Progetto

Pablo Andres Balbuena Rios

Progetto della settimana 9

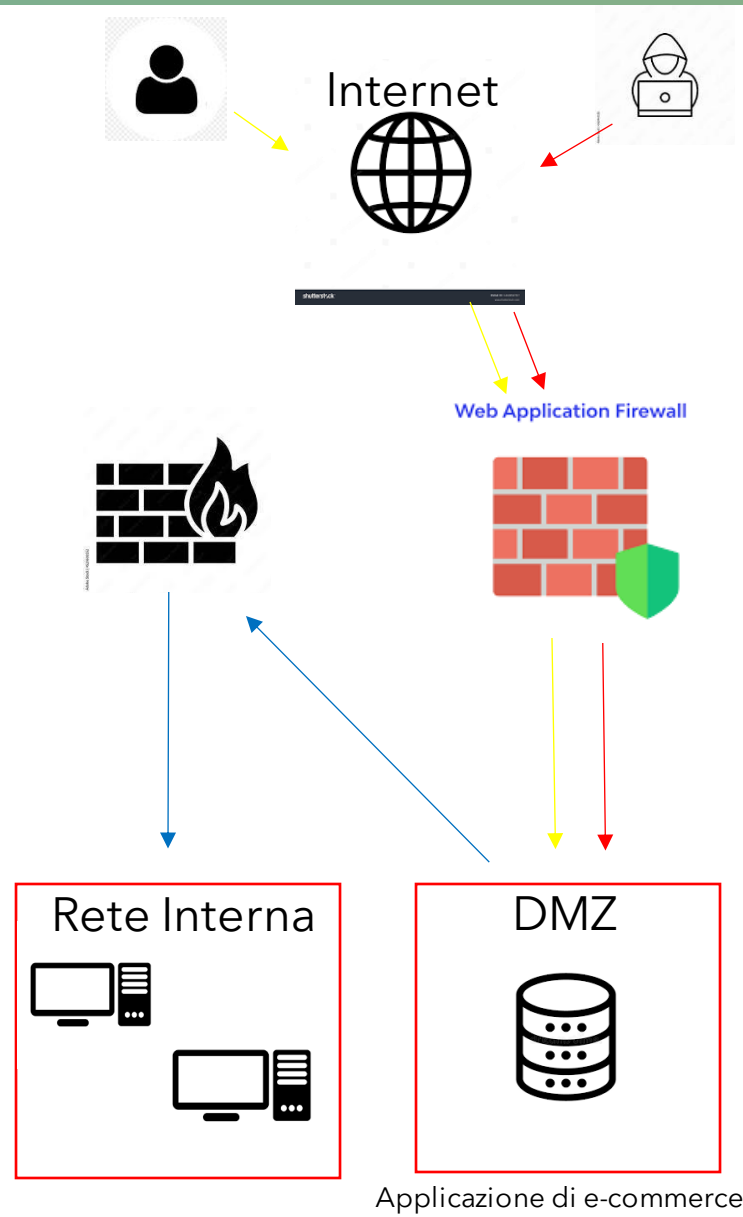
Traccia: Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1.Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLioppure 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 DDoSdall'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 malwarenon 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: integrando eventuali altri elementi di sicurezza

Azioni preventive

Per prevenire da un attacco come SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), abbiamo bisogno di un Web Application Firewall (WAF), cioè un'applicazione o dispositivo progettato per proteggere le applicazioni web da una varietà di minacce online.

In questo caso facciamo il modo che tutte le persone fuori dalla rete interna che vogliono andare all'applicazione di e-commerce, che si trova nel DMZ "Zona demilitarizzata", debbano passare attraverso il WAF, invece le persone che stanno nella rete interna possono comunicarsi attraverso il Firewall.



Impatti sul business

Se noi volessimo calcolare l'impatto sul Business da un punto di vista quantitativo, si calcola trovando la media di perdita durante quel periodo di non raggiungibilità:
10*1500= 15000 €

DATI	
Tempo	10 min
perdita/tempo	1500 €/min

Misurare l'impatto sul business è un processo fondamentale per valutare gli effetti delle decisioni e delle attività aziendali su vari aspetti, compresi quelli finanziari, operativi e strategici. Questa misurazione fornisce un quadro chiaro delle conseguenze delle azioni intraprese, aiutando le organizzazioni a prendere decisioni informate e a ottimizzare le proprie operazioni.

Invece se noi volessimo calcolare l'impatto sul Business da un punto di vista qualitativo, bisognerebbe considerare tutti gli impatti «non numerici» sul business come:

- Fiducia del Cliente
- Soddisfazione del Cliente
- Reputazione

Impatti sul business

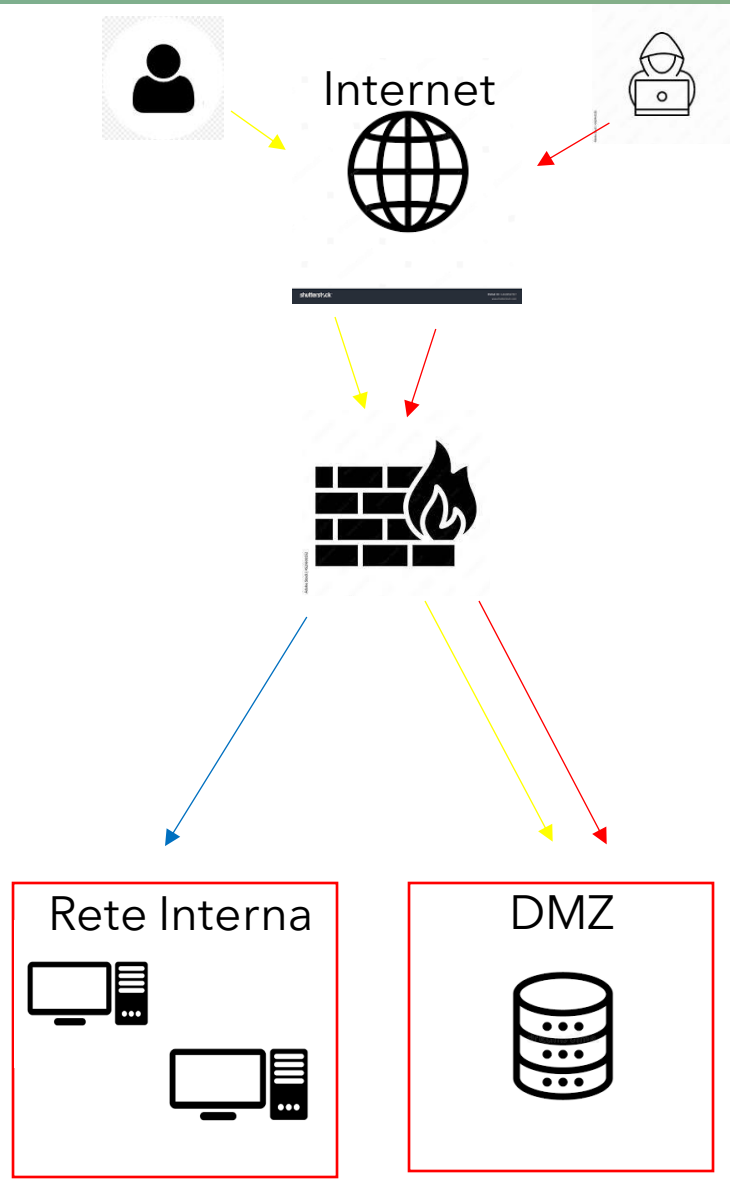
Come possiamo prevenire un attacco DDOS:

- Usare un Bilanciamento del carico, ovvero distribuire il traffico in modo uniforme tra più server. Questo aiuta a prevenire la saturazione di un singolo server durante un attacco DDoS.
- Oppure Utilizzo di una Content Delivery Network (CDN), cioè una distribuzione del carico su server distribuiti geograficamente.

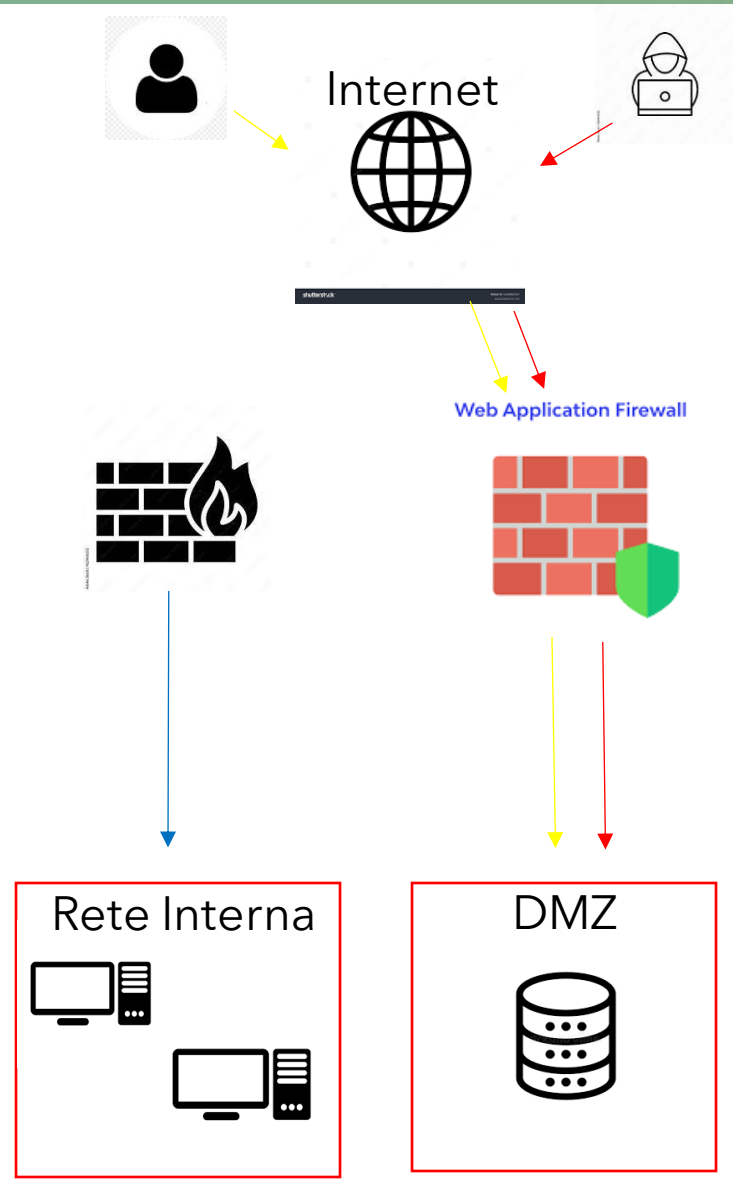
- Tramite l'utilizzo di un SIEM (Security Information Event Management), un insieme di strumenti in grado di analizzare in tempo reale i log, è possibile garantire un elevato livello di protezione contro minacce interne ed esterne. Grazie a questa tecnologia, è possibile anche formulare una policy di sicurezza che notifica immediatamente il responsabile del sistema al rilevamento di accessi anomali alla macchina, evidenziando potenziali minacce o comportamenti sospetti.

Response

Nel caso che e-commerce è infettato e che non siamo interessati a rimuovere l'accesso da parte dell'attaccante, possiamo ridurre gli impatti causati dall'incidente attraverso l'**isolamento** dell'applicazione Web, ovvero la completa disconnessione del sistema infetto dalla rete interna, per restringere l'accesso all'attaccante, questo si fa togliendo le policy sul firewall che precedentemente serviva a raggiungere la rete interna



Soluzione completa



Infrastruttura aggressiva

Per rendere più sicuro possibile la rete, dobbiamo prevenire gli attacchi:

- Per l'attacco SQL Injection ed XSS: dobbiamo avere il WAF
- Per l'attacco DDOS: dobbiamo avere più server per bilanciare il carico.
- Per prevenire l'entrata di un attaccante dal DMZ : Dobbiamo avere un IPS che ci serve per prevenire attacchi informatici in tempo reale.