TRACCIA

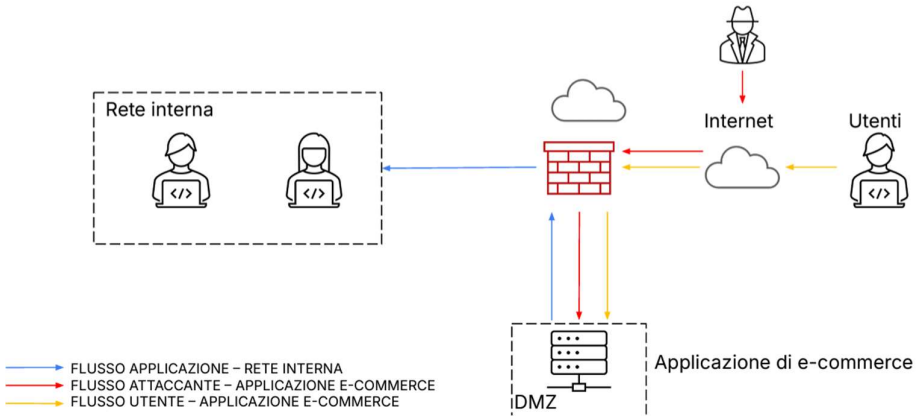
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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)

Relazione sulla Sicurezza Informatica: Prevenzione, Impatto e Risposta agli Attacchi

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.



SVOLGIMENTO

1. Azioni Preventive contro SQLi e XSS

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

1.1 Prevenzione SQL Injection

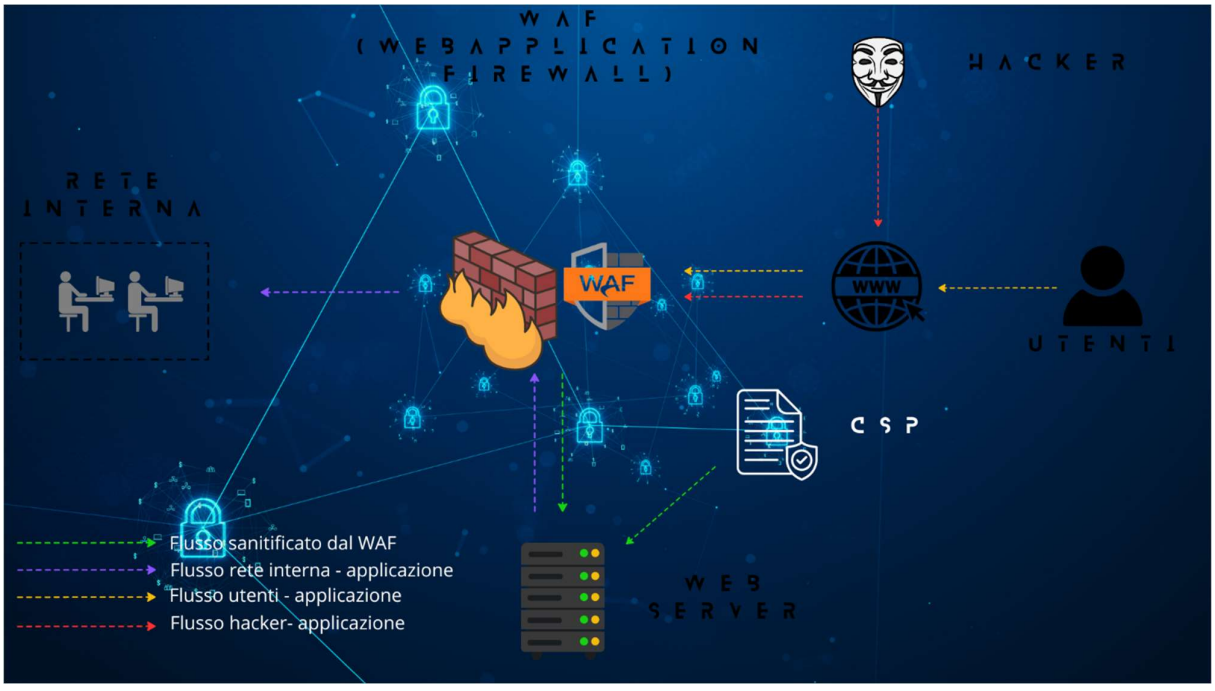
- Utilizzo di query parametrizzate
- Implementazione di Object-Relational Mapping (ORM)
- Validazione e sanitizzazione degli input utente

1.2 Prevenzione Cross-Site Scripting

- Escape dei dati in output
- Sanitizzazione degli input HTML
- Implementazione di Content Security Policy (CSP)

1.3 Misure Generali di Sicurezza

- Implementazione di un Web Application Firewall (WAF)
- Utilizzo di strumenti di testing e auditing come OWASP ZAP, Burp Suite, e SQLMap



2. Impatto sul Business di un Attacco DDoS

L'applicazione Web ha subito un attacco DDoS che l'ha resa non raggiungibile per 10 minuti. Calcoliamo l'impatto economico:

Costo del Tempo di Inattività (CoD) = Guadagno per Minuto (GpM) x Tempo di Inattività (TdI)

CoD = 1.500 € x 10 minuti = 15.000 €

L'impatto economico diretto dell'attacco DDoS è stato di 15.000 €.

2.1 Azioni Preventive contro Attacchi DDoS

- Implementazione di sistemi di filtraggio del traffico e blocco IP
- Utilizzo di Content Delivery Network (CDN)
- Implementazione di sistemi di rilevamento e mitigazione DDoS
- Scaling delle risorse server
- Attivazione di SYN Cookies

3. Response a un'Infezione da Malware

In caso di infezione da malware, la priorità è impedire la propagazione sulla rete interna. Ecco le azioni di risposta proposte:

3.1 Isolamento della Macchina Infetta

- Utilizzo di Network Segmentation e VLAN con pfSense o firewall avanzati

- Creazione di una VLAN di quarantena per la macchina infetta

3.2 Blocco dell'Accesso dell'Attaccante

- Implementazione di regole firewall con iptables o Windows Firewall
- Utilizzo di IDS/IPS come Snort o Suricata

3.3 Monitoraggio del Traffico di Rete

- Analisi del traffico con Wireshark o Zeek
- Identificazione e blocco di comunicazioni sospette

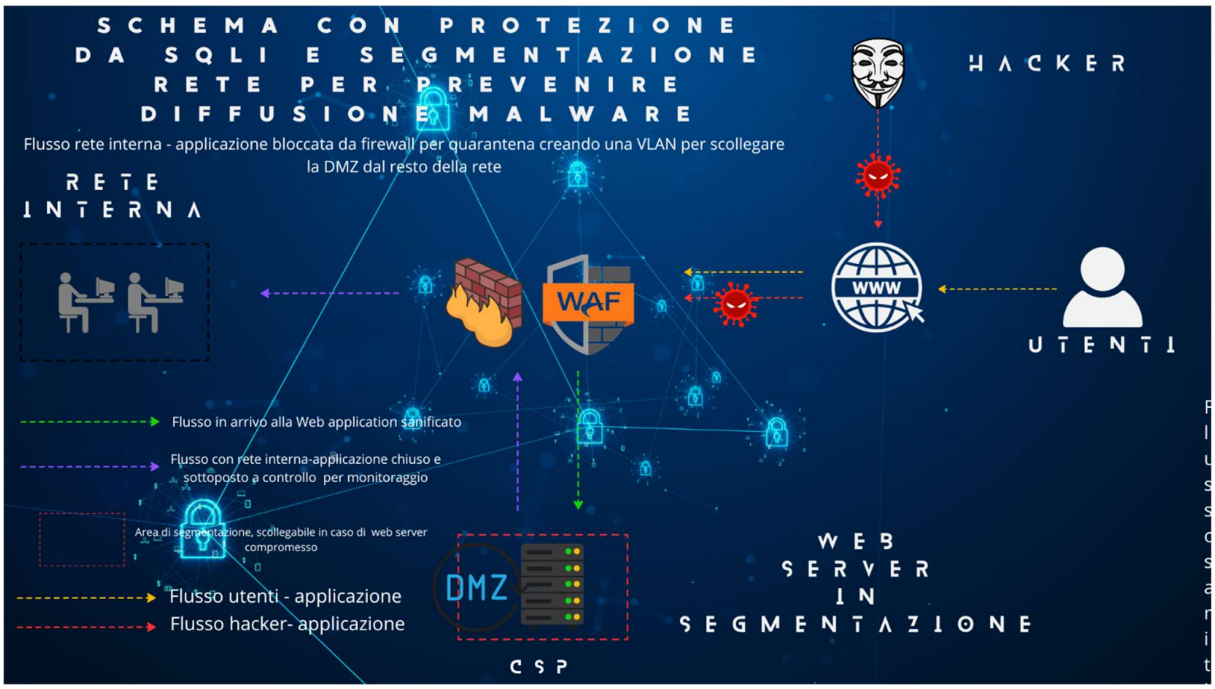
3.4 Contenimento del Malware

- Implementazione di soluzioni EDR come CrowdStrike Falcon o Microsoft Defender for Endpoint
- Analisi del malware in ambiente sandbox come Cuckoo Sandbox

4. Soluzione Completa di Sicurezza

Unendo le azioni preventive e di risposta, otteniamo una soluzione completa che include:

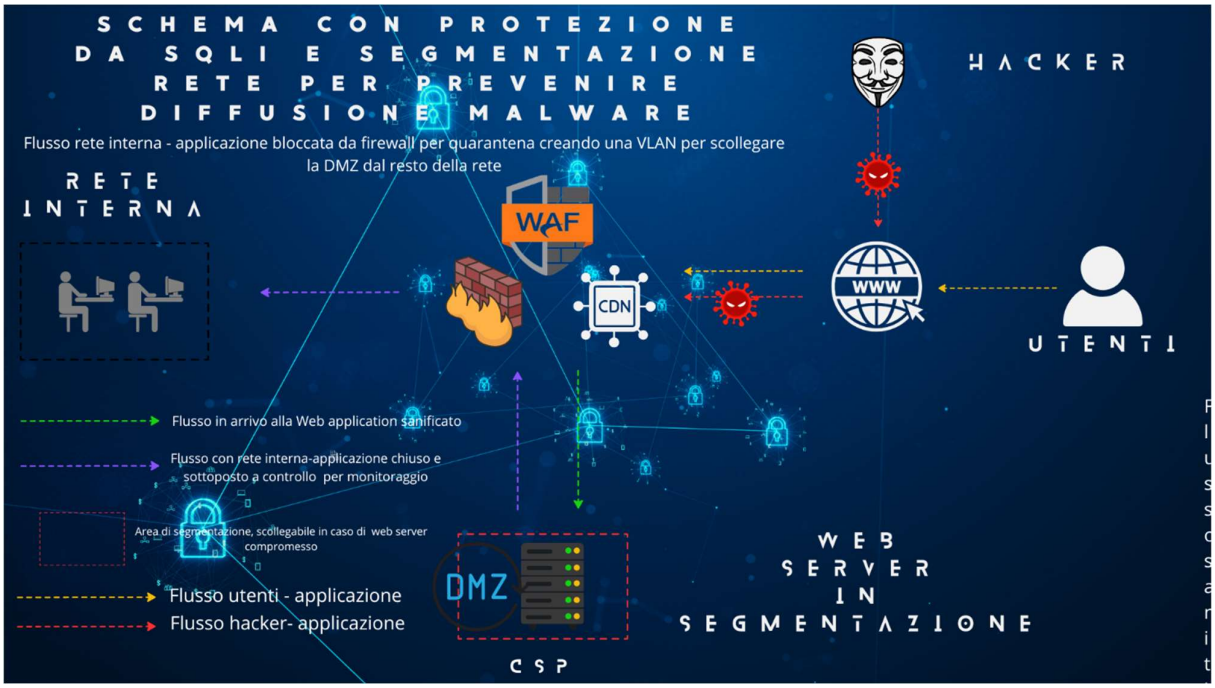
- Prevenzione di SQLi e XSS attraverso pratiche di codifica sicura e WAF
- Mitigazione di attacchi DDoS con CDN e sistemi di filtraggio avanzati
- Isolamento e contenimento rapido in caso di infezioni da malware
- Monitoraggio continuo e analisi del traffico di rete
- Implementazione di un approccio Zero Trust e principio del least privilege



5. Modifiche Aggressive all'Infrastruttura

Per una protezione ancora più robusta, si potrebbero implementare le seguenti modifiche aggressive:

- Adozione completa di un'architettura Zero Trust
- Implementazione di microsegmentazione della rete
- Utilizzo di honeypot per attirare e studiare potenziali attacchi
- Implementazione di sistemi di Threat Intelligence per prevenzione proattiva
- Adozione di soluzioni di sicurezza basate su Intelligenza Artificiale e Machine Learning



Conclusione

Questa relazione ha presentato una strategia completa per affrontare diverse minacce alla sicurezza informatica, dall'implementazione di misure preventive alla gestione di incidenti e al miglioramento continuo dell'infrastruttura. L'adozione di queste pratiche e tecnologie può significativamente ridurre il rischio di compromissione e minimizzare l'impatto di potenziali attacchi.