ESERCIZIO WEEK 20 DAY 4

Studente: Orazio Ciccozzi

Traccia:

Esercizio Traccia e requisiti 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

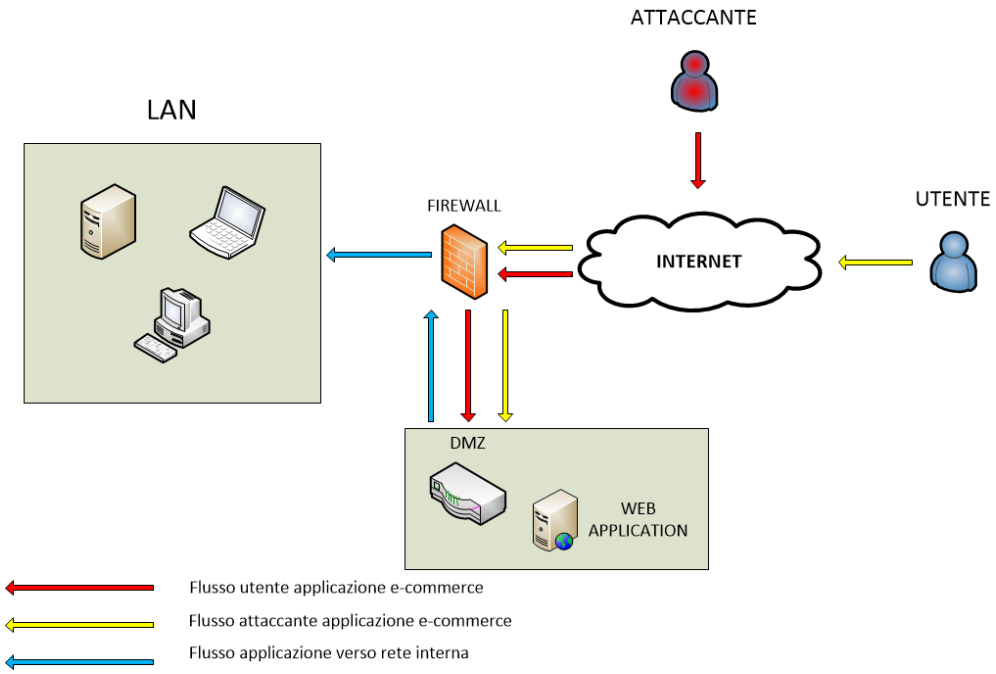
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma 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.

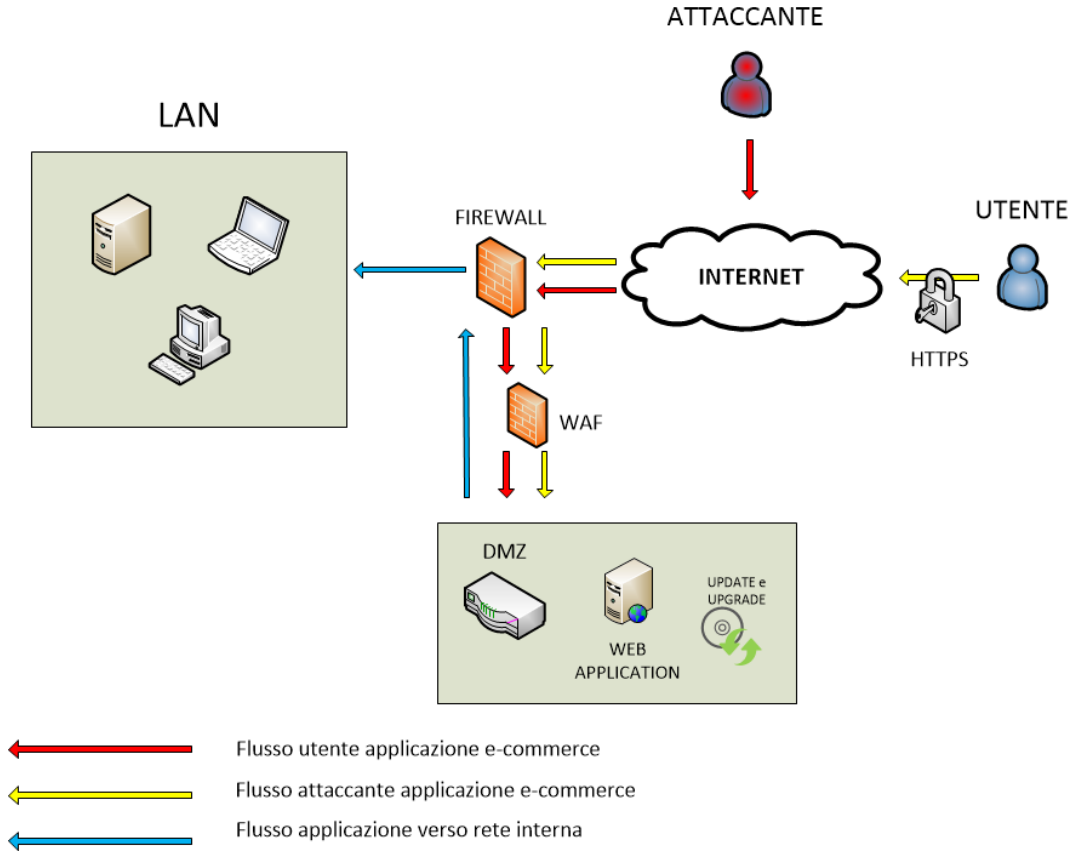


1. Azioni preventive

Descrizione: Per difendere un'applicazione web da attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS), è fondamentale implementare una serie di misure di sicurezza. Questi attacchi sfruttano le vulnerabilità dell'applicazione per eseguire codice malevolo, rubare dati sensibili o compromettere la sicurezza del sistema.

Soluzione:

1. **Web Application Firewall (WAF):**
   - **Implementazione:** Un WAF monitora e filtra il traffico HTTP diretto verso l'applicazione web, bloccando tentativi di attacchi SQLi e XSS. Configurare il WAF per rilevare e prevenire schemi di attacco noti.
2. **Validazione e Sanitizzazione degli Input:**
   - **Implementazione:** Utilizzare funzioni di validazione per controllare e limitare i dati che gli utenti possono inserire nei form dell'applicazione. Sanitizzare gli input per rimuovere caratteri potenzialmente pericolosi.
   - **Esempio:** Utilizzare prepare statements con bound parameters per SQLi e librerie di sanitizzazione come OWASP Java HTML Sanitizer per XSS.
3. **Cifratura delle Comunicazioni:**
   - **Implementazione:** Abilitare HTTPS per tutte le comunicazioni tra gli utenti e l'applicazione web. Utilizzare certificati SSL/TLS validi per cifrare i dati in transito, prevenendo intercettazioni e man-in-the-middle attacks.
4. **Aggiornamenti e Patch:**
   - **Implementazione:** Mantenere sempre aggiornato il software dell'applicazione e applicare tempestivamente le patch di sicurezza rilasciate dai fornitori. Monitorare i bollettini di sicurezza per identificare e correggere vulnerabilità note.



2. Impatti sul business

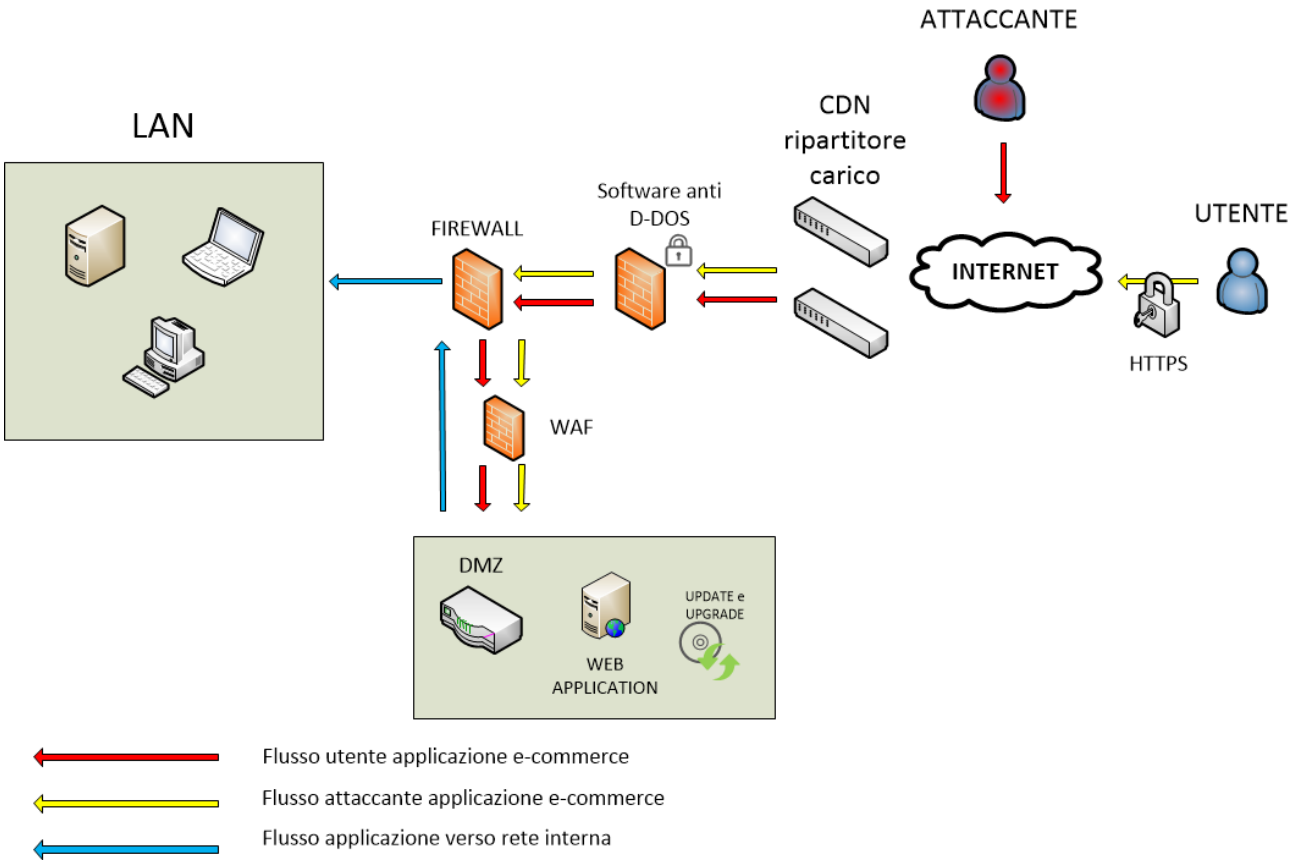
Descrizione: Un attacco Distributed Denial of Service (DDoS) può rendere un'applicazione web non raggiungibile, causando significative perdite economiche e danni alla reputazione aziendale. L'impatto economico di tali attacchi deve essere quantificato per valutare l'urgenza delle contromisure da implementare.

Calcolo dell'Impatto:

Impatto sul business = Perdite per minuto * Minuti di inattività = 1.500 € * 10 minuti = 15.000 €

Soluzione:

1. **Content Delivery Network (CDN):**
   - **Implementazione:** Utilizzare una CDN per distribuire il carico di traffico su più server distribuiti globalmente, riducendo la probabilità che un singolo attacco DDoS possa interrompere il servizio.
2. **Rate Limiting:**
   - **Implementazione:** Configurare rate limiting per limitare il numero di richieste che ogni indirizzo IP può effettuare in un determinato intervallo di tempo. Questo aiuta a mitigare gli effetti degli attacchi DDoS basati su un alto volume di richieste.
3. **Servizi Anti-DDoS:**
   - **Implementazione:** Integrare servizi specializzati di mitigazione DDoS, che possono identificare e neutralizzare il traffico malevolo prima che raggiunga l'applicazione web.



3. Response

Descrizione: Quando un malware infetta un'applicazione web, è cruciale prevenire la sua propagazione all'interno della rete aziendale, proteggendo al contempo l'accesso ai dati compromessi.

Soluzione:

1. **Isolamento della Macchina Infetta:**
    - **Implementazione:** Disconnettere la macchina infetta dalla rete interna per impedire la propagazione del malware. Tuttavia, mantenere la connessione internet per consentire all'attaccante di rimanere connesso, facilitando il monitoraggio delle sue attività.

2. **Segmentazione della Rete:**
    - **Implementazione:** Implementare segmenti di rete separati per isolare i sistemi critici e limitare l'accesso tra i segmenti, riducendo il rischio di propagazione.

3. **Access Control Lists (ACLs):**
    - **Implementazione:** Utilizzare ACLs per restringere l'accesso alla rete interna solo a dispositivi autorizzati, impedendo al malware di comunicare con altre parti della rete.

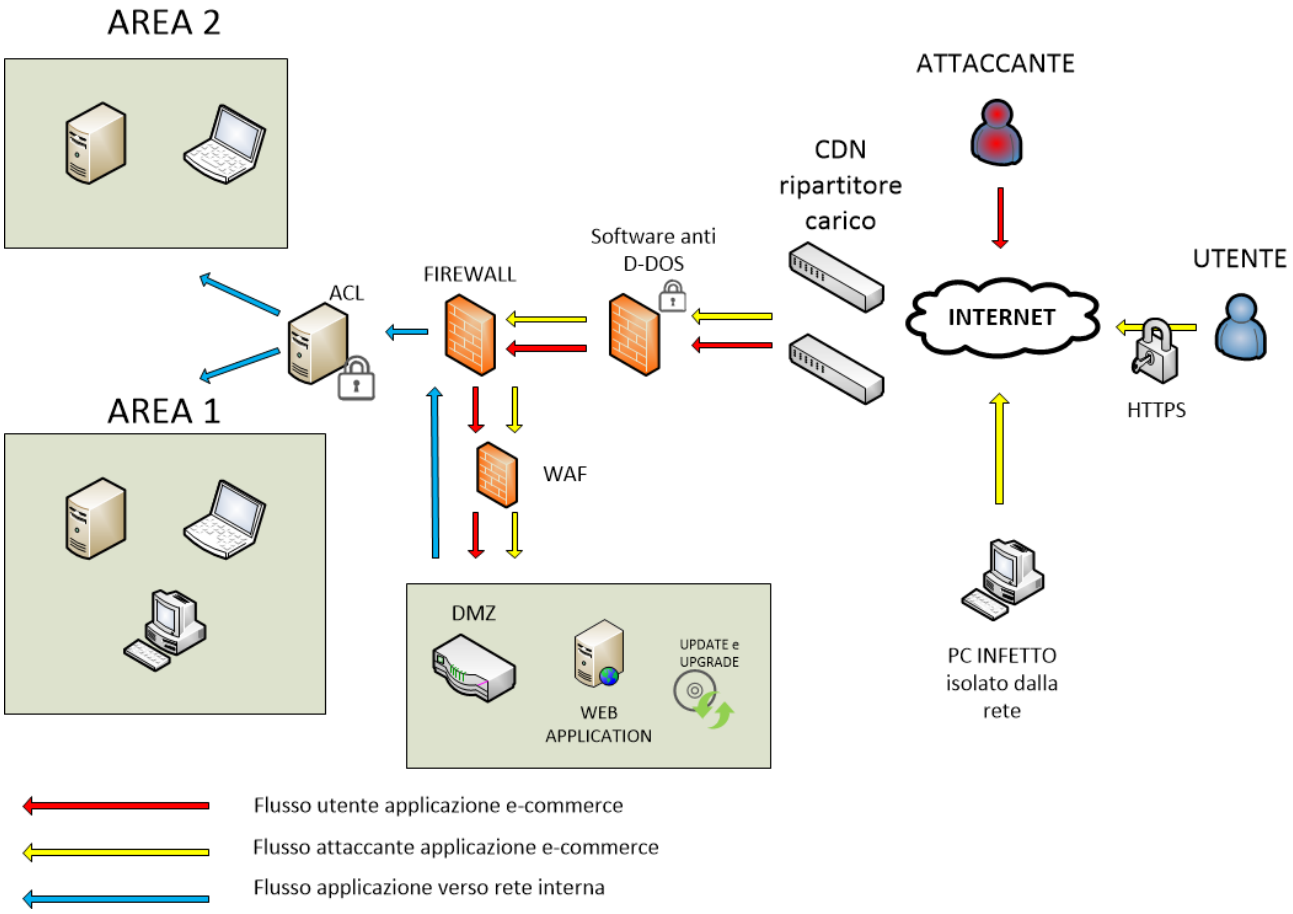
4. **Monitoraggio Continuo:**
    - **Implementazione:** Attivare il monitoraggio continuo della rete per rilevare attività sospette e reagire rapidamente a nuove infezioni o tentativi di propagazione.

4. Soluzione completa

Descrizione: Integrare tutte le soluzioni preventive e di risposta in un'unica architettura di rete completa che protegga l'applicazione web da vari tipi di attacchi e gestisca le minacce in corso.

Soluzione Integrata:

1. **Prevenzione e Protezione:**
    - Integrare il WAF, validazione degli input, HTTPS, aggiornamenti e patch.
    - Integrare CDN, rate limiting e servizi anti-DDoS per mitigare gli attacchi DDoS.
2. **Risposta e Isolamento:**
    - Implementare l'isolamento della macchina infetta e la segmentazione della rete.
    - Utilizzare ACLs e monitoraggio continuo per impedire la propagazione del malware.



5. Modifica più aggressiva

Descrizione: Considerare ulteriori modifiche all'infrastruttura per migliorare la sicurezza complessiva, integrando le soluzioni preventive e di risposta precedenti e aggiungendo ulteriori misure avanzate.

Soluzione:

1. **Zero Trust Architecture:**
   - **Implementazione:** Adottare un modello di sicurezza Zero Trust, dove ogni richiesta di accesso è verificata e autenticata continuamente, indipendentemente dall'origine della richiesta.
2. **Segregazione Avanzata:**
   - **Implementazione:** Implementare una segregazione più rigorosa tra i diversi segmenti di rete, utilizzando VLANs (Virtual Local Area Networks) e micro-segmentazione per limitare ulteriormente l'accesso.
3. **Risposta Automatica agli Incidenti:**
   - **Implementazione:** Utilizzare sistemi di risposta automatizzata agli incidenti (SOAR - Security Orchestration, Automation, and Response) per rilevare e reagire rapidamente alle minacce, riducendo il tempo di risposta e minimizzando l'impatto.
4. **Formazione e Consapevolezza:**
   - **Implementazione:** Implementare programmi di formazione continua per il personale per riconoscere e rispondere alle minacce di sicurezza.