GIORNO 5 – PROGETTO

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.

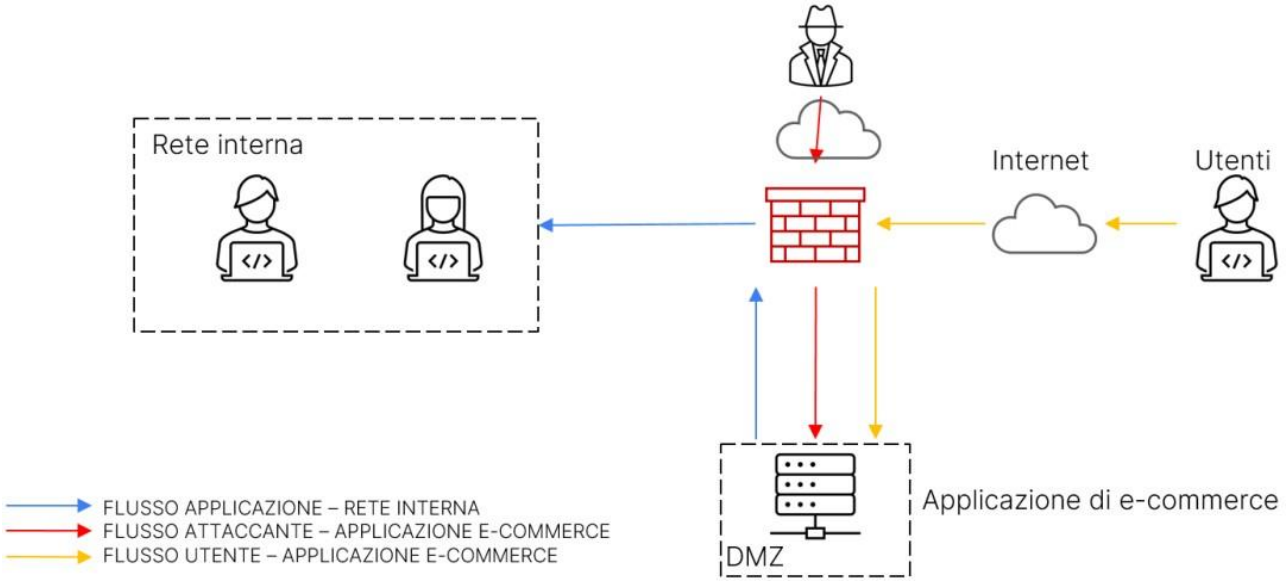
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response

5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo)**

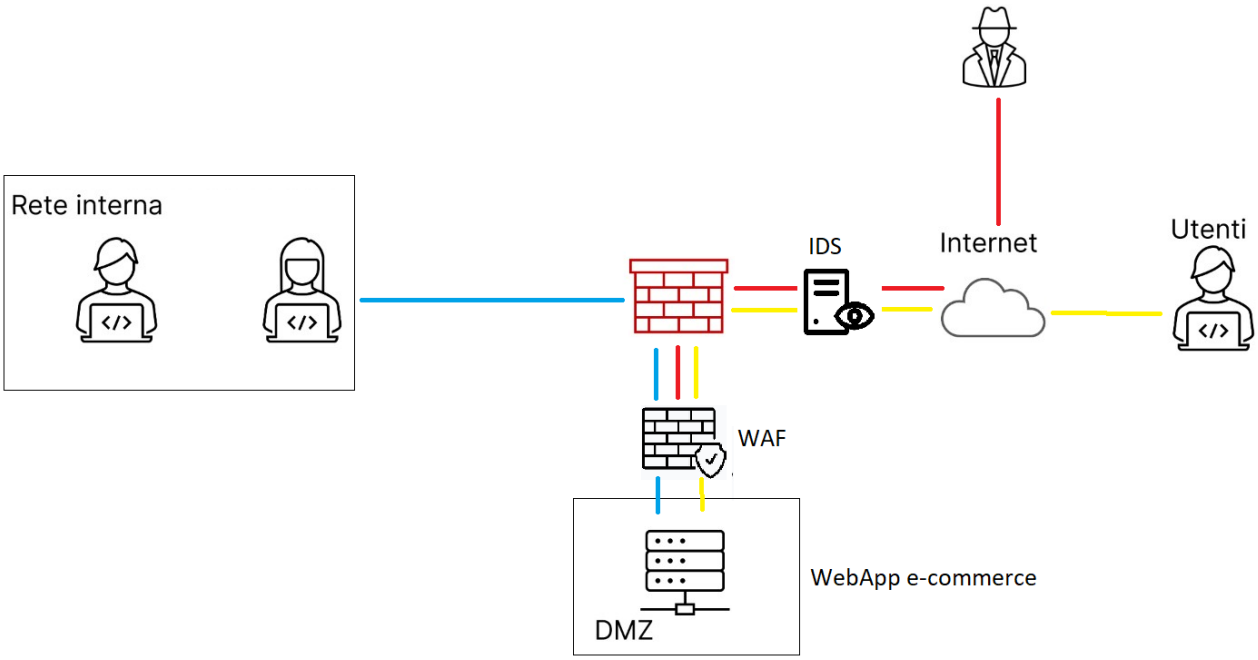
Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

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.



1. **<u>Azioni preventive:</u>**
   Possiamo vedere questo tipo di azioni come l'insieme dei controlli di sicurezza adottati per aumentare il livello di protezione perimetrale/interno per ridurre il rischio di potenziali attacchi.

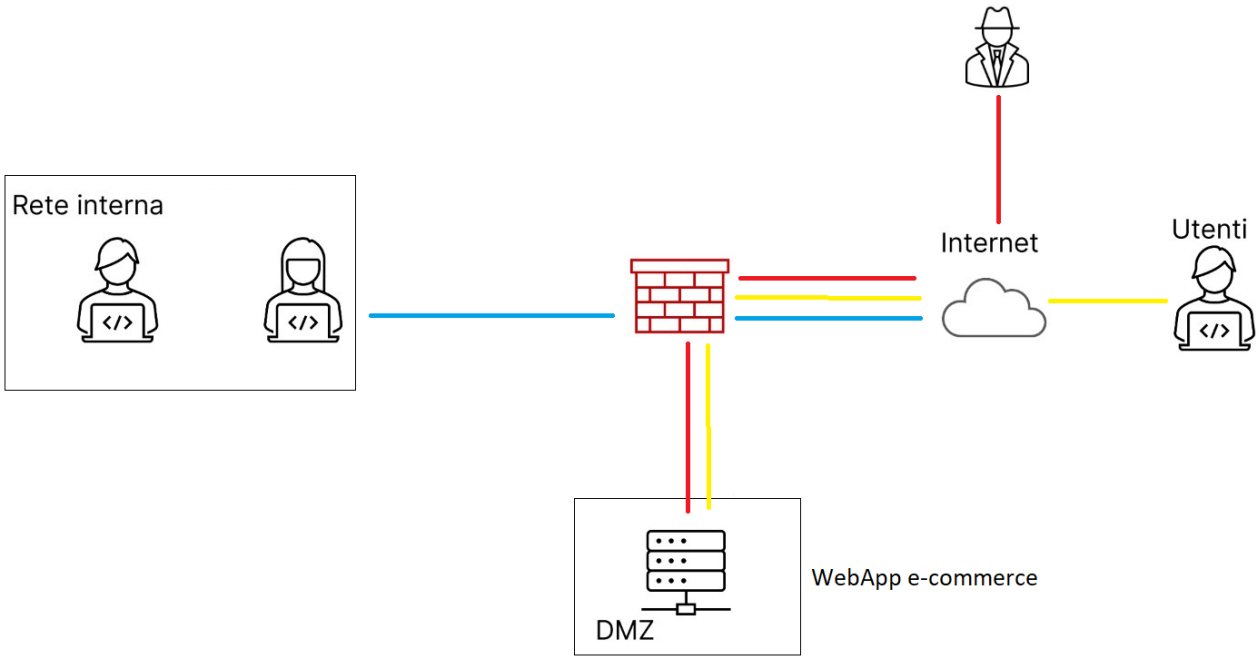
L’implementazione di Firewall perimetrali aiuta a ridurre il rischio di attacchi dall’esterno e funzionano in base a regole e policy ce ne automatizzano la gestione della comunicazione.
Nel nostro caso un **WAF** (Web Application Firewall) sarà il dispositivo di sicurezza più indicato, in quanto specifico per la protezione delle WebApp da attacchi come XSS e SQLi.
Potremo implementare la rete anche con un **IDS** (Intrusion Detection System), un sistema di rilevamento intrusioni, che ha come scopo quello di individuare preventivamente attacchi alla rete monitorandola in tempo reale in cerca di anomalie



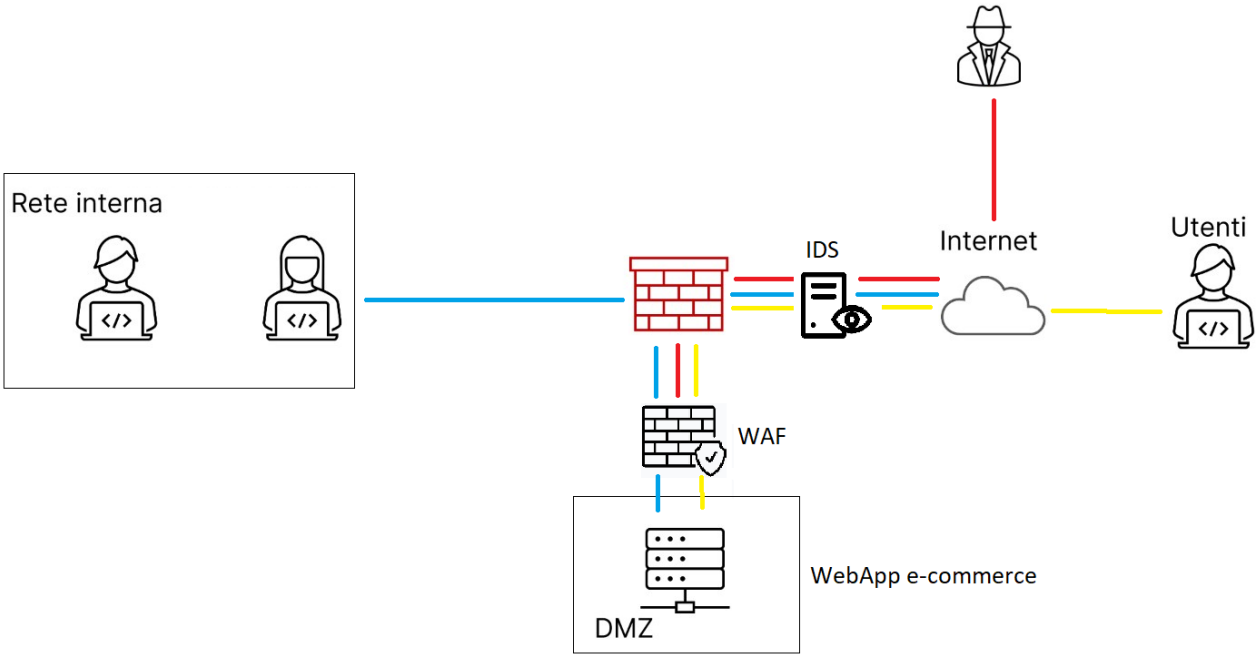
sospette.

2. **<u>Impatti sul business:</u>**
   La WebApp della compagnia sta subendo un attacco **DDoS**; gli attacchi DoS hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, come potrebbe essere un'applicazione web o un sito web. Una delle forme più comune di attacco DoS è la trasmissione di un grande numero di pacchetti ad un server al fine di saturarne la CPU. La forma più comune di DoS è il Distributed DOS (DDoS), come nel nostro caso, ovvero un attacco di tipo denial-of-service che viene inviato contemporaneamente verso un target da sorgenti multiple.
   La WebApp non sarà raggiungibile per 10 minuti per una perdita di 1500€ al minuto, la **perdita totale** per questo lasso di tempo sarà:
   1500 * 10 = **15000€**
   Secondo il fattore di categorizzazione degli incidenti, cioè l’impatto negativo sugli asset della compagnia sia in termini funzionali sia monetari potremo dedurre che la **criticità** dell’evento sarà **Media**, in quanto la compagnia non riuscirà ad erogare alcun servizio critico agli utenti con un impatto economico non indifferente (>10000€/<500000€).
3. **<u>Response:</u>**
   La fase di valutazione ha individuato un malware sulla WebApp, ha inizio quindi la fase di **Contenimento, Eliminazione e Recupero** che ha come scopo la riduzione degli

impatti causati dall'incidente, l'eliminazione dell'incidente dalla rete e dai sistemi e il recupero dei servizi e delle operatività standard.
L'attività di contenimento ha come scopo primario quello di isolare l'incidente in modo tale che non possa creare ulteriori danni e che il malware non si riproduca su altri nodi della rete.
Andremo quindi a creare una rete di quarantena tramite l'**isolamento** della DMZ, con la WebApp infettata, dalla rete interna, lasciando però aperto l'accesso al malintenzionato così da poterne studiare le attività e gli obiettivi.



4. **<u>Soluzione completa:</u>**
   Andremo ad implementare la rete con dei controlli network come:
   NAC (Network Access Control) cioè soluzioni di sicurezza che aiutano a controllare gli accessi alla propria rete limitando l'accesso solo agli utenti autorizzati ed assicurare che solo sistemi che ne soddisfano i requisiti di sicurezza possano accedervi.
   WAF (Web Application Firewall) cioè dispositivi di sicurezza dedicati alla protezione delle WebApp da attacchi di tipo XSS e SQLi.
   IPS/IDS cioè sistemi di prevenzione e rilevamento intrusioni che monitorano la rete per individuare a prevenire preventivamente potenziali attacchi alla rete stessa e alle macchine.
   Controlli sugli end-point quali pc, smartphone o server come **Hardening** dei sistemi e delle configurazioni e **Patching** dei sistemi, oltre a **Group Policy**, cioè delle policy di gruppo che permettono agli amministratori di reti e sistemi di gestire la sicurezza degli end-point in maniera centralizzata.



5. **<u>Modifica aggressiva:</u>**
   Se volessimo implementare più “aggressivamente” l’architettura di rete potremmo includere anche un **IPS** (Intrusion Prevention System), che a differenza del sistema di rilevamento supporta anche delle azioni automatiche per fermare le potenziali intrusioni preventivamente, e un **HoneyPot**, cioè una macchina vulnerabile che funge da esca per gli attaccanti, per garantire ancor più sicurezza alla rete.
   Questo potrebbe comunque comportare latenza, quindi sarebbe bene valutare i pro ed i contro di una eventuale aggiunta di elementi di protezione e prevenzione.