



FLORES ALEX

EPICODE S9

INDICE

Introduzione al progetto

Architettura di rete

Azioni preventive

Impatti sul business

Response

Conclusioni finali

INTRODUZIONE AL PROGETTO

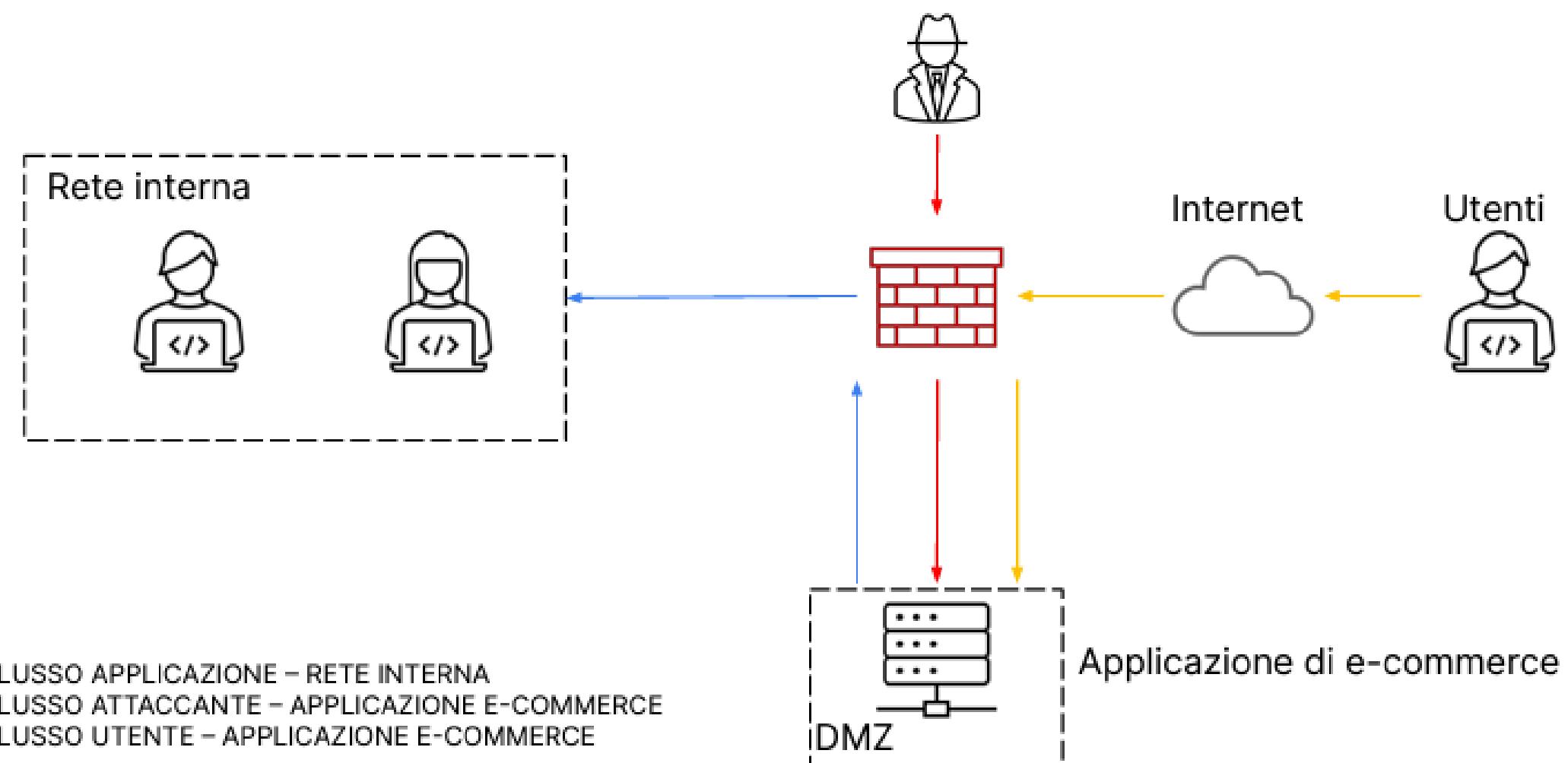
Questo progetto si concentra sull'analisi e sul miglioramento della sicurezza di un'applicazione Web, con particolare attenzione agli attacchi di tipo SQLi (Structured Query Language Injection) e XSS (Cross-Site Scripting), nonché sulla gestione degli impatti aziendali derivanti da attacchi DDoS (Distributed Denial of Service) e infezioni da malware.

Attraverso l'analisi e la proposizione di soluzioni specifiche, il progetto mira a migliorare la sicurezza dell'applicazione Web e a mitigare gli impatti negativi sul business derivanti da potenziali attacchi e infezioni da malware.

ARCHITETTURA DI RETE

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 (una zona di rete intermedia tra una rete interna sicura e una rete esterna non fidata, come ad esempio Internet. La sua funzione principale è quella di fornire uno strato aggiuntivo di sicurezza separando i servizi pubblici accessibili dall'esterno (come server Web, server di posta elettronica, ecc.) dalla rete interna contenente risorse sensibili come server di database, file aziendali, ecc.) per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE

AZIONI PREVENTIVE

Il progetto richiede allo studente quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato, modificando quindi l'architettura di rete in modo da evidenziare le implementazioni

AZIONI PREVENTIVE

Per la protezione della Web App da minacce quali XSS e SQLi si può preventivamente adottare una soluzione basata su Web Application Firewall, che a differenza dei firewall standard, sono dedicati per proteggere le Web App da attacchi XSS e SQLi. La figura iniziale si modifica di conseguenza come la figura in slide 2, dove abbiamo ipotizzato che il WAF sia a protezione del traffico in entrata sulla Web App da internet (quindi utenti e attaccante).

AZIONI PREVENTIVE

SQLI , XSS & FIREWALL

SQLI

Un **SQL Injection** (SQLi) è un tipo di attacco informatico che sfrutta le vulnerabilità presenti nelle applicazioni Web per manipolare le istruzioni SQL inviate al database. In sostanza, un SQLi consente a un attaccante di inserire o "iniettare" codice SQL dannoso attraverso i campi di input delle applicazioni Web, come moduli di login o campi di ricerca. Quando il server Web processa queste informazioni, il codice SQL dannoso viene eseguito dal database, consentendo all'attaccante di ottenere accesso non autorizzato ai dati del database, modificarli o persino eliminare informazioni sensibili.

XSS

Cross-Site Scripting (XSS) è un tipo di attacco informatico che sfrutta le vulnerabilità presenti nelle pagine web per inserire script dannosi all'interno del codice HTML o JavaScript visualizzato dai browser degli utenti. In pratica, un attacco XSS consente a un aggressore di iniettare codice malevolo, come script JavaScript, all'interno delle pagine web visitate da altri utenti. Questo codice può essere utilizzato per rubare informazioni sensibili, come cookie di sessione o dati personali degli utenti, redirezionare gli utenti verso siti di phishing o malware, o manipolare il contenuto della pagina web visualizzato.

FIREWALL

Un **firewall** è un dispositivo o un'applicazione software progettata per monitorare e controllare il traffico di rete, sia in entrata che in uscita, tra una rete privata e una rete esterna, come Internet. Il suo obiettivo principale è quello di proteggere una rete informatica da accessi non autorizzati o da potenziali minacce provenienti dall'esterno, filtrando il traffico in base a regole di sicurezza predefinite. In pratica, un firewall può bloccare o consentire il passaggio del traffico di rete in base a criteri come l'indirizzo IP di origine o di destinazione, il tipo di protocollo utilizzato (ad esempio TCP, UDP), la porta di destinazione etc.

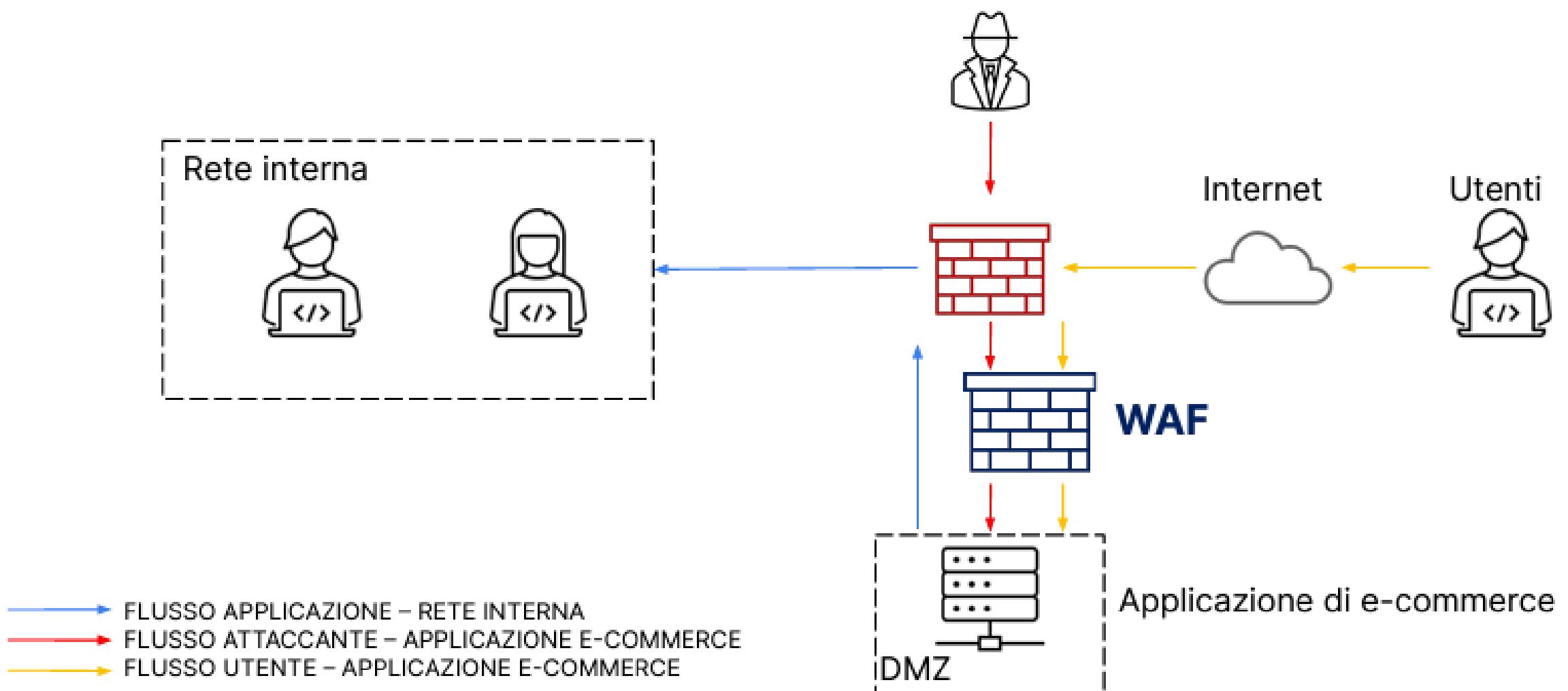
AZIONI PREVENTIVE

Nel contesto dell'e-commerce, l'applicazione deve essere accessibile agli utenti via Internet per consentire loro di effettuare acquisti sulla piattaforma. Tuttavia, affinché gli utenti possano raggiungere l'applicazione, essa viene posizionata all'interno di una DMZ, una zona di rete intermedia tra la rete interna protetta e Internet.

Questa disposizione consente agli utenti esterni di interagire con l'applicazione senza accedere direttamente alla rete interna dell'azienda.

Tuttavia, se il server all'interno della DMZ venisse compromesso, potrebbe rappresentare un punto di ingresso per gli attaccanti per accedere alla rete interna, poiché le politiche di firewall consentono la comunicazione tra la DMZ e la rete interna.

In sostanza, mentre la DMZ protegge la rete interna dagli attacchi diretti da Internet, è importante implementare misure di sicurezza aggiuntive per garantire che eventuali compromissioni nella DMZ non possano essere sfruttate per accedere alla rete interna, proteggendo così i dati sensibili e le risorse aziendali.



IMPATTI SUL BUSINESS

IMPATTI SUL BUSINESS

L'applicazione Web subisce un attacco di tipo Ddos (un tipo di attacco informatico in cui un grande numero di dispositivi collegati a Internet invia numerose richieste di servizio ad un server, riuscendo a sovraccaricarlo)dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Lo studente quindi dovrà 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.

IMPATTO SUL BUSINESS

Durante l'attacco DDoS, la piattaforma di e-commerce è stata resa inaccessibile per un periodo di 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo calcolare il danno finanziario derivante dall'indisponibilità del servizio moltiplicando la spesa media degli utenti per il numero di minuti di interruzione.

Quindi:

$$\text{Impatto sul business} = 1.500\text{€} \times 10 \text{ minuti} = 15.000\text{€}.$$

In altre parole, durante i 10 minuti di indisponibilità, l'azienda ha perso potenzialmente 15.000€ di entrate.

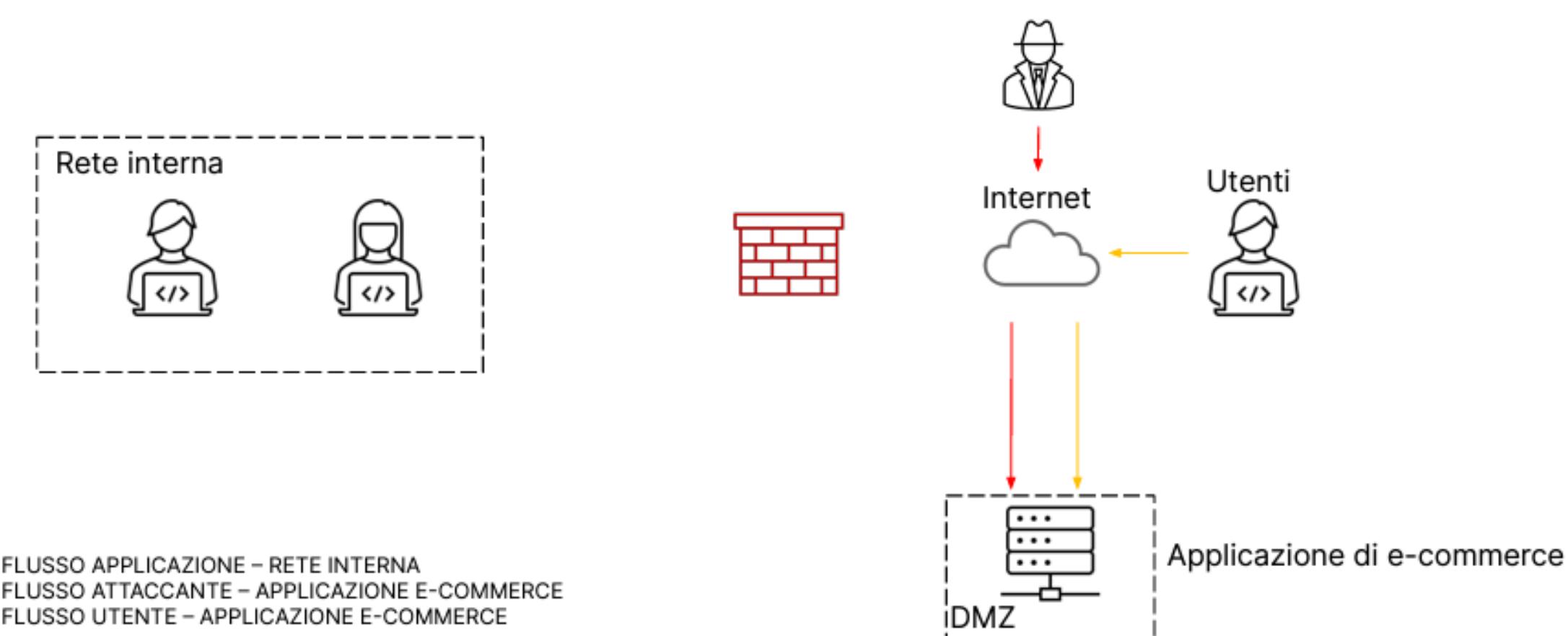


RESPONSE

L'applicazione Web viene infettata da un malware. La priorità dello studente è che il malware non si propaghi sulla rete, mentre non è interessato a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modifichiamo quindi l'architettura di rete con annessa una soluzione.

RESPONSE

Dato l'obiettivo prioritario di impedire la propagazione del malware sulla rete interna, si può optare per una strategia di isolamento della macchina infettata. In questa configurazione, la macchina compromessa sarebbe direttamente connessa a Internet, rendendola accessibile all'attaccante ma isolata dalla rete interna dell'azienda. Nella figura successiva, si può osservare la soluzione implementata con questa strategia di isolamento della macchina infetta. È evidente come, in questa nuova configurazione, non ci sia più alcuna comunicazione tra l'applicazione Web e la rete interna, riducendo così il rischio di diffusione del malware all'interno dell'ambiente aziendale. 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.



CONCLUSIONI FINALI

CONCLUSIONI FINALI

Le considerazioni finali sull'esercizio sono estremamente positive, in quanto sono state affrontate in modo completo e efficace tutte le task proposte. Le azioni preventive per difendere l'applicazione Web da attacchi di tipo SQLi e XSS sono state identificate e implementate, evidenziando un'approfondita comprensione delle vulnerabilità e delle contromisure necessarie per mitigare.

Inoltre, l'analisi dell'impatto sul business derivante dall'attacco DDoS ha dimostrato una valutazione accurata dei danni finanziari causati dall'indisponibilità del servizio, mostrando una consapevolezza dell'importanza di valutare gli effetti economici degli attacchi informatici sulle attività aziendali.

Infine, la risposta efficace all'infezione da malware, focalizzata sull'isolamento della macchina infetta per prevenire la propagazione della minaccia, evidenzia una strategia di risposta pronta e mirata, focalizzata sulla protezione della rete interna senza compromettere la continuità dell'accesso dell'attaccante alla macchina infettata.