per gestire il carico extra durante l’attacco.

**Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.**

L'obiettivo principale in questa situazione è impedire la propagazione del malware e limitare i danni alla vostra rete e ai vostri dati, mantenendo l'accesso dell'attaccante alla macchina infettata per scopi di monitoraggio e analisi. La sicurezza della rete e dei dati rimane una priorità, e quindi è importante mettere in atto misure di isolamento e protezione.

**Per far ciò è possibile eseguire le seguenti operazioni:**

* **Isolamento della macchina infetta:** Isolare immediatamente la macchina infettata dalla rete. Ciò può essere fatto fisicamente o tramite l'uso del firewall per impedire la comunicazione tra la macchina infetta e il resto della rete.
* **Quarantena del traffico:** Utilizzare una soluzione di sicurezza che possa filtrare e analizzare il traffico in uscita dalla macchina infettata, in modo da impedire la propagazione del malware su altri sistemi nella rete. È importante monitorare e bloccare qualsiasi tentativo del malware di comunicare con altri dispositivi.
* **Analisi approfondita:** Effettuare un'analisi dettagliata della macchina infetta per identificare la natura e il comportamento del malware. Questo potrebbe includere l'analisi del traffico di rete, dei file e dei processi in esecuzione sulla macchina.