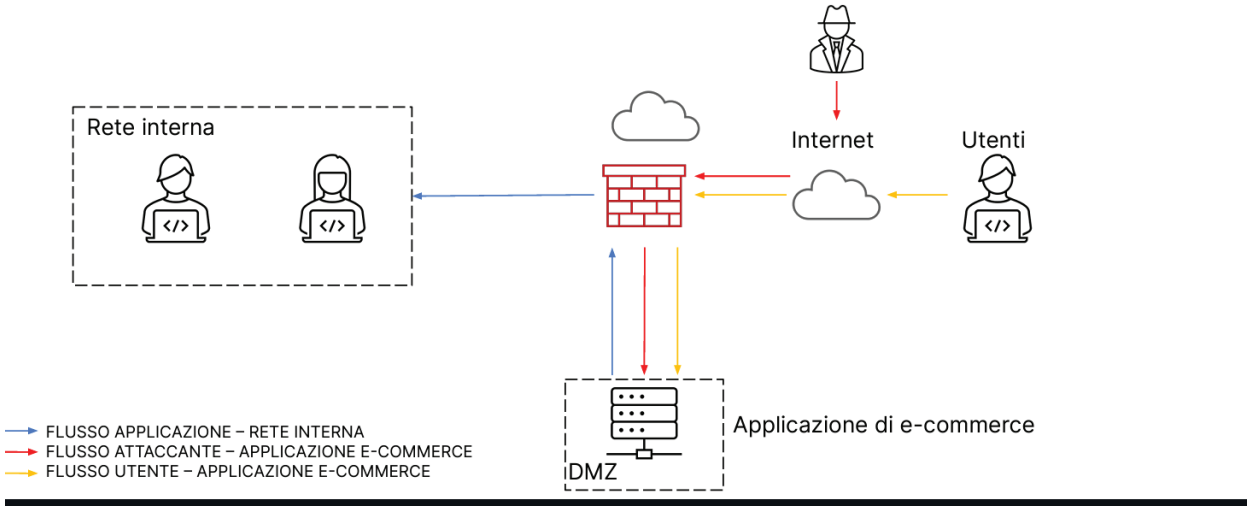
Report Splunk - W20D4

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.



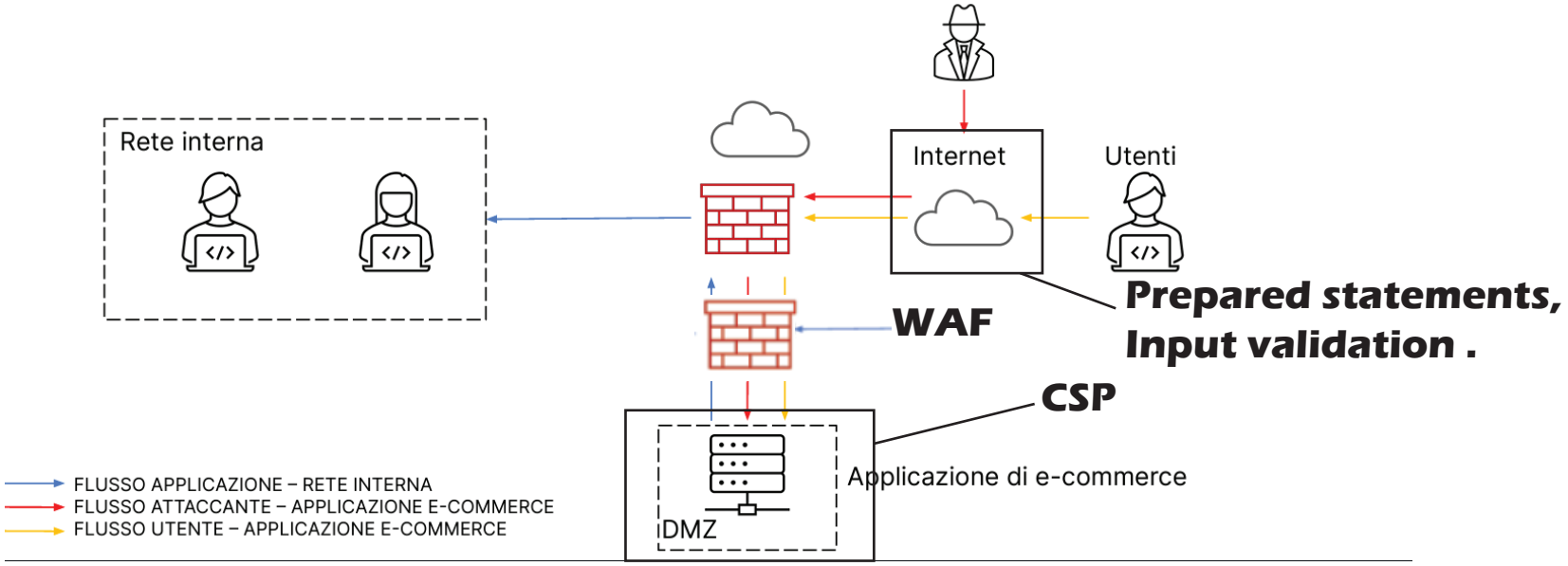
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni

Le azioni preventive che possiamo prendere sono :

1. **WAF (Web Application Firewall) è un firewall apposito per la protezione delle Web App che difende da questi tipi di attacchi .**
2. **La validazione degli input che riguarda tutte le informazioni legate agli input che l'user digita in caso di login o registrazione come "Username" , "Password" , "Password Confirmation" ecc.. Quindi definire un metodo apposito per verifiche complesse .**
3. **L'uso di prepared statements per le query SQL , sono modelli già pronti all'uso per le interrogazioni nei sistemi di database in SQL, che non contengono valori per i singoli parametri . Questi non possono essere manipolati e quindi sono molto sicuri, poiché i valori concreti vengono assegnati solamente all'interno del sistema.**

4. **CSP - (Content Security Policy) - Consente a gestori di siti web di definire una whitelist di fonti affidabili da cui il browser può caricare contenuti , include script , immagini e media . Offre protezione da attacchi XSS , clickjacking e l'inserimento di risorse esterne dannose .**

5. **Configurare il sito in modo che eventuali errori non vengano mostrati a user or potenziali attaccanti e non rivelino informazioni riguardante il sito o il codice che lo compone .**



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. **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**

- **L'impatto sul business viene calcolato moltiplicando il guadagno per minuto per il tempo totale in cui l'applicazione non è raggiungibile quindi : 1500 euro x 10 minuti = 15 000 euro . Per prevenire il problema è possibile :**

1. **Limitare il numero di richieste che un utente può fare in un determinato periodo di tempo .**
2. **Aumentare la capacità di banda e dei server in modo da poter resistere a possibili sovraccarichi**
3. **Monitoraggio della rete in tempo reale , utilizzo di DDoS Protection tools .**

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.

Se l'applicazione Web viene infettata da un malware dobbiamo effettuare i seguenti passaggi:

1. ***Isolamento della Macchina infettata : Isolare il server o la macchina affetti da malware per evitare la diffusione del virus , possiamo fare questo bloccando il traffico o scollegando la macchina dalla connessione direttamente .***
2. ***Analisi del Malware a livello Statico e/o Dinamico con controllo dei log per capire come il malware abbia infettato la nostra macchina . E capire se eventuali dati sono stati compromessi .***
3. ***Dopo aver capito come siamo stati attaccati , cerchiamo di impedire che l'attacco si ripeta rafforzando le nostre difese e mettendo in sicurezza gli altri server .***
4. ***Infine mettere in sicurezza la macchina infetta dove possibile altrimenti effettuare un factory reset con rafforzamento delle difese .***
5. ***Effettuare Real Time monitoring per vedere se le misure di sicurezza prese sono adeguate .***