Progetto M5:

Traccia:

Traccia:

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**

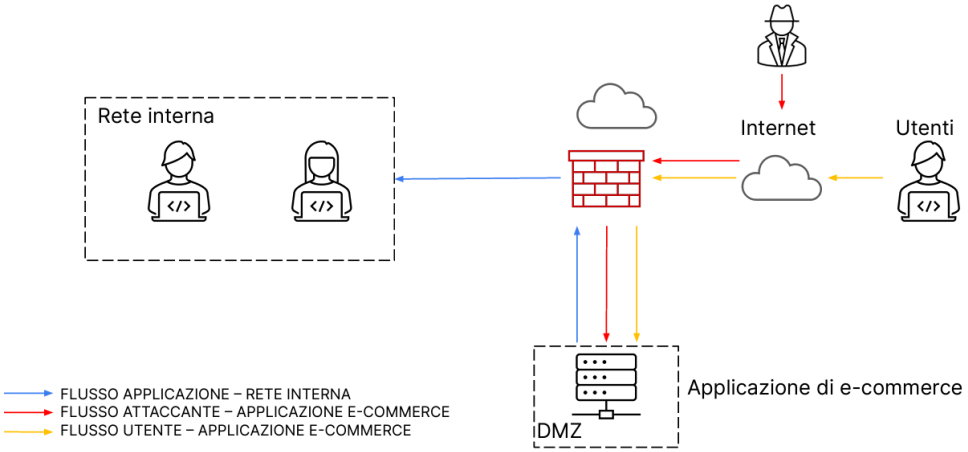
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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.



Soluzione:

1. Azioni preventive contro SQLi e XSS:

Per difendere un'applicazione Web da attacchi di tipo SQLi e XSS, si possono implementare diverse azioni preventive:

Per SQL Injection (SQLi):

1. Utilizzo di prepared statements o query parametrizzate.
2. Validazione e sanitizzazione dei dati di input.
3. Limitazione dei privilegi del database per l'account utilizzato dall'applicazione.
4. Implementazione di firewall per filtrare e monitorare il traffico SQL.

Per Cross-Site Scripting (XSS):

1. Utilizzo di librerie/framework che offrono meccanismi di escape automatico (es. React.js, AngularJS).
2. Validazione e sanitizzazione dei dati di input e output.
3. Impostazione di header HTTP corretti per prevenire attacchi XSS (es. Content-Security-Policy).
4. Implementazione di meccanismi di validazione lato server per ridurre la possibilità di inserire codice dannoso.

2. Impatti sul business dell'attacco DDoS:

Calcolo dell'impatto sul business:

10 minuti * 1.500 €/minuto = 15.000 €

L'impatto sull'attività dovuto alla non raggiungibilità del servizio è di 15.000 €.

Azioni preventive:

1. Implementazione di servizi di mitigazione DDoS (es. CDN con funzionalità anti-DDoS).
2. Monitoraggio attivo del traffico di rete per rilevare e rispondere rapidamente agli attacchi DDoS.
3. Utilizzo di firewall e regole di filtraggio per bloccare il traffico sospetto.
4. Distribuzione geografica dei server per ridurre l'effetto di un attacco DDoS su un singolo punto di fallimento.

3. Response all'attacco di malware:

Poiché la priorità è impedire la propagazione del malware sulla rete senza rimuovere l'accesso dell'attaccante alla macchina infettata, le azioni da intraprendere possono includere:

1. Isolare immediatamente la macchina infetta dalla rete principale utilizzando VLAN o subnet separate.
2. Impostare regole di firewall per bloccare il traffico proveniente dalla macchina infetta verso altri dispositivi nella rete.
3. Eseguire una scansione completa del sistema per individuare e rimuovere il malware.
4. Monitorare attentamente il traffico di rete per rilevare eventuali tentativi dell'attaccante di propagare ulteriormente il malware.
5. Aggiornare i sistemi operativi e le applicazioni con patch di sicurezza per chiudere eventuali vulnerabilità utilizzate dall'attaccante.

Queste azioni possono aiutare a limitare l'espansione del malware sulla rete senza interrompere l'accesso dell'attaccante alla macchina infetta.

4. Soluzione completa: Unendo le azioni preventive (soluzione 1) e la response (soluzione 3), si ottiene una strategia completa per proteggere l'applicazione Web e gestire gli attacchi.

5. Soluzione "aggressiva": Per implementare una modifica più aggressiva dell'infrastruttura per affrontare le minacce di sicurezza, possiamo considerare le seguenti opzioni:

- **Suddivisione in microservizi**: Riduci la superficie di attacco suddividendo l'applicazione in microservizi. In questo modo, un'eventuale compromissione di uno dei servizi avrebbe un impatto limitato sul resto del sistema.
- **Architettura serverless**: Passa a un'architettura serverless per eliminare la necessità di gestire l'infrastruttura del server. Le piattaforme serverless gestiscono automaticamente la scalabilità e la sicurezza dell'applicazione.
- **Implementazione di un Web Application Firewall (WAF)**: Utilizza un WAF per filtrare e monitorare il traffico HTTP/HTTPS in ingresso e in uscita, identificando e bloccando potenziali attacchi.
- **Adozione di crittografia end-to-end**: Implementa la crittografia end-to-end per proteggere i dati sensibili durante il trasporto e durante l'archiviazione.

- **Rafforzamento delle politiche di autenticazione e autorizzazione**: Implementa politiche di autenticazione a più fattori (MFA) e autorizzazione granulare per garantire che solo gli utenti autorizzati possano accedere alle risorse dell'applicazione.
- **Continuous Security Testing**: Integra i test di sicurezza nel ciclo di sviluppo del software utilizzando tecniche come DevSecOps per identificare e correggere le vulnerabilità in modo tempestivo.
- **Utilizzo di soluzioni AI per la sicurezza**: Implementa soluzioni basate sull'intelligenza artificiale per rilevare e rispondere automaticamente alle minacce di sicurezza in tempo reale.
- **Monitoraggio e analisi dei log avanzati**: Utilizza strumenti di monitoraggio dei log avanzati per rilevare comportamenti sospetti e anomalie nel sistema.

Backup e ripristino sicuro dei dati: Implementa procedure regolari di backup dei dati e piani di ripristino per garantire la disponibilità e l'integrità dei dati in caso di attacco o perdita.