W20D4

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**

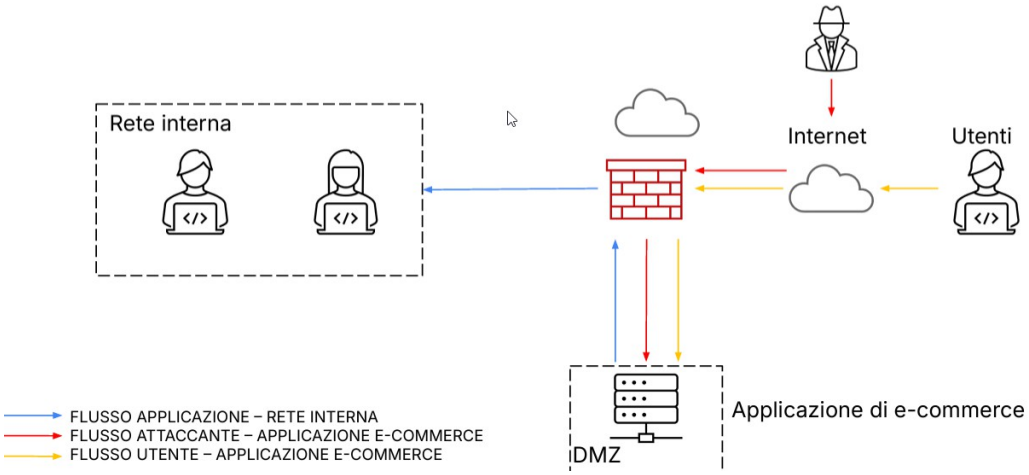
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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.



Di seguito un'analisi delle azioni preventive, degli impatti sul business, delle risposte a incidenti di sicurezza, e una proposta per una soluzione completa.

1. Azioni preventive

Per proteggere l'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), si possono implementare le seguenti azioni preventive:

- **Validazione e sanitizzazione degli input**: Assicurarsi che tutti i dati inseriti dagli utenti siano controllati e filtrati per rimuovere eventuali codici malevoli.
- **Utilizzo di query parametrizzate**: Le query parametrizzate impediscono l'esecuzione di codice SQL non autorizzato.
- **Content Security Policy (CSP)**: Implementare una CSP per ridurre il rischio di attacchi XSS, limitando le origini delle risorse caricate nel browser.
- **Firewall per applicazioni web (WAF)**: Utilizzare un WAF per monitorare e filtrare il traffico HTTP e HTTPS

per proteggere l'applicazione da attacchi comuni.

- **Autenticazione e autorizzazione forti**: Assicurarsi che solo gli utenti autenticati e autorizzati possano accedere a determinate funzionalità dell'applicazione.

2. Impatti sul business

In caso di un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, possiamo calcolare l'impatto economico:

- Spesa media al minuto: 1.500 €
- Tempo di inattività: 10 minuti

Calcolo dell'impatto:

Impatto = 1.500 € \times 10 = **15.000 €**

Azioni preventive:

- **Ridondanza**: Implementare un bilanciatore di carico per distribuire il traffico su più server.
- **Soluzioni anti-DDoS**: Utilizzare servizi specifici che mitigano gli attacchi DDoS, come Cloudflare o Akamai.
- **Sistemi di allerta**: Monitorare il traffico in tempo reale per identificare attacchi in corso e attivare risposte automatiche.

3. Response

Se l'applicazione web viene infettata da un malware e l'obiettivo è prevenire la propagazione sulla rete interna:

-**Isolamento della macchina compromessa**: Separare il server compromesso dal resto della rete attraverso VLAN o firewall interni.
-**Monitoraggio del traffico**: Implementare un sistema di monitoraggio per analizzare il traffico in uscita dalla macchina compromessa.
- **Segmentazione della rete**: Usare la segmentazione per limitare l'accesso ai dati critici e ridurre il rischio di propagazione del malware.

4. Soluzione completa

La soluzione completa unisce le azioni preventive per proteggere l'applicazione da SQLi e XSS e le strategie di risposta in caso di malware. Ecco come si potrebbero implementare :

- **DMZ**:
  -WAF per protezione DDoS
  - Server web con validazione input e CSP

- **Rete interna**:
  - Segmentazione della rete per isolare i server critici
  - Monitoraggio del traffico per rilevare attività sospette

- **Procedure di risposta**:
  - Isolamento automatico dei server compromessi
  - Implementazione di sistemi di allerta per anomalie di traffico

Considerazioni finali:

Adottando un approccio multilivello per la sicurezza,si puo migliorare significativamente la protezione dell' applicazione di e-commerce e mitigare i potenziali impatti sul business derivanti da attacchi informatici.