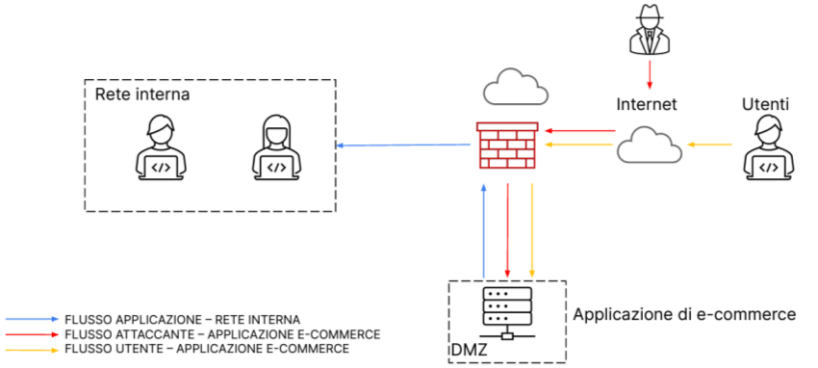
ESERCIZIO W20D4

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)**



1. Azioni preventive contro SQLi e XSS:

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

- **Validazione dei dati in input:** Verificare e validare tutti i dati in ingresso dall'utente per assicurarsi che non contengano codice dannoso o non autorizzato. Utilizzare whitelist per accettare solo input con caratteri previsti.
- **Utilizzo di parametri sicuri nelle query SQL:** Utilizzare query parametrizzate o procedure memorizzate anziché concatenare direttamente stringhe SQL con input utente.
- **Encoding dei dati:** Codificare correttamente i dati in uscita per prevenire attacchi XSS. Utilizzare funzioni di encoding come HTML entities encoding.
- **Aggiornamenti regolari:** Mantenere aggiornati tutti i componenti del software, inclusi framework, librerie e plugin, per ridurre le vulnerabilità note.
- **Firewall e WAF:** Implementare un Web Application Firewall (WAF) per filtrare e monitorare il traffico HTTP/HTTPS e rilevare attacchi noti.

2. Impatti sul business del DDoS:

Se l'applicazione Web è resa non raggiungibile per 10 minuti a causa di un attacco DDoS, l'impatto sul business può essere calcolato come segue:

- **Impatto totale:** (€1500/ minuto) x (10 minuti) = €15,000

Per mitigare gli effetti di un attacco DDoS, si possono adottare azioni preventive come:

- **Utilizzo di CDN:** Utilizzare una Content Delivery Network (CDN) per distribuire il traffico e filtrare il traffico malevolo in caso di attacco DDoS.
- **Servizi di mitigazione DDoS:** Sottoscrivere servizi di mitigazione DDoS forniti da terze parti per filtrare il traffico dannoso prima che raggiunga l'applicazione.

3. **Response contro il malware:**

Se l'applicazione Web è infettata da un malware e l'obiettivo principale è prevenire la propagazione all'interno della rete interna, si possono adottare le seguenti azioni:

1. Isolamento della Macchina Infetta:

- **Disconnessione dalla Rete Interna:** La prima azione dovrebbe essere disconnettere immediatamente la macchina infetta dalla rete interna. Questo può essere fatto attraverso regole di firewall o configurazioni di rete che impediscono la comunicazione della macchina compromessa con altri dispositivi all'interno della rete.
- **Segmentazione di Rete:** L'architettura di rete dovrebbe essere progettata in modo tale da avere segmenti distinti o zone demilitarizzate (DMZ) che limitano il potenziale danno in caso di compromissione. Isolare la macchina infetta in un segmento separato riduce il rischio di diffusione del malware alla rete interna.

2. Analisi del Malware:

- **Identificazione della Minaccia:** Analizzare il malware per comprendere la sua natura e il comportamento. Questo può coinvolgere l'uso di software antivirus/antimalware avanzato o servizi di analisi comportamentale per identificare la firma e il comportamento del malware.
- **Monitoraggio del Traffico:** Implementare un monitoraggio attivo del traffico di rete per rilevare eventuali tentativi di comunicazione o propagazione da parte del malware. Questo può aiutare a identificare altri dispositivi o segmenti di rete che potrebbero essere stati compromessi.

3. Pulizia e Ripristino:

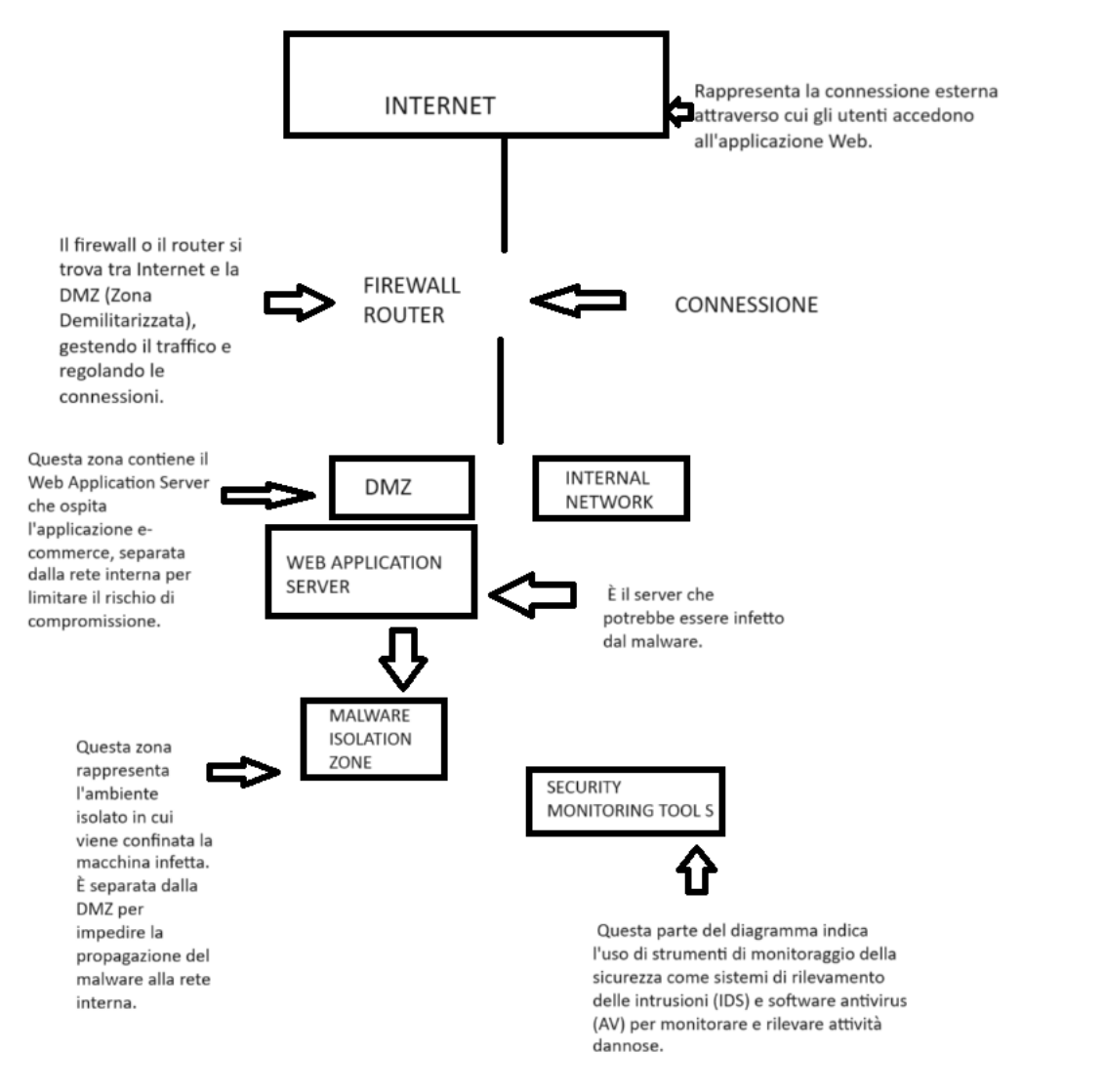
- **Rimozione del Malware:** Una volta identificato il malware, procedere con la sua rimozione completa dalla macchina infetta. Questo può richiedere l'utilizzo di strumenti specializzati e l'intervento da parte di esperti di sicurezza informatica.
- **Ripristino dei Servizi:** Dopo aver rimosso il malware, eseguire un processo di ripristino dei servizi e delle funzionalità dell'applicazione Web. Verificare l'integrità del sistema e applicare patch di sicurezza per chiudere eventuali falle che potrebbero essere state sfruttate dal malware.

4. Monitoraggio Post-incidente:

- **Analisi delle Cause:** Condurre un'analisi post-incidente per comprendere le cause radicate che hanno permesso al malware di compromettere l'applicazione. Questo può portare a miglioramenti nelle politiche di sicurezza, nelle procedure di gestione degli accessi e nelle misure di protezione.
- **Implementazione di Misure Preventive:** Basandosi sull'analisi dell'incidente, implementare azioni preventive aggiuntive per rafforzare la sicurezza dell'applicazione e della rete. Questo può includere aggiornamenti dei sistemi, formazione degli utenti e miglioramenti dell'infrastruttura di sicurezza.

4. **Soluzione completa:**

Unendo le azioni preventive contro SQLi e XSS con la response al malware, l'architettura modificata potrebbe assomigliare a qualcosa di simile al seguente diagramma:



In questo modo, si implementa un approccio completo per proteggere l'applicazione Web da varie minacce, prevenire gli attacchi e reagire prontamente in caso di compromissione.