



UNA PROPOSTA DI

LY DUC TIN

PROGETTO
BUSINESS CONTINUITY
PLAN E DISASTER
RECOVERY

PROGETTO S9L5





INTRODUZIONE

Traccia:

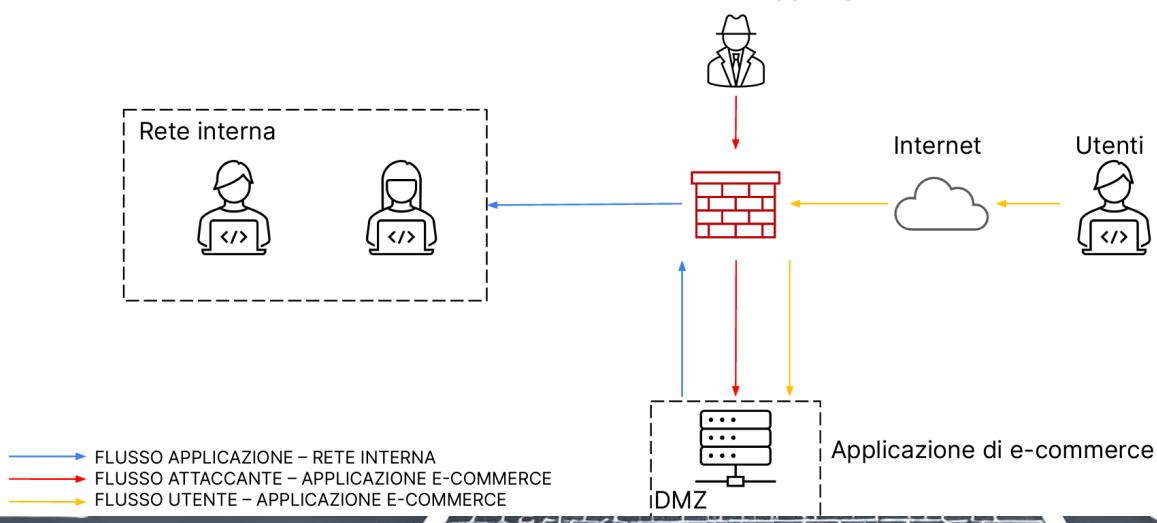
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

- 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
- 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.
- 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.





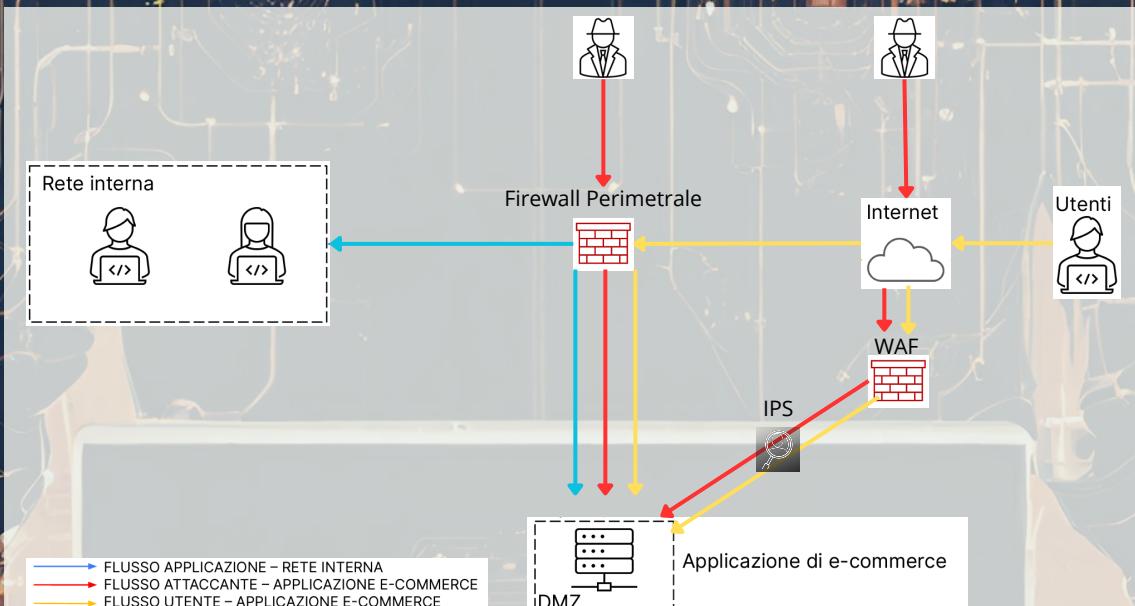
AZIONI PREVENTIVE

Prima di elencare le azioni che potremmo implementare per la difesa dell'applicazione Web da attacchi di tipo SQLi o XSS andiamo a spiegare questi attacchi:

SQLi (Structured Query Language injection) è uno dei tre macro categorie di attacchi che prevede di forzare l'immissione di codici di richiesta o di query nei sistemi di database questo permette all'attaccante di mettere del codice malevolo. Vi sono due tipi di SQLi: SQLi non blind SQLi blind La differenza è che il blind di base non mostra nessun risultato all'output invece il non blind di base si.

XSS injection (Cross Site Scripting) è una delle tre macro categorie di attacchi a sua volta è suddiviso in altre due: reflected e stored. Il reflected (riflesso) è uno script malevolo che non appena scrivo lo script lo esegue, mi esce subito come l'output. XSS stored (permanente) è uno script che permette di iniettare dei malware semplicemente passandoci sopra con il puntatore del mouse o cliccandoci con il dito. Rispetto al reflected, lo stored rimane fino a quando un programmatore non lo toglie.

DIMOSTRAZIONE DELLE MODIFICHE APPLICATE



Azioni preventive:

-Risanare il programma;

-Aggiornare l'applicazione;

-Monitorare costantemente l'applicazione web per individuare eventuali attacchi (IPS);

-Formare il personale sulla sicurezza delle applicazioni web e sui rischi associati alle vulnerabilità XSS e SQL;

-Utilizzo del firewall (WAF);

-Eseguire dei backup regolari;

-Eseguire dei pentesting regolari;





IMPATTO SUL BUSINESS

Data dalla consegna ci chiede di calcolare l'impatto sul business che ha l'attacco DDOS sull'applicazione Web. Sapendo che l'applicazione Web non è raggiungibile per 10 minuti e che i clienti in 1 minuto spendono 1500 euro allora potremmo fare il calcolo che è:

perdite totali=1.500€ x 10 = 15.000€

Attacco DDOS è una degli attacchi più frequenti insieme al MITM, ingegneria sociale, brute force/al dizionario e SQLi/XSS che prevede la negazione di un servizio il sovraccaricando la cpu. Rispetto all'attacco DOS vi sono più dispositivi coinvolti nell'attacco cioè l'attaccante controlla 10k o 20k dispositivi già infettati (botnet) per effettuare l'attacco invece nel DOS solo uno.

Soluzioni per contrastare DDOS:

- Utilizzare un firewall(WAF) può aiutare a rilevare e mitigare gli attacchi DDoS in tempo reale(es. bloccare l' indirizzo IP);
- Implementare un Content Delivery Network (CDN) per distribuire il carico di traffico e mitigare attacchi DDOS;
 - i captcha,rallentano gli attacchi DOS-DDOS;
 - Implementazione di una rete elastica o scalabile ;
 - Affittare un server web;
 - DNS syncall ;
- C2 (Command and control).



RESPONSE

In questo caso l'applicazione Web è stata infettata da un malware e come soluzione l'esercizio chiede di isolarlo dalla rete interna così da non infettare gli altri dispositivi dell'azienda ma questo permette agli utenti e all'attaccante di accedere all'applicazione Web infettato facendo sì che ancora loro vengono infettati in questo modo si pensa che questa soluzione sia più conveniente economicamente per l'azienda.

DIMOSTRAZIONE DI ISOLAMENTO

