Analisi e Proposte di Mitigazione per l'Architettura E-commerce

1. Misure Preventive contro Attacchi a Livello Applicativo (SQL e XSS)

La protezione della Web Application (allocata in DMZ) da attacchi iniettivi (SQL) e di scripting (XSS) richiede un approccio a doppio livello: protezione perimetrale e sicurezza intrinseca del codice.

1.1 Modifiche Architetturali e Perimetrali

L'azione preventiva fondamentale a livello perimetrale è l'introduzione di un **Web Application Firewall (WAF)**.

- **Posizionamento e Funzione del WAF:** Il WAF deve essere interposto tra il Firewall di frontiera (o il livello Internet) e la Web Application in DMZ. A differenza dei firewall di rete standard, il WAF opera al Livello 7 (Applicazione) del modello OSI, ispezionando il contenuto del traffico HTTP/HTTPS e bloccando *payload* malevoli che non rispettano i profili di sicurezza definiti (es. tentativi di iniezione di codice SQL o script XSS).
- **Centralizzazione della Visibilità (SIEM/SOAR):** Per garantire una gestione proattiva degli incidenti, si propone l'integrazione di una piattaforma **Security Information and Event Management (SIEM)** e **Security Orchestration, Automation, and Response (SOAR)**. Questa soluzione centralizza gli *event log* provenienti dal WAF, dai Firewall e dagli host della DMZ e della Rete Interna, consentendo l'analisi correlata degli eventi e l'automazione delle risposte in caso di rilevamento di attacchi complessi.

1.2 Misure di Sicurezza del Codice

Le *Secure Coding Practices* agiscono come difesa di ultima istanza:

- **Prevenzione SQL:** L'unica tecnica efficace è l'uso sistematico di **Prepared Statements** o **Query Parametrizzate**. Questo assicura che qualsiasi input utente venga trattato come dato letterale e non come parte del comando SQL eseguibile, neutralizzando di fatto l'attacco.
- **Prevenzione XSS:** Implementazione dell'**Output Encoding**. Qualsiasi dato fornito dall'utente e destinato alla visualizzazione nel *browser* deve essere codificato in modo che venga interpretato come testo (dati) e non come codice HTML o JavaScript.

2. Valutazione e Mitigazione dell'Impatto Finanziario da Attacco DDoS

2.1 Calcolo dell'Impatto Economico

L'attacco Distributed Denial of Service (DDoS), causando l'indisponibilità del servizio e-commerce per 10 minuti, comporta una perdita diretta di ricavi:

- $$1.500\ €/\text{minuto} \times 10\ \text{minuti} = 15.000\ €$$

2.2 Strategie Preventive Anti-DDoS

La prevenzione del DDoS richiede l'esternalizzazione della mitigazione a un livello superiore:

- **Integrazione Cloud-Based DDoS Mitigation Service:** È necessario instradare il traffico Internet attraverso un **Content Delivery Network (CDN)** o un servizio specializzato di mitigazione DDoS basato su Cloud (es. Provider Tier 1). Tali servizi possiedono la capacità di *scrubbing* e banda illimitata per assorbire e filtrare attacchi volumetrici (L3/L4) e a livello applicativo (L7) prima che il traffico raggiunga la connettività di base dell'azienda.
- **Rate Limiting e Throttling:** Configurazione di policy sul WAF o sul *load balancer* per limitare il numero di richieste (RPS) provenienti da singole sorgenti IP, mitigando attacchi a basso volume o tentativi di *scraping*.

3. Risposta agli Incidenti: Contenimento della Propagazione Malware

Lo scenario richiede una risposta rapida e chirurgica per contenere un'infezione malware su un server ospite, impedendo il movimento laterale e la compromissione di altri asset.

3.1 Tecniche di Contenimento e Architetturali

Tecnica di Risposta	Descrizione e Ruolo Strategico
Endpoint Detection and Response (EDR)	L'installazione di agenti EDR su tutti gli host (DMZ e Interna) è cruciale per la visibilità in tempo reale e l'analisi comportamentale. L'EDR può identificare e bloccare automaticamente i tentativi di persistenza e movimento laterale.
Micro-segmentazione e Network Access Control (NAC)	Implementazione di firewall interni e/o del NAC per segmentare logicamente la rete. In caso di rilevamento di un host infetto, il NAC applica immediatamente una policy di **isolamento**, declassando il dispositivo ad un ambiente di quarantena con accesso limitato (solo verso il server EDR/SIEM).

Intrusion Prevention System (IPS)	Posizionare un IPS tra la DMZ e la Rete Interna. Questo sistema ispeziona il traffico per rilevare firme di *Command and Control* (C2) o exploit noti utilizzati per la comunicazione o la propagazione del malware.

Azione di Risposta Chiave: L'azione prioritaria è l'**isolamento immediato** dell'host infetto tramite la disabilitazione della porta di rete (attuata dal NAC) o l'applicazione di policy restrittive sul firewall che ne blocchino il traffico in uscita e in entrata, confinandolo.

4. Evoluzione Architetturale Aggressiva (Zero Trust)

L'azione più incisiva per rafforzare globalmente la sicurezza implica una migrazione verso un'architettura **Zero Trust** e la consolidazione delle funzionalità di sicurezza.

1. **Adozione Completa del Modello Zero Trust:**
    - **Principio del Minimo Privilegio:** Tutte le comunicazioni interne ed esterne devono essere basate su un rigoroso principio di *need-to-know access*.
    - **Micro-segmentazione Olistica:** Estendere la segmentazione al livello dell'applicazione e dell'host, implementando firewall software o policy VPC/VLAN strette, rendendo il movimento laterale estremamente complesso per gli attaccanti.
2. **Integrazione CDN/DDoS Professionale:** Come proposto al punto 2, l'esposizione Internet deve essere interamente gestita da un servizio di mitigazione DDoS/CDN esterno.
3. **Next-Generation Firewall (NGFW) con Ispezione SSL/TLS:** Sostituire o potenziare i firewall perimetrali con NGFW capaci di:
    - Funzionalità integrate di WAF e IPS avanzate.
    - **Ispezione del Traffico Cifrato (SSL/TLS Inspection):** Decifrare e ispezionare il traffico criptato in transito (ove legalmente e tecnicamente permesso) per rilevare minacce nascoste all'interno delle sessioni sicure

Questa strategia sposta il baricentro della sicurezza dalla protezione del perimetro (che da solo è insufficiente) alla verifica continua di ogni singola transazione e accesso all'interno della rete.