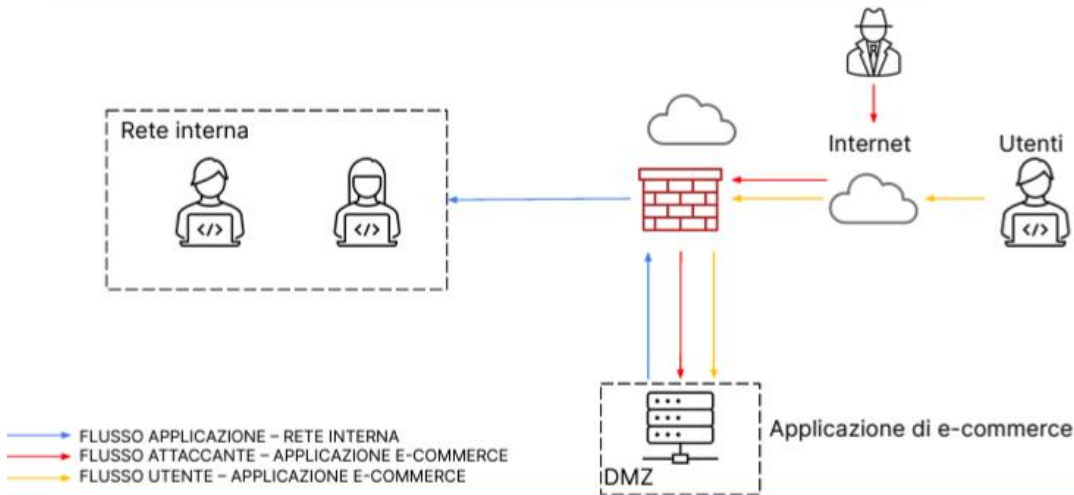


SPLUNK: ESERCIZIO FINALE

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. **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

Basandomi sulla descrizione dell'esercizio, per proteggere un'applicazione di e-commerce all'interno di una rete con una:

Azioni preventive contro SQL Injection (SQLi):

1. **Validazione dell'input:** È fondamentale assicurarsi che tutti gli input degli utenti siano validati seguendo criteri rigorosi, utilizzando liste di permessi per limitare i tipi di input accettabili.
2. **Parametrizzazione delle Query:** È essenziale usare query parametrizzate o prepared statements per l'accesso al database, che impediscono l'esecuzione di input dannosi come parte di una query SQL.
3. **Minimizzazione dei privilegi:** È importante che le connessioni al database dall'applicazione web utilizzino un account con i minimi privilegi necessari per eseguire le operazioni richieste.
4. **Uso di ORM (Object-Relational Mapping):** Utilizzare un ORM può ridurre il rischio di SQLi poiché genera automaticamente query SQL da codice di alto livello.

5. **Risposta ambigua agli errori:** Configurare le risposte dell'applicazione agli errori in modo che non rivelino dettagli sul database o sulla struttura del codice.

Azioni preventive contro Cross-Site Scripting (XSS):

1. **Escape dell'output:** Prima di mostrare dati forniti dagli utenti nel browser, è necessario applicare funzioni di escaping per neutralizzare o rimuovere elementi potenzialmente pericolosi come tag o script.
2. **Utilizzo di Content Security Policy (CSP):** Implementare CSP per ridurre le possibilità che contenuti dannosi possano essere eseguiti o caricati sulla pagina.
3. **Validazione dell'input:** Similmente alla prevenzione di SQLi, è necessario utilizzare una validazione rigorosa dell'input per rifiutare dati che contengono script non autorizzati o tag HTML.
4. **Cookie sicuri:** Configurare i cookie con l'attributo 'HttpOnly' per impedire l'accesso ai cookie tramite script lato client.

Implementazione nella Figura

Per integrare queste misure su questa architettura di rete, si possono considerare i seguenti soluzioni:

- **Firewall Application Layer:** Aggiungere un firewall di applicazione (WAF) nella DMZ per filtrare il traffico sia in entrata che in uscita, specificamente per rilevare e bloccare tentativi di SQLi e XSS.
- **Log e monitoraggio:** Integrare un sistema di log e monitoraggio delle attività sospette, che potrebbe essere visualizzato nella DMZ come parte del controllo di sicurezza.
- **Separazione dei servizi:** Mostrare la separazione tra i server che gestiscono la logica applicativa e quelli che gestiscono l'accesso al database.

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**

Il calcolo dell'impatto economico di un attacco DDoS dell'applicazione di e-commerce:

Calcolo dell'Impatto Economico:

L'applicazione web ha subito un attacco DDoS che ha reso il servizio inaccessibile per 10 minuti. Considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma, l'impatto economico diretto dell'attacco può essere calcolato come segue:

- Perdita diretta: 1.500 € per minuto x 10 minuti = 15.000 €

Questa cifra rappresenta solo le perdite dirette e non include altri possibili impatti negativi come la perdita di fiducia dei clienti, il danno all'immagine aziendale e la possibile perdita di clienti futuri.

Misure Preventive Contro Attacchi DDoS:

1. **Aumento della capacità di banda:** Mi assicurerò che la tua infrastruttura di rete abbia sufficiente capacità di banda per gestire aumenti significativi del traffico, che possono essere un indicatore di un attacco DDoS.
2. **Mitigazione basata su cloud:** Utilizzerò servizi di mitigazione DDoS basati su cloud che possono assorbire il traffico anomalo prima che raggiunga la tua infrastruttura.
3. **Rate limiting:** Imposterò limiti al numero di richieste che un utente può fare in un determinato periodo di tempo per prevenire sovraccarichi al server.
4. **Geo-blocking:** Bloccherò o limiterò il traffico proveniente da regioni geografiche che non sono rilevanti per il tuo business.

5. **Redundancy e failover:** Implementerò soluzioni di ridondanza e failover per garantire che l'applicazione possa rimanere operativa anche in caso di attacco, distribuendo il carico su più server o data center.

6. **Monitoraggio e allerta precoce:** Utilizzerò sistemi di monitoraggio del traffico in tempo reale per rilevare e rispondere rapidamente agli attacchi DDoS.

Implementazione nella Figura

Per integrare queste misure nella configurazione di rete esistente, si può aggiungere un servizio di mitigazione DDoS cloud-based rappresentato nel DMZ e punti di controllo per il rate limiting e il geo-blocking illustrati come filtri nel traffico in ingresso.

Queste misure possono aiutare a ridurre la vulnerabilità agli attacchi DDoS e a minimizzare l'impatto economico di eventuali interruzioni future del servizio.

3. **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.
Modificate la figura in slide 2 con la soluzione proposta.

Quando l'applicazione di e-commerce è stata infettata da un malware, la priorità è assicurarsi che il malware non si propaghi sulla tua rete interna, invece di rimuovere immediatamente dell'accesso dell'attaccante alla macchina infettata. Di seguito, una soluzione che potrebbe essere implementata per contenere il problema:

Soluzione Proposta:

1. **Isolamento della Macchina Infetta:** Primo passo sarà isolare il server infetto nella DMZ per prevenire ulteriori danni o la diffusione del malware. Posso fare ciò modificando le regole del firewall per bloccare tutto il traffico in uscita dal

server verso la rete interna, mentre permetto il traffico essenziale per operazioni di manutenzione e analisi.

2. Analisi del Malware: Successivamente, analizzerò il malware per comprendere il suo comportamento e l'eventuale presenza di altri punti di infezione. Questo include esaminare i log del server e utilizzare strumenti di sicurezza per identificare e analizzare il codice maligno.

3. Rafforzamento delle Difese: Mentre la macchina infetta rimane isolata, si rafforzano le difese delle altre parti del sistema. Questo comprende l'aggiornamento di software e firewall, la verifica delle configurazioni di sicurezza e l'implementazione di nuove politiche di sicurezza per prevenire futuri incidenti.

4. Comunicazione e Formazione: Informare il personale coinvolto sull'incidente e fornire formazione aggiuntiva se necessario per evitare errori che potrebbero portare a future infezioni.

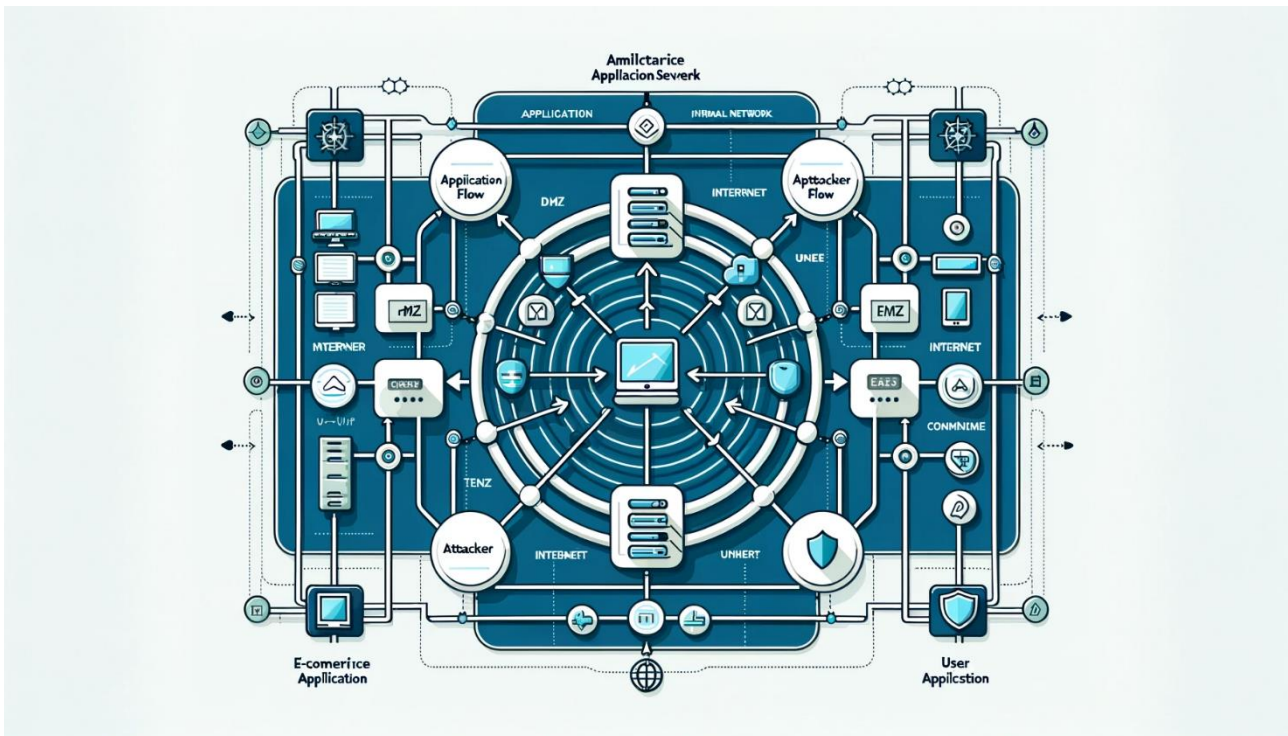
5. Monitoraggio Continuo: Infine, implementerò un sistema di monitoraggio più rigoroso, con alert automatici per attività sospette che potrebbero indicare tentativi di infezione o altri attacchi.

Implementazione nella Figura

Per visualizzare queste misure, posso modificare il diagramma di rete esistente includendo:

- Un'icona di isolamento per il server infetto nella DMZ.
- Linee di comunicazione che mostrano solo connessioni limitate e controllate con il server infetto.
- Simboli che rappresentano il monitoraggio intensificato e le nuove politiche di sicurezza.

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



Ho aggiornato il diagramma della rete per l'applicazione di e-commerce includendo le misure di sicurezza specificate. Nel diagramma aggiornato puoi vedere:

1. Un server isolato nella DMZ, con accesso limitato e chiaramente segnato per il contenimento a causa di un'infezione da malware.
2. L'implementazione di misure di sicurezza come un firewall di applicazione web (WAF) che filtra il traffico in entrata e in uscita specificamente per la prevenzione di SQLi e XSS.
3. Rappresentazioni visive di sistemi di monitoraggio avanzati all'interno della DMZ, che indicano analisi del traffico in tempo reale e rilevamento di anomalie.
4. Simboli per percorsi di dati sicuri e connessioni crittografate tra i server e la rete esterna per garantire l'integrità e la privacy dei dati.

Queste modifiche sono state fatte per assicurare che le misure preventive contro le minacce di sicurezza siano chiaramente rappresentate e per mantenere la separazione tra i server che gestiscono la logica applicativa e quelli che gestiscono l'accesso al database, prevenendo così la diffusione di infezioni.

Queste modifiche mirano a prevenire la diffusione di infezioni e garantire un'alta resilienza agli attacchi, mantenendo una sofisticata separazione dei compiti tra i server.

Puoi visualizzare l'immagine aggiornata nel messaggio precedente. Fammi sapere se ci sono ulteriori dettagli o modifiche che desideri apportare!