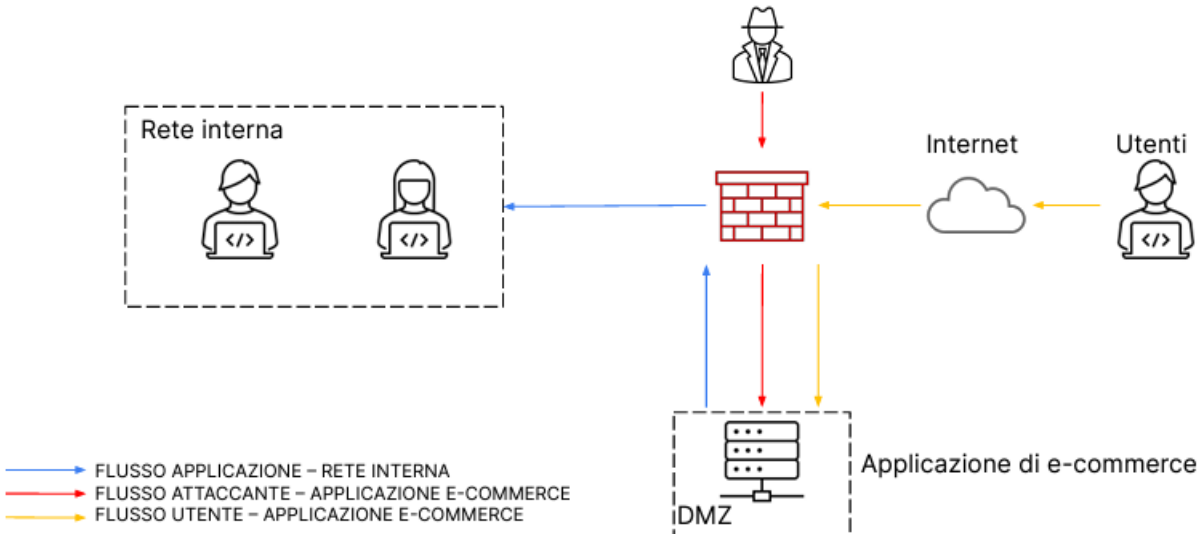
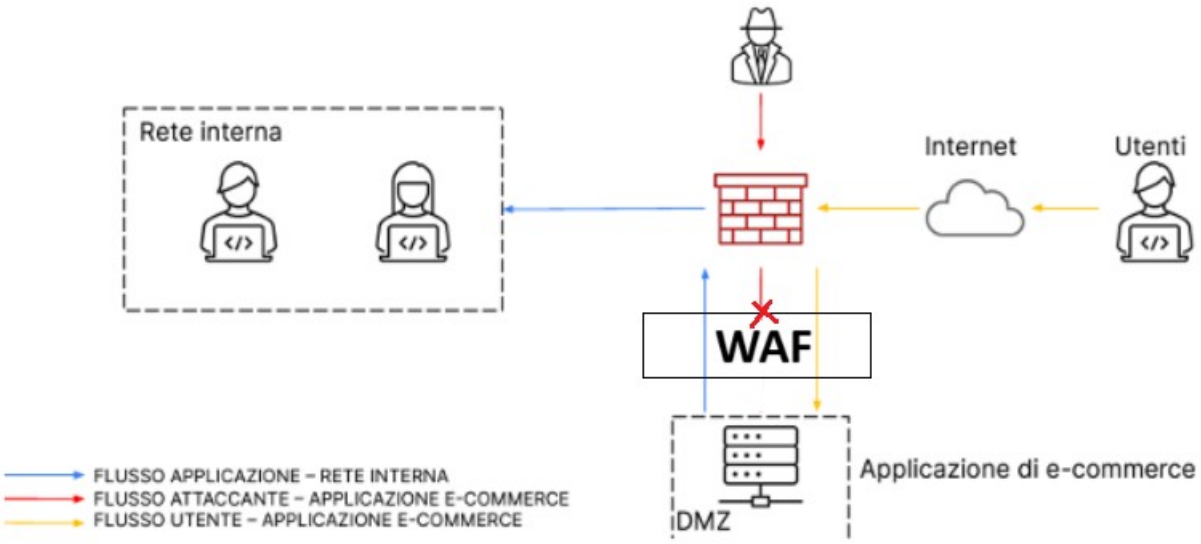
Azioni preventive, calcolo del danno e incident response

Con riferimento alla figura, 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.



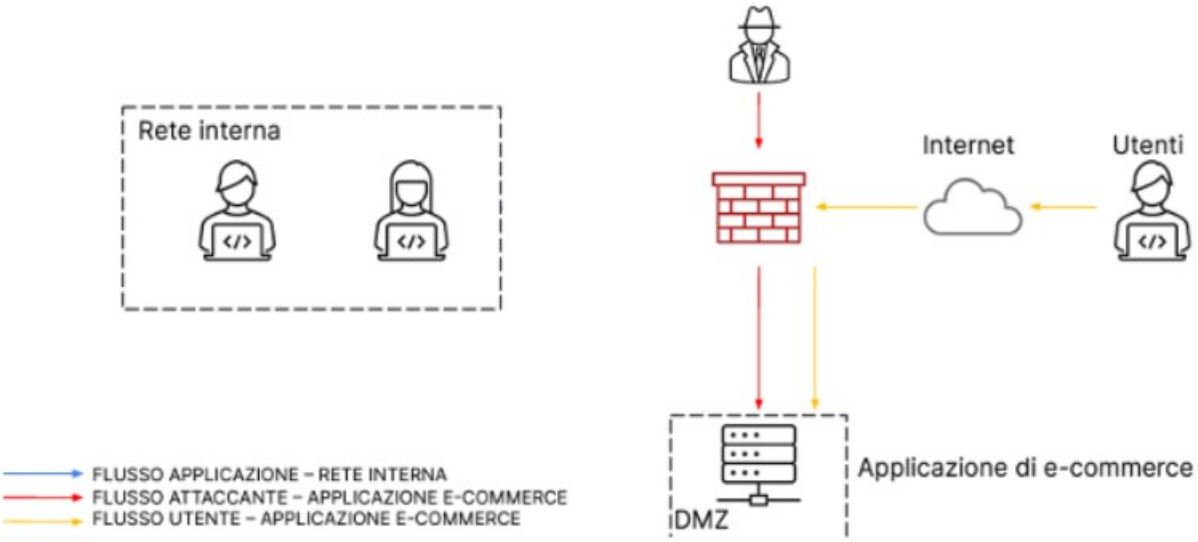
1. Nella prima situazione dobbiamo adottare misure preventive per prevenire attacchi SQL Injection o XSS alla web app. La prima cosa da fare è implementare un WAF (Web Application Firewall) a difesa della DMZ. Il WAF è un tipo di firewall che adotta un approccio diverso nel filtraggio dei pacchetti in entrata rispetto agli stateful firewall perimetrali; va a controllare i contenuti di ogni pacchetto e li confronta con tabelle (presenti all'interno del WAF o fornite da aziende specializzate) che riportano le firme dei malware noti, di modo che se il WAF trova un riscontro, il pacchetto con contenuto malevolo sarà bloccato. Per essere efficace, ovviamente le tablle a cui il WAF si riferisce devono essere il più aggiornate possibili.



Gli attacchi SQLi e XSS sfruttano vulnerabilità presenti nelle web app che permettono agli utenti di inserire input. Se l'input utente non è filtrato a dovere, si incorre nel rischio che si possa caricare del codice malevolo attraverso i punti di injection; sarebbe bene quindi assicurarsi a livello di programmazione che la web app non accetti questo tipo di input, andando a sanitizzare il codice.

2. Nella seconda situazione dobbiamo calcolare l'impatto economico di un attacco DdoS che rende inagibile la web app per 10 minuti. Considerando che la piattafroma genera un introito medio di 1.500 euro al minuto, eseguiamo una semplice moltiplicazione per ottenere la perdita su 10 minuti: 1.500 * 10 = 15.000 euro.
   Un attacco DdoS è un tipo di attacco portato avanti da un team di black hat (solitamente tramite una botnet) che mira a saturare le risorse della CPU di un dispositivo per provocarne latenza o addirittura il crash del sistema. Per mitigarne gli effetti si suggerisce di adottare misure preventive come settare un limite di connessioni al server e se possibile ricorrere alla distribuzione del carico di traffico tramite l'utilizzo di più server (se sostenibile economicamente).

3. Nell'ultima situazione dobbiamo adottare un incident response a valle di un attacco malware alla web app, facendo in modo che il malware non si propaghi nella rete interna dell'azienda.
   Dal momento che l'azienda non è momentaneamente interessata a rimuovere l'accesso al server web da parte dell'attaccante, la prima misura da adottare è la rimozione della rete interna dalla WAN. In questo modo il server web, benché sotto attacco, continuerà a funzionare, mentre si lavora per rimuovere il malware (sacrificando però la sicurezza informatica dei clienti presenti sulla web app) e anche in rete interna si potranno svolgere compiti che non necessitano di accesso ad Internet, minimizzando i danni per l'azienda.


Rete interna
Internet
Utenti
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE
DMZ
Applicazione di e-commerce