TEST 23/12/2022

FACCILONGO DOMENICO

PROGETTO ANALISI DEI LOG – CASO REALE

TASK

In riferimento alla figura di seguito, rispondere ai seguenti quesiti:

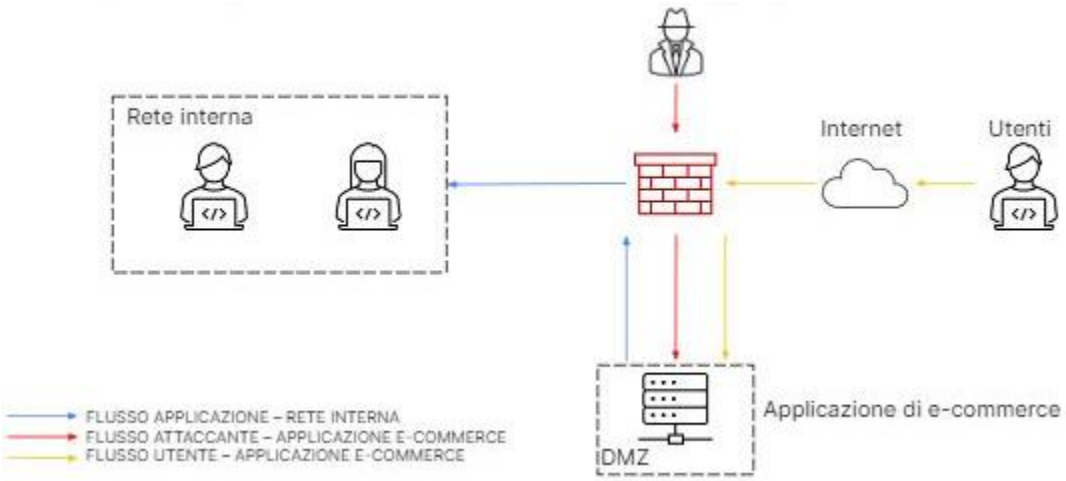
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni

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

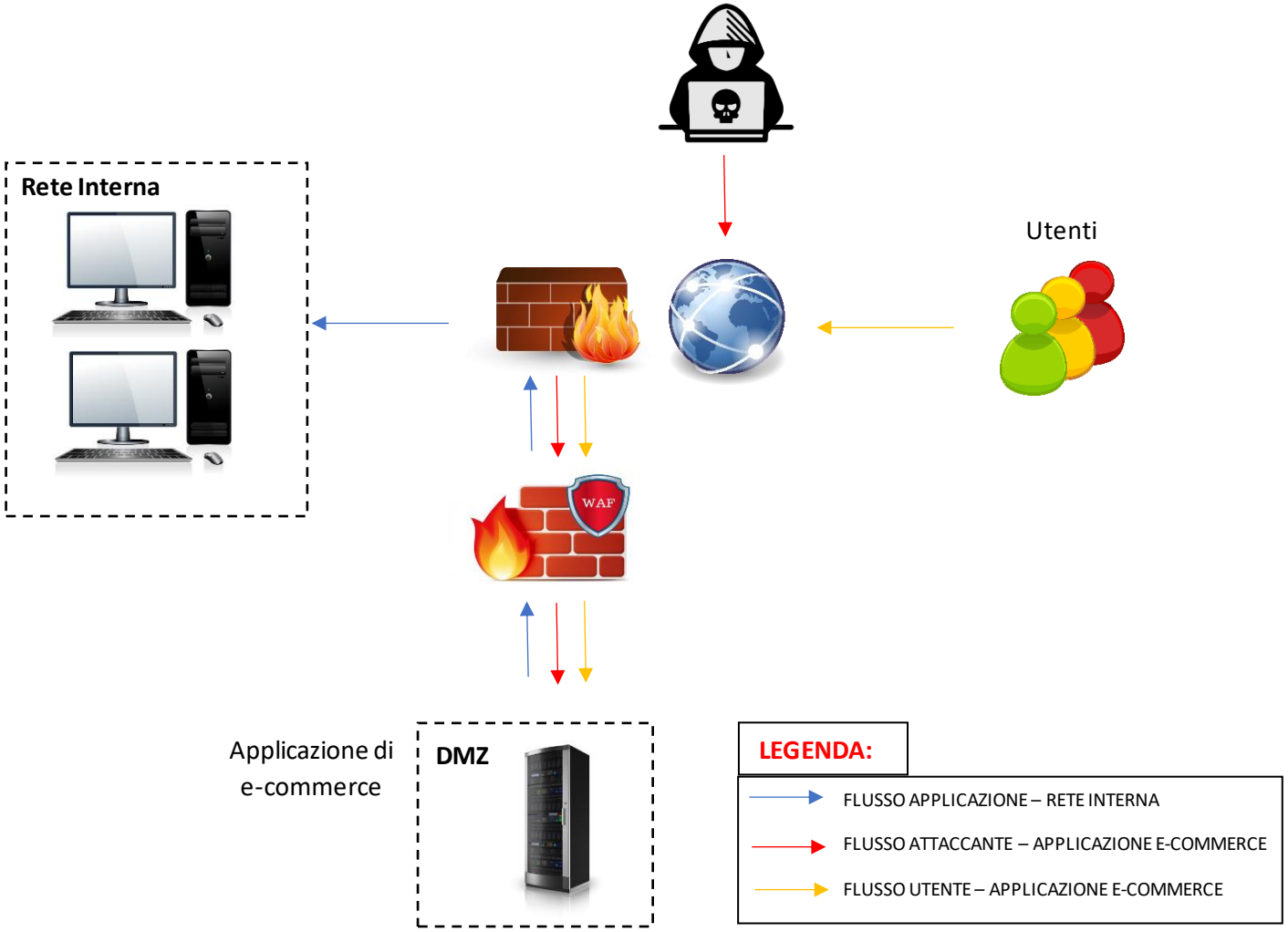
5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo)**



ANALISI E VALUTAZIONE

Eseguiamo i passaggi uno dopo l'altro andando ad analizzare ciascun punto della traccia. Partendo dal presupposto che l'applicazione di e-commerce è disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla **DMZ** per via delle policy firewall, quindi se il server in **DMZ** viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

1. **AZIONI PREVENTIVE:** Supponendo che un utente malintenzionato voglia attaccarci con attacchi del tipo **SQLi** oppure **XSS** la soluzione a tale problema è andare ad inserire uno **WAF** tra il Firewall e la **DMZ**. Il **WAF** è una forma specifica di application firewall che filtra, monitora e blocca il traffico HTTP da e verso un servizio web. Ispezionando il traffico HTTP, può prevenire gli attacchi che sfruttano le vulnerabilità note di un'applicazione Web, come SQL injection, cross-site scripting (XSS). La soluzione, dunque, a questo tipo di problema è rappresentata come da immagine che segue:



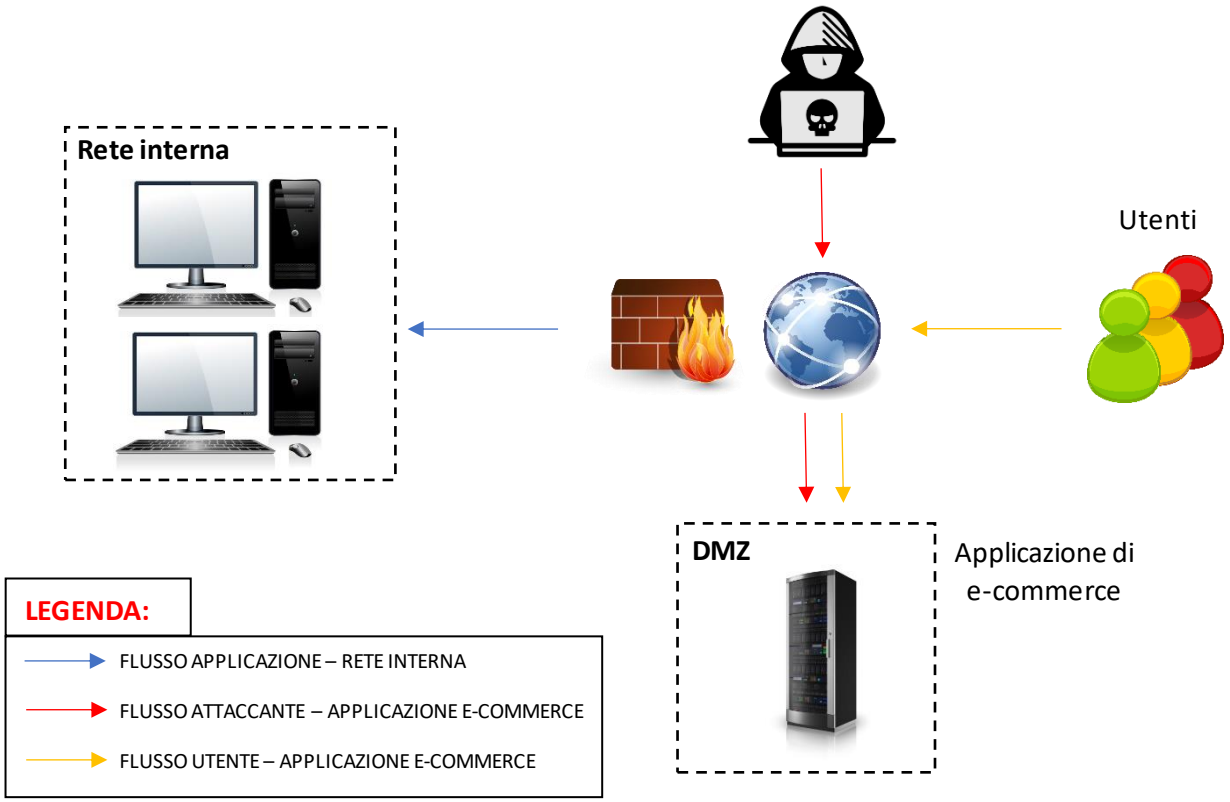
2. IMPATTI SUL BUSINESS

Supponendo di avere una situazione in cui un azienda subisce un attacco **DDos** all'applicazione WEB proviamo a calcolare le perdite che l'azienda può avere. Ipotizzando che l'applicazione a causa del **DDos** non sia raggiungibile per 10 minuti e che ogni minuto gli utenti spendono circa 1.500€, allora le perdite subite dall'azienda sono rispettivamente:

Perdite economiche = 10 (minuti) x 1.500€ (spese degli utenti per un minuto) = 15.000€ ogni 10 minuti

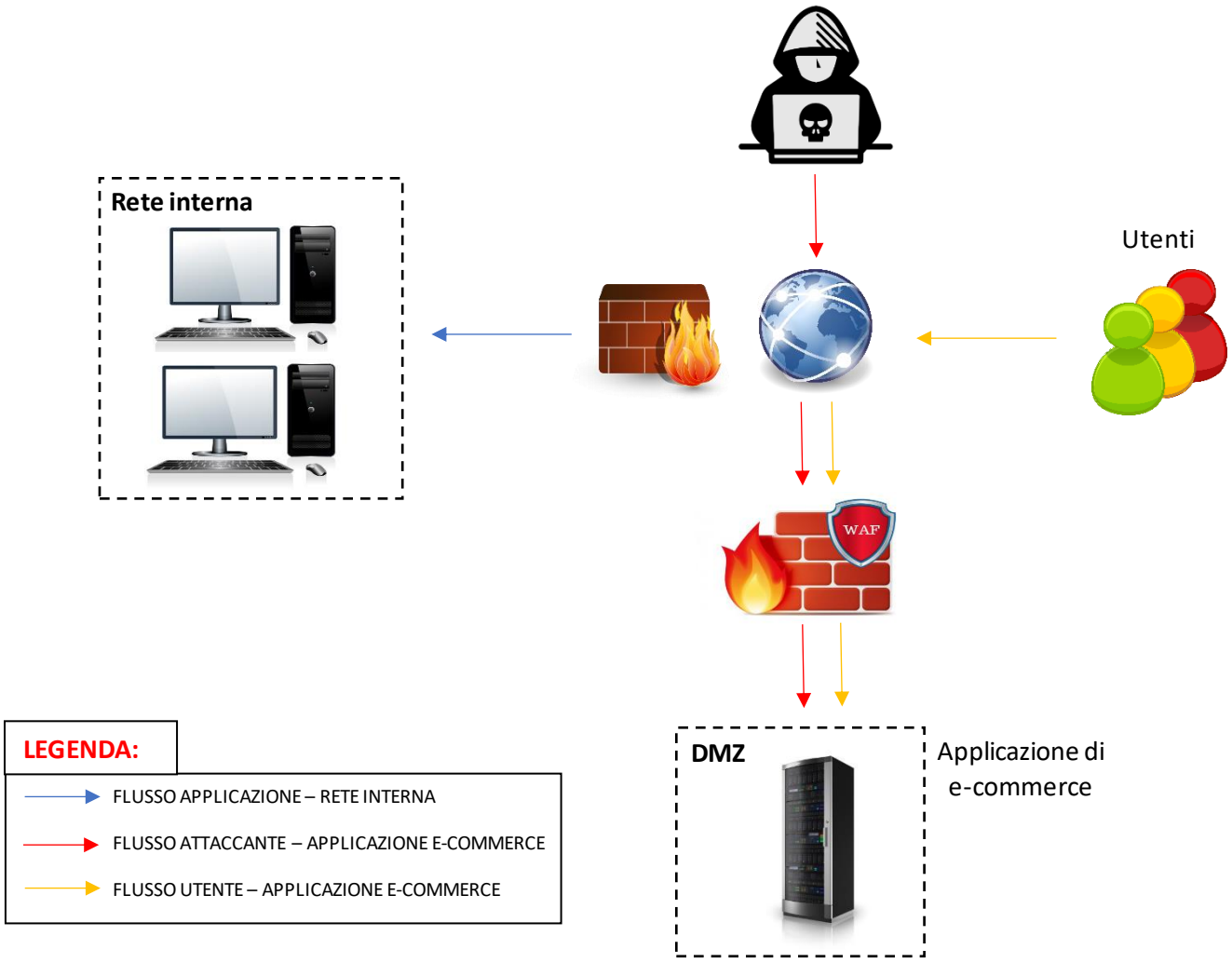
3. RESPONSE

Supponiamo ora che l'applicazione Web venga infettata da un **malware**. La nostra azione sarà quella di evitare che il **malware** infetti anche la rete interna della nostra azienda, per farlo andremo ad operare con un sistema di **isolamento** della nostra applicazione Web portandola al di fuori del Firewall e resa attiva solo agli utenti esterni per i loro acquisti. Questo permetterà all'azienda la sicurezza di non essere infettata ma anche di compiere azioni (possibilmente nel più breve tempo possibile) nella rimozione del Malware. La soluzione dunque è rappresentata nell'immagine di seguito:



4. **SOLUZIONE COMPLETA**

In tal caso invece andremo ad analizzare una situazione di procedure di sicurezza nel caso in cui un attaccante infetti la nostra applicazione Web con un **malware** e che attui anche attacchi del tipo **XSS** o **SQLi**. La soluzione, dunque, non sarà altro che unire le due immagini precedenti nel caso 1. e nel caso 3. La soluzione pertanto è la seguente:



5. MODIFICA PIU' AGGRESSIVA

Supponiamo ora di voler apportare modifiche alla nostra struttura di rete in modo tale da evitare qualsiasi tipo di attacco futuro. Come abbiamo visto precedentemente si sono analizzati due casi di attacco, dal quale abbiamo implementato un WAF e un Isolamento. Facciamo delle ipotesi: supponiamo che la nostra azienda sia un azienda di e-commerce importante (es. Amazon); trovarsi nella condizione di dover lasciare chiuso il sito per manutenzioni dovute all'attacco di un malintenzionato, provocherebbe enormi perdite economiche e finanziarie per essa. Pertanto una soluzione potrebbe essere quella di inserire un IPS/IDS i quali altro non sono che delle misure di sicurezza come sistemi di rilevamento delle intrusioni (IDS) e di prevenzione delle intrusioni (IPS). Tali misure di sicurezza permettono appunto il monitoraggio del traffico di rete e l'analisi dei segnali di possibili intrusioni. Quest'ultima è il processo che consiste nel rilevare le intrusioni e quindi di interrompere gli incidenti rilevati, in genere scartando i pacchetti o terminando le sessioni.

Come altra soluzione potremmo aggiungere un nodo all'applicazione Web. Questo concetto è chiamato **Ridondanza** il quale, in caso di server, trova applicazione pratica nel **<<failover cluser>>**. Quest'ultimo include due o più server e permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quindi, quando il server attivo smette di funzionare, il secondo server (nodo) prende il suo posto come server attivo tramite il suo processo che è chiamato appunto **<<failover>>**.

La soluzione finale dunque è la seguente: