S9_L5
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

Giorno 5 - Progetto

TRACCIA

Con riferimento alla figura, 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. È richiesta sola modifica.
2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per **10 minuti** . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono ogni 1.200 €** 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)

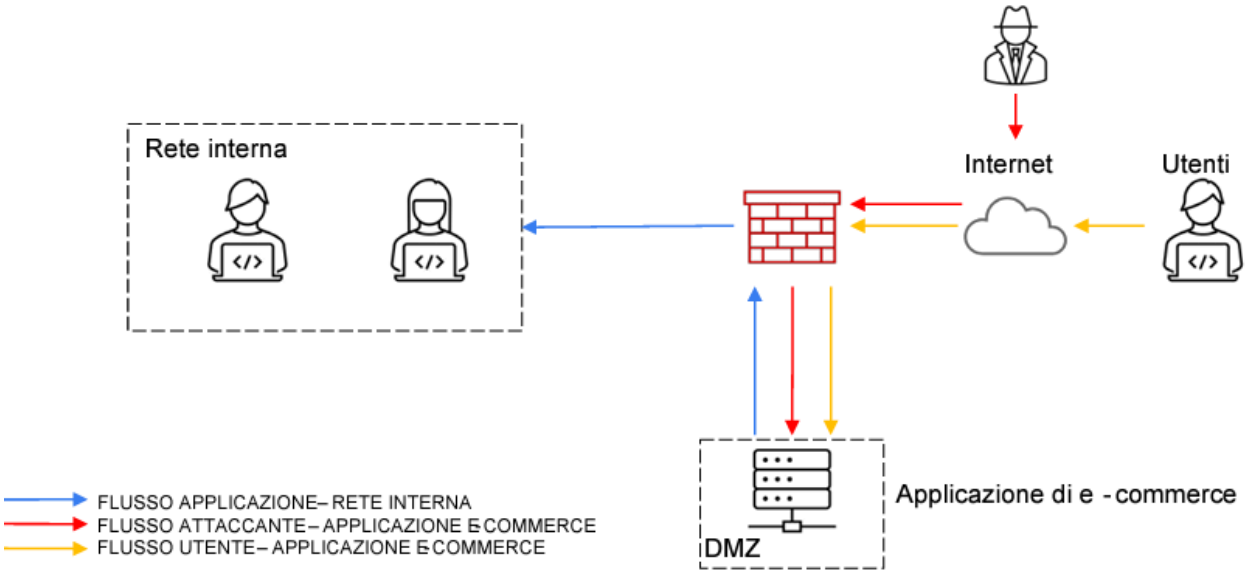
5. **Modifica «più aggressiva» dell'infrastruttura**: integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2)

   Budget 5000-10000 euro. Eventualmente fare più proposte di spesa.

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

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?

Per prevenire gli attacchi SQL injection e XSS si possono implementare diverse azioni, tra cui:

- **Educare il personale** sulle pratiche di sicurezza;
- Mantenere il **software aggiornato**;
- Eseguire spesso **test di sicurezza** per identificare nuove vulnerabilità;
- Filtrare il traffico usando dei **WAF** (Web Application Firewall).

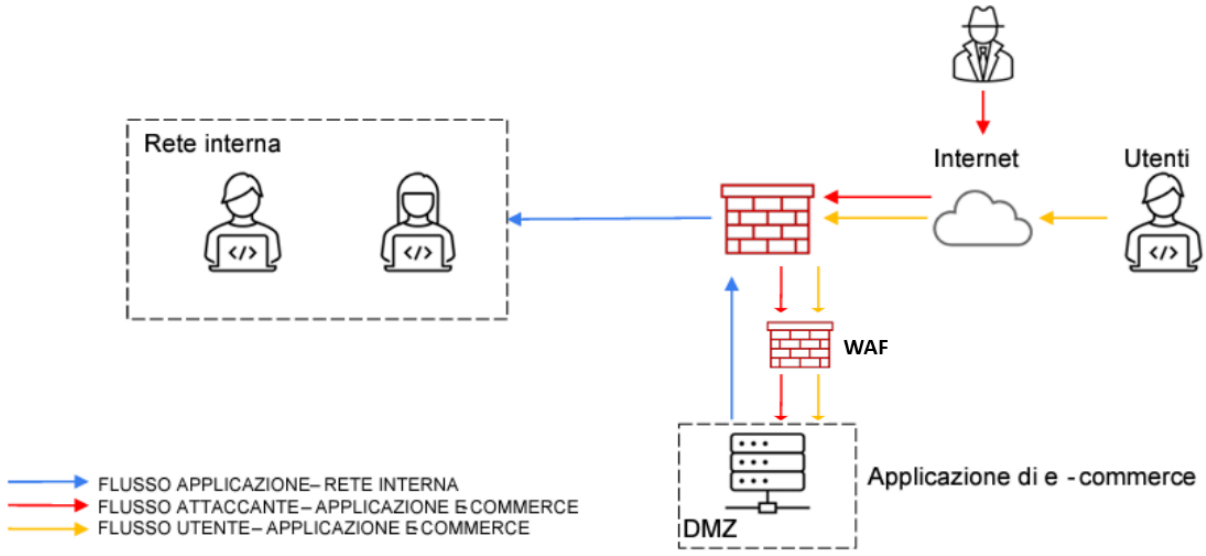
L'azione per prevenire qualsiasi attacco SQLi ed XSS consiste, come prima cosa, nel sanitizzare gli input. Facendo ciò chiudiamo le vie d'attacco dei potenziali attaccanti.

In quanto si parla di possibili attacchi di tipo SQLi e XSS, si può implementare uno strumento progettato per proteggere le applicazioni Web, monitorando e filtrando il traffico, ovvero il **WAF.**

Il WAF:

- Controlla tutte le richieste che arrivano all'applicazione web e blocca quelle sospette.
- Riconosce e blocca tentativi di attacchi comuni come SQL Injection e Cross-Site Scripting (XSS).
- Permette di creare regole specifiche per proteggere meglio l'applicazione.
- Aiuta a difendersi da nuove vulnerabilità, anche quelle appena scoperte.
- Registra tutti i tentativi di attacco e fornisce report dettagliati per analizzare cosa è successo.

Quindi implementare un WAF migliora la sicurezza delle applicazioni web e protegge il server da vari tipi di attacchi.



Impatti sul business

L'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per **10 minuti** . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono ogni 1.200 €** sulla piattaforma di e-commerce . **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.**

L'impatto sul business è uguale ad:

10 minuti x (1200€/minuto) = 10 x 1200€ = ***12000€***

Le possibili azioni preventive consistono nel:

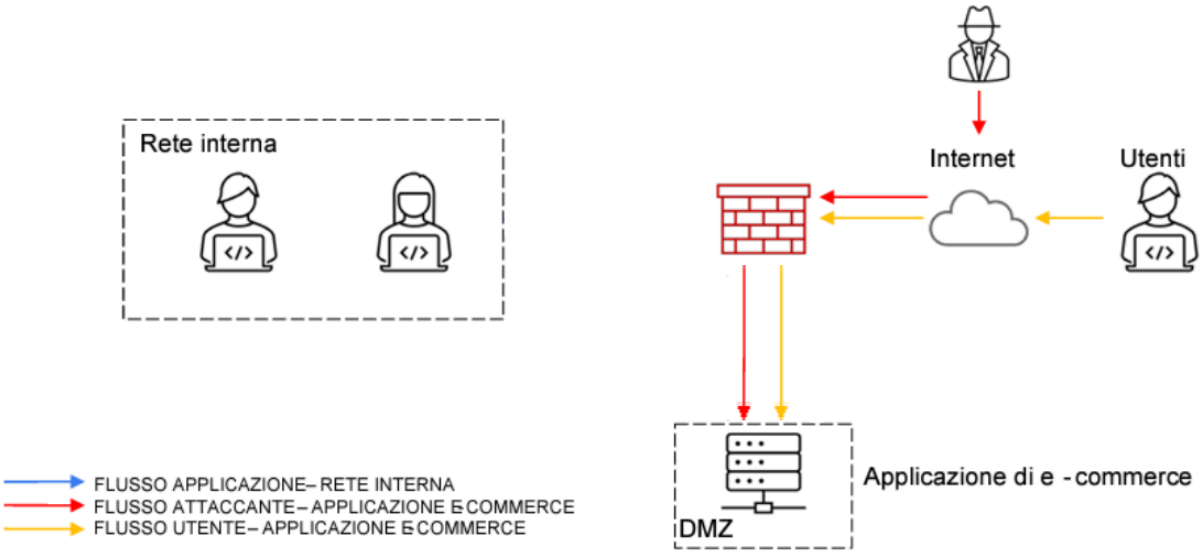
- Utilizzare un **WAF**, per filtrare il blocco malevolo e riducendo il rischio di attacchi tipo DDoS;
- **Servizi Anti-DDoS**, che rilevano e mitigano gli attacchi in tempo reale;
- **CDN**, per mitigare gli effetti degli attacchi DDoS;
- **Bilanciare il carico**, distribuendo il traffico tra più server per evitare il sovraccarico di un singolo server;
- **Monitorare il traffico**, in modo continuo, configurando allarmi per rilevare le attività sospette;
- **Backup e ridondanza**, configurando sistemi di backup pronti per essere attivati in caso di interruzione del servizio.

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.

La priorità consiste nel non far propagare il malware.

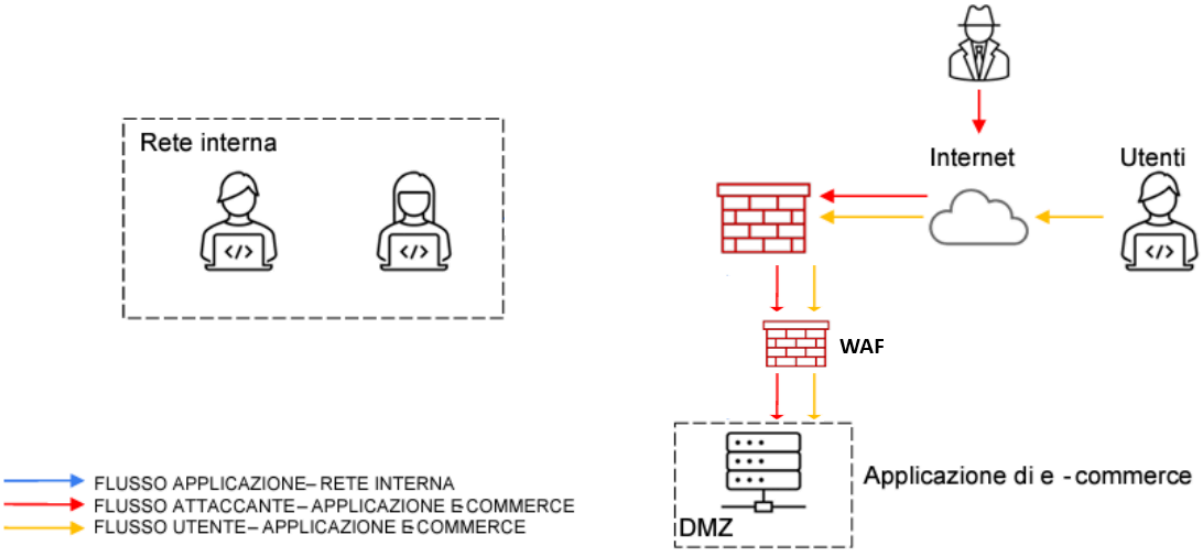
Essendo che il nostro server sarà accessibile via internet, l'obiettivo è quello di non fare propagare il malware nella rete interna, anche se lo stesso server sarà ancora accessibile dall’attaccante.



Si entrerà, quindi, in fase di contenimento, mettendo in isolamento la rete interna. La rete interna non avrà più accesso alla DMZ, mentre gli utenti e l'attaccante avranno ancora la possibilità di connettersi.

Soluzione completa

Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)



Modifica «più aggressiva» dell'infrastruttura

Integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2).

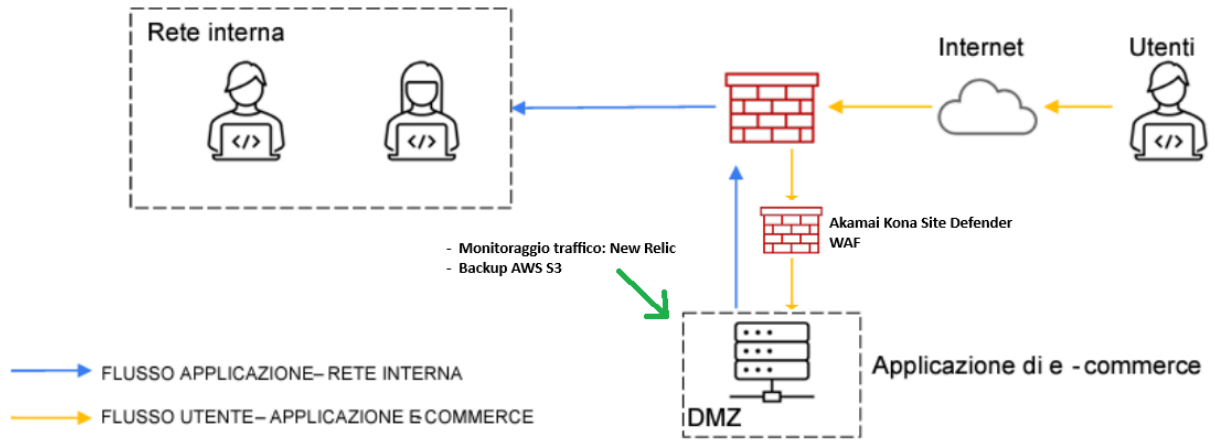
Budget 5000-10000 euro. Eventualmente fare più proposte di spesa.

Con un budget di 5000-10000 euro, possono venire proposte diverse configurazioni per migliorare la sicurezza dell'e-commerce integrando WAF, servizi Anti-DDoS, CDN, monitoraggio del traffico e backup con ridondanze, come precedentemente citate dopo il calcolo dell'impatto sul business.

Configurazione 1:

- **WAF e Servizi Anti-DDoS**: ***Akamai Kona Site Defender***, protezione avanzata contro DDoS e WAF integrato (circa 700-800 euro/mese). Costo annuale: 8400-9600 euro.
- **CDN**: Incluso nel servizio Akamai
- **Monitoraggio del Traffico**: ***New Relic*** (circa 50 euro/mese). Costo annuale: 600 euro.
- **Backup e Ridondanze**: ***AWS S3*** con backup ridondanti (circa 500 euro/anno per 1TB di spazio). Costo annuale: 500 euro.

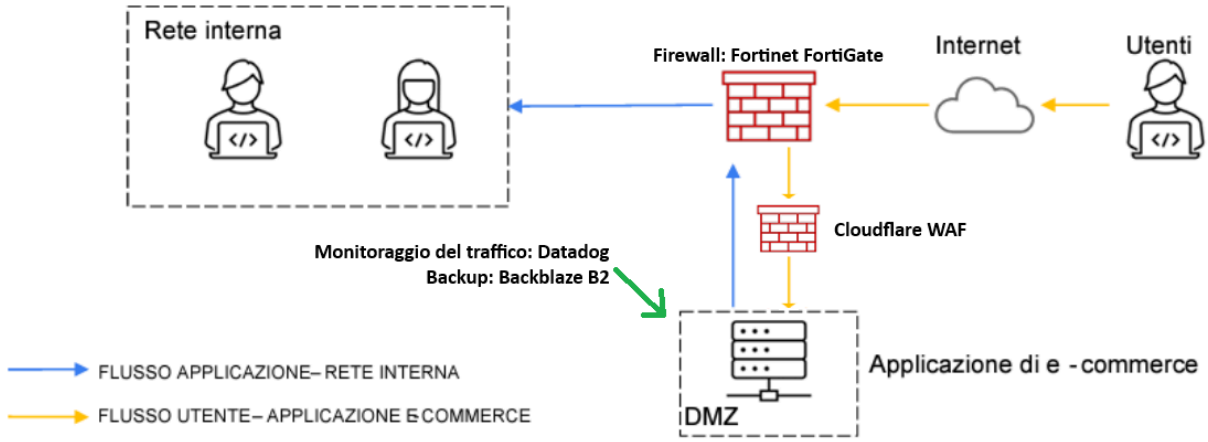
Totale: 9500-10700 euro/anno.



Configurazione 2 (con la sostituzione del Firewall):

- **WAF e Servizi Anti-DDoS**: ***Cloudflare Business Plan***, protezione avanzata contro DDoS e WAF integrato (circa 200 euro/mese). Costo annuale: 2400 euro.
- **CDN**: Incluso nel servizio Cloudflare.
- **Monitoraggio del Traffico**: ***Datadog*** (circa 15 euro/host/mese). Costo annuale: 180 euro per un host.
- **Backup e Ridondanze**: ***Backblaze B2*** (circa 100 euro/anno per 1TB di spazio). Costo annuale: 100 euro.
- **Firewall**: ***Fortinet FortiGate*** firewall hardware con protezione avanzata (circa 5000 euro/anno per l'hardware e la licenza base). Costo annuale: 5000 euro.

Totale: 7680 euro/anno



Nella seconda configurazione è stata proposta anche la sostituzione del Firewall con uno più affidabile.