Settimana 9 Lezione 5

Analisi dei Log

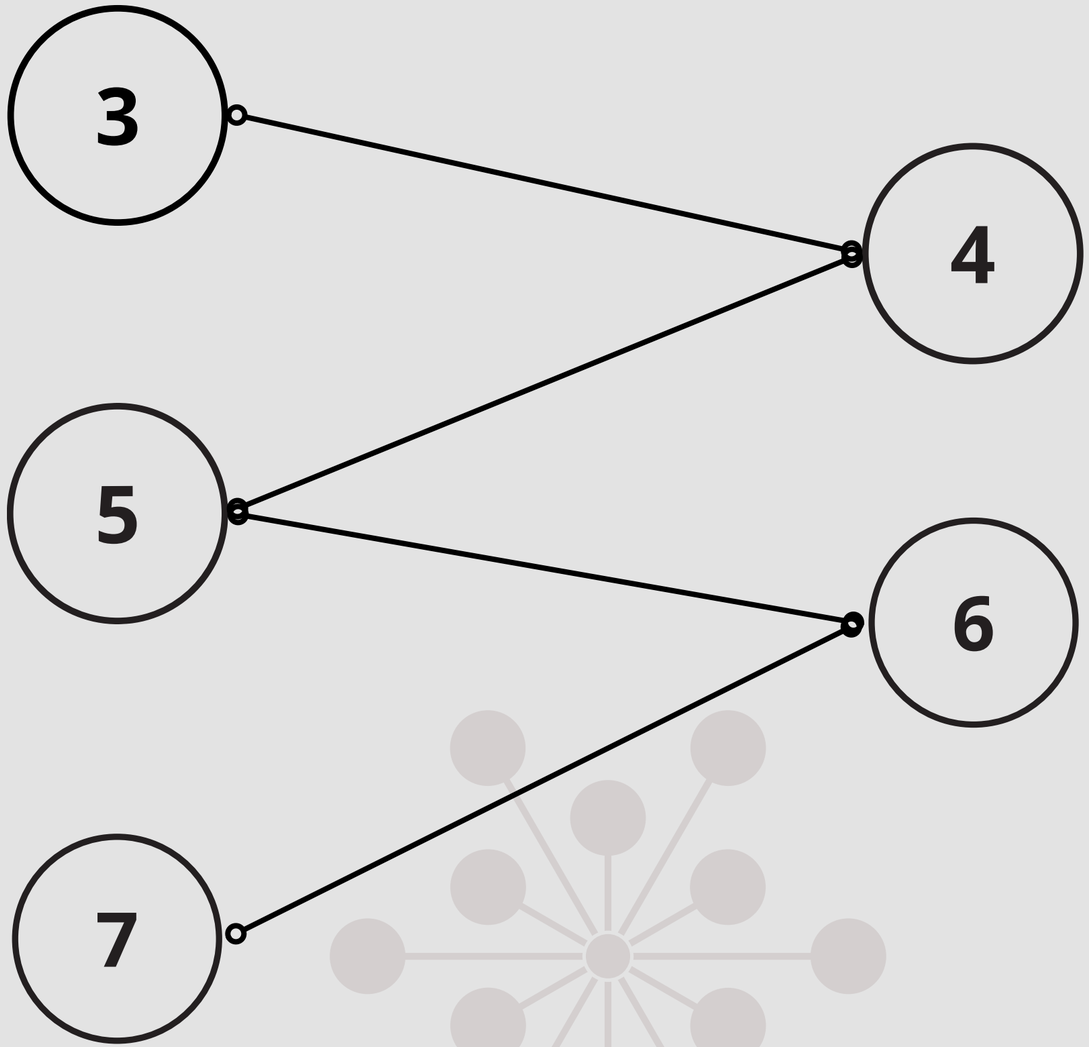
@epicode

Indice

Traccia

Azioni Preventive

Response



Architettura di rete

Impatto sul Buisness

Traccia

Con riferimento alla figura in slide 3, rispondere ai seguenti quesiti.

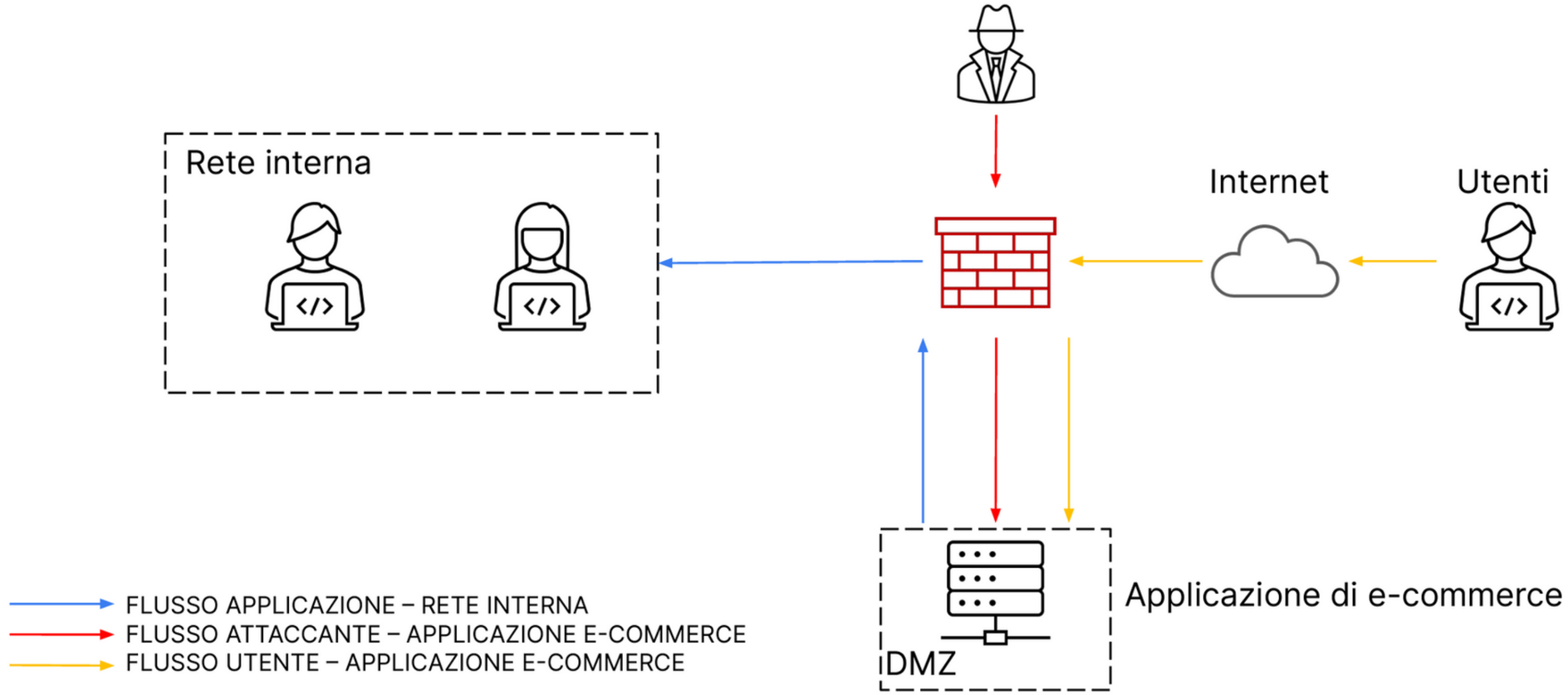
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

1. **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.

1. **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.

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.



Azioni Preventive

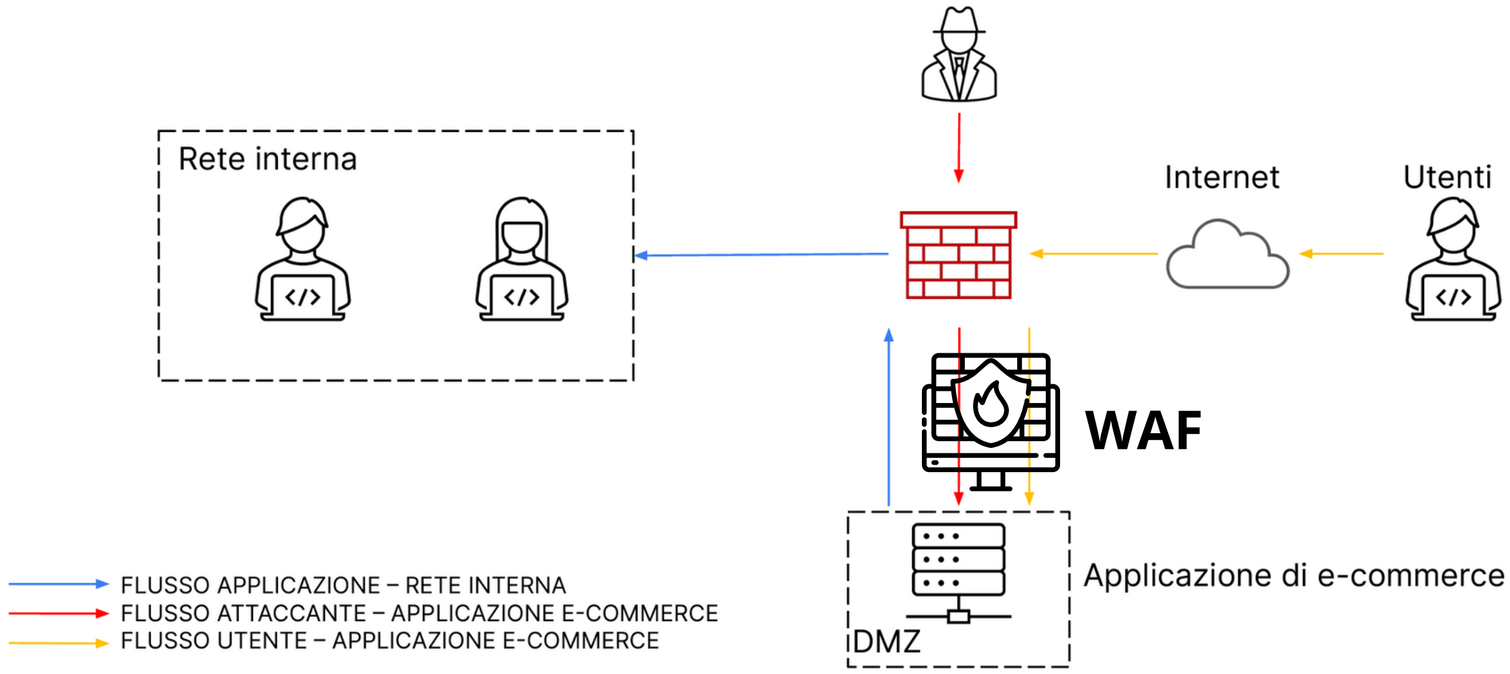
Per difendersi da attacchi di tipo XSS e SQLi oltre ad implementare la sicurezza della rete con un Web Application Firewall, come mostrato in figura.

Ricordiamo che un WAF è un firewall che difende le applicazioni web tramite configurazioni specifiche;
oltre ad evitare l'inserimento di codice malevolo (attacchi SQLi e XSS, come nel nostro caso), permette di evitare il traffico da parte dei bot, riconosce e bloccare gli attacchi Dos .

Come mostrato in figura il WAF è stato impostato sul flusso dell'attaccante e dell'utente in quanto sarebbero i due vettori di attacco principali, cioè da dove potrebbe entrare l'attacco.

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.



Impatti sul Buisness

Ci viene riferito che attraverso un attacco DDos della durata di **10 minuti**, la compagnia, offrendo servizi di e-commerce, subisce una perdita in termini economici.
Sapendo che ogni **1 minuto** la Web App produce un introito di **1500 euro**, ci viene chiesto di calcolare il totale della perdita economica di questo attacco.

Il calcolo è abbastanza elementare:

perdita totale = 1500 x 10 = 15.000 €

Cioè se per ogni minuto si perdono 1500 €, moltiplicando per il totale dei minuti che dura l'attacco, otterremo l perdita totale dell'attacco.

Ora i dati forniti non sono comunque sufficienti per fare una stima realistica; in una situazione reale entrano in. gioco altri fattori come per esempio in quale fascia orari della giornata avviene l'attacco, quale è il mercato dell'e-commerce (per determinare in quale area geografica ha le maggiori vendite). Questi dati in più sarebbero fondamentali in quanto se il grosso delle vendite viene effettuato durante il giorno e l'e-commerce subisce l'attacco in piena notte, la stima della media sarebbe superficiale, e bisognerebbe andare ad utilizzare dati differenti.
Questo per dire che quando vengono fatte queste stime ci deve essere a monte un analisi dati estremamente accurata e non generica , al fine di investire nella prevenzione in modo logico e mirato.
L'utilizzo di medie non accurate ed estranea dal vero contesto potrebbero portare a **Buisness Impact Analisys** (**BIA**), errati e potenzialmente inutili.

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.

Per evitare che il malware si propaghi all’interno della rete interna e infetti altre parti dell’organizzazione la soluzione più efficace è quella dell’ **Isolamento**, in quanto ci viene richiesto di mantenere la Web App in funzione per i servizi client.
Se scegliessimo di **mettere in quarantene** non potremmo offrire i servizi di e-commerce ai clienti e avremmo anche una pesante perdita in termini economici. Tuttavia vogliamo sottolineare che lasciare i servizi di e-commerce attivi per gli utenti potrebbe portare la propagazione del malware sulle reti dei clienti.
Qui c’è da far un attenta valutazione se mettere offline il server fino all’effettiva risoluzione del problema. Cioè capire se la perdita economica subita nel periodo necessario alla risoluzione del problema (malware) sia sopportabile e non irrecuperabile da parte dell’azienda.

Comunque, ricordiamo che durante l’ **Isolamento** una squadra di tecnici devo comunque lavorare per risolvere il problema, per poter tornare il prima possibile ad uno stato di normalità.

Nella figura della slide seguente possiamo notare come sia stata cancellata la linea di comunicazione tra la Web App e la rete interna dell’azienda.

La connessione (freccia blue) è stata rimossa a significare che la Web App non è più raggiungibile dalla rete interna. In questo modo il malware non si può propagare sulla rete interna arrecando ulteriori danni. Tuttavia potrebbe propagarsi verso internet e verso gli utenti dell'e-commerce.