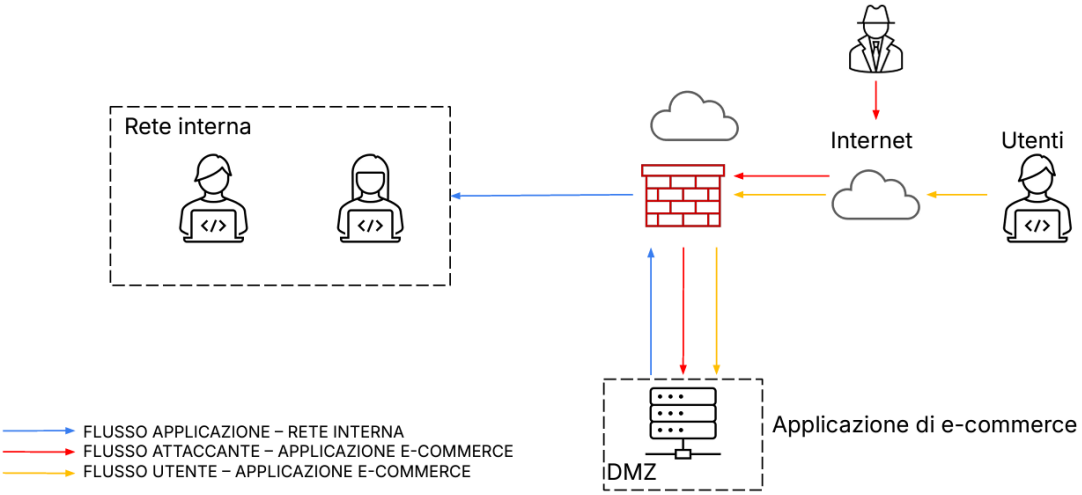
EPICODE PROGETTO W20D4

Report: Security Operation

Data di esecuzione: 06/04/2025
Sviluppato da: **Andrea Surico**
Ambiente:

- ☐ **Attaccante:** Presunto utente malintenzionato
- ☐ **Target:** Rete Interna, piattaforma di e-commerce



Rispondere ai quesiti di un ipotetico scenario presente in slide:

1) **Azioni Preventive:** implementazioni per difesa da attacchi di tipo SQLi oppure XSS
2) **Impatti sul business:** calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio
3) **Response:** gestione priorità e propagazione malware
4) **Soluzione completa:** unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

1. Azioni Preventive

L'obiettivo è quello di difendere l'applicazione web da attacchi di tipo SQL Injection e Cross-Site Scripting da parte di un utente malintenzionato.

Misure di sicurezza consigliate:

1. **Web Application Firewall (WAF):** Il WAF è in grado di analizzare il traffico HTTP/HTTPS e bloccare pattern noti di SQLi e XSS, dovrebbe essere posizionato tra Internet e l'applicazione e-commerce.
2. **Input Validation e Output Encoding:** Il primo è una tecnica di protezione a livello di codice, usata per evitare attacchi come **SQL injection o XSS.** Controlla che i dati inseriti dall'utente siano corretti, attesi e sicuri. Il secondo codifica i caratteri speciali in modo che **non vengano interpretati come codice**. Serve a **sanitizzare l'output** prima che venga visualizzato all'utente, così da **evitare XSS (Cross-Site Scripting)**.
3. **Aggiornamenti e patch:** Mantenere sempre aggiornati il sistema operativo, il database e le librerie applicative, per ridurre la superficie di attacco.
4. **Least Privilege e segmentazione di rete:** Il primo è un principio di sicurezza secondo cui ogni utente, dispositivo o processo deve **avere solo i privilegi strettamente necessari** per svolgere il proprio compito, **niente di più.** La **segmentazione** consiste nel dividere la rete in blocchi separati **(subnet o VLAN),** ognuno con accesso limitato alle altre parti. L'obiettivo è quello di limitare la diffusione degli attacchi e migliorare il controllo del traffico.

- **Least Privilege** controlla **chi può fare cosa**.

- **Segmentazione** controlla **chi può andare dove**.

2. Impatto sul business

Scenario: L'applicazione Web subisce un attacco DDoS dall'esterno, risultando non raggiungibile per 10 minuti.

Calcolo dell'impatto economico

- Dato: ogni minuto gli utenti spendono in media 1.500 € sulla piattaforma.
- Se il servizio non è raggiungibile per 10 minuti, la perdita stimata = 1.500 € * 10 = **15.000 €** di mancato guadagno.

(Ovviamente, questo è un calcolo semplificato, nella realtà potrebbero esserci altri impatti, come danno)

Azioni preventive contro i DDoS:

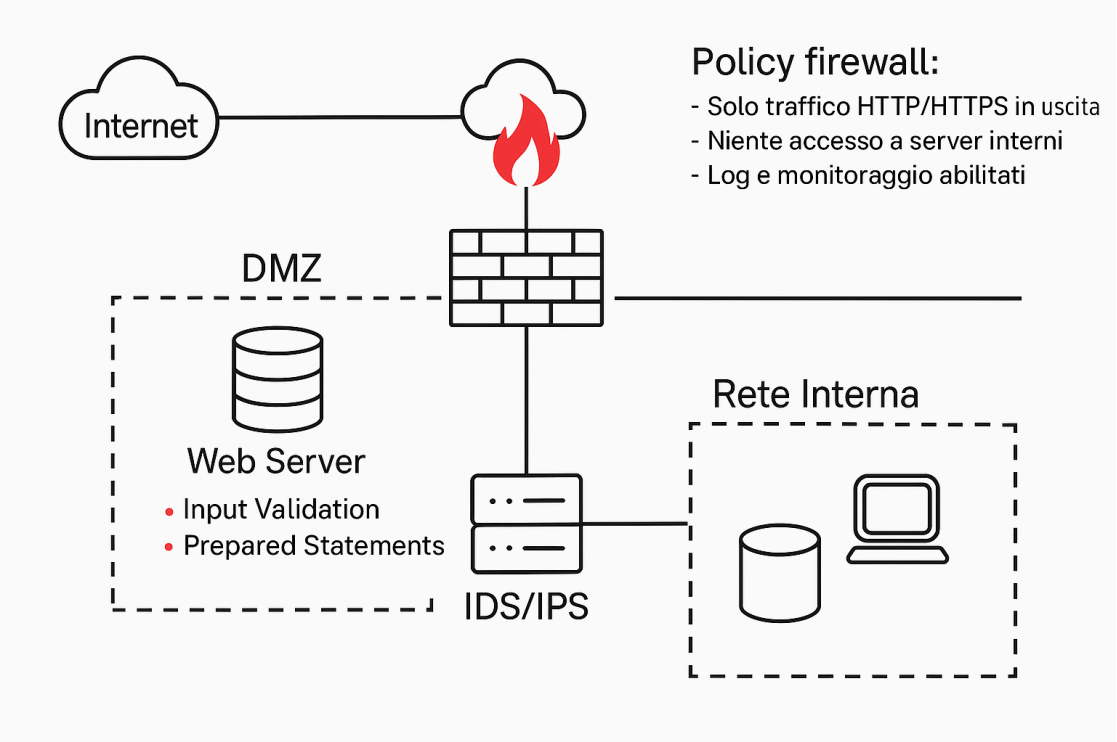
E' possibile aggiungere dei servizi che assorbono e filtrano il traffico malevolo prima che raggiunga la rete.

3. Response

Scenario: Il server Web nella DMZ viene infettato da un malware.
Priorità: Impedire la propagazione del malware sulla rete interna. Non è prioritario rimuovere l'accesso all'attaccante al server infetto.

- Aggiornare le regole di firewall per bloccare o limitare i flussi dal server DMZ verso la rete interna
- Mantenere l'accesso alla macchina infetta per osservare i movimenti dell'attaccante (honeypot parziale).
- Configurare un **IDS/IPS** (Intrusion Detection/Prevention System) o un **SIEM** (Security Information and Event Management) per registrare i tentativi di movimento laterale.

4. Soluzione completa



🔐 **Firewall** ben configurato
🛡️ **IDS/IPS** per monitoraggio tra DMZ e rete interna
🌐 **DMZ separata** con web server esposto
🏠 **Rete interna protetta** con database e postazioni isolate

N.B. Avrei voluto creare una presentazione più pratica e diretta attraverso l'utilizzo di **Cisco Packet Tracer**, non l'ho fatto per mancanza di tempo. Lo schema è stato creato con **IA.**