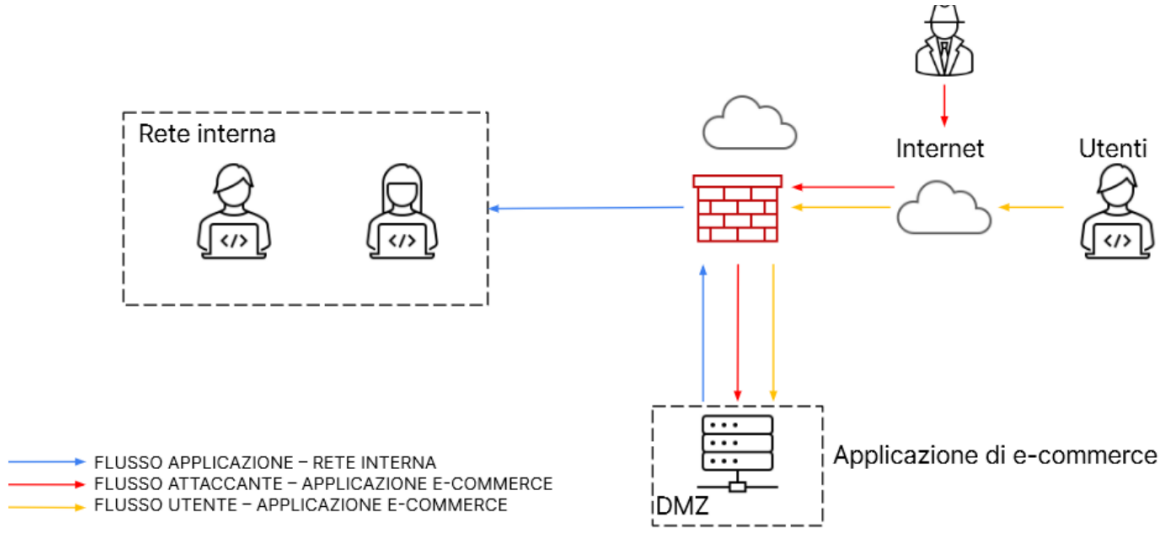
Progetto "Modulo 05"

Angelo Marino

Indice

1.Azione di prevenzione : Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLj oppure XSS da parte di un utente malintenzionato ?



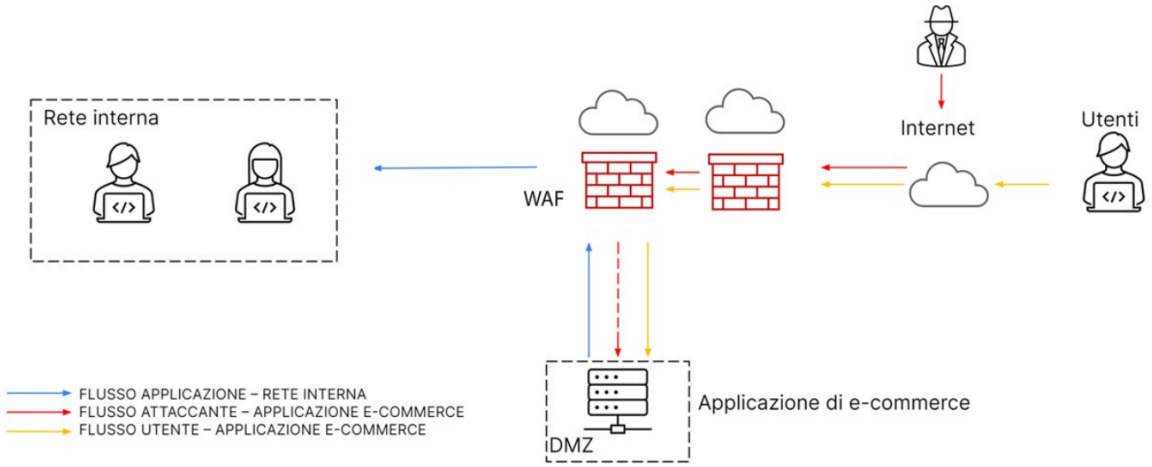
Per far fronte alle minacce elencate nella traccia (SQL ; XSS) bisognerebbe integrare un WAF .

WAF è l'acronimo di " Web Application Firewall " Si tratta di un tipo di sistema di sicurezza progettato per la protezione delle applicazioni web da una serie di minacce .

una WAF funziona come una barriera tra richiesta web e l'applicazione web stessa. Il suo obiettivo principe è il filtrare, monitorale,bloccare il traffico web in base a regole inserite dall'operatore.

Altre tecniche per poter mitigare questi attacchi possono ricadere su un "ORM"

ORM acronimo di " Object-Relational Mapping " utilizzato per gestire l'interazione con il database, essi generano automaticamente query parametrizzate.


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

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 1500 euro sulla piattaforma e-commerce. Fare Eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Supponiamo che in media gli utenti spendano 1500 euro al minuto sulla tua piattaforma di e-commerce.

Se il servizio è irraggiungibile per un certo periodo, ad esempio 10 minuti, l'impatto finanziario potrebbe essere calcolato come segue:

Impatto finanziario = (Valore medio di spesa al minuto) x (Minuti di non raggiungibilità)

Impatto finanziario = 1500 euro/minuto x 10 minuti = 15.000 euro

Quindi, in questo esempio, l'irraggiungibilità del servizio per 10 minuti avrebbe un impatto finanziario di 15.000 euro.

Per poter mitigare questa problematica possiamo implementare alcune azioni del tipo :

- Backup dei dati
- Pianificazione di emergenza
- Test di carico
- Cloud-based DDos protection

* Un attacco DDoS, acronimo di Distributed Denial of Service, è un tipo di attacco informatico in cui un gruppo di dispositivi o computer compromessi, noti come "botnet" (che sta per "rete di robot"), viene utilizzato per sovraccaricare un server, un sito web o un'applicazione online con una

quantità massiccia di traffico, rendendoli inaccessibili agli utenti legittimi.

L'obiettivo principale di un attacco DDoS è quello di causare una "denial of service", ovvero impedire o rallentare in modo significativo il normale funzionamento di un servizio online.*

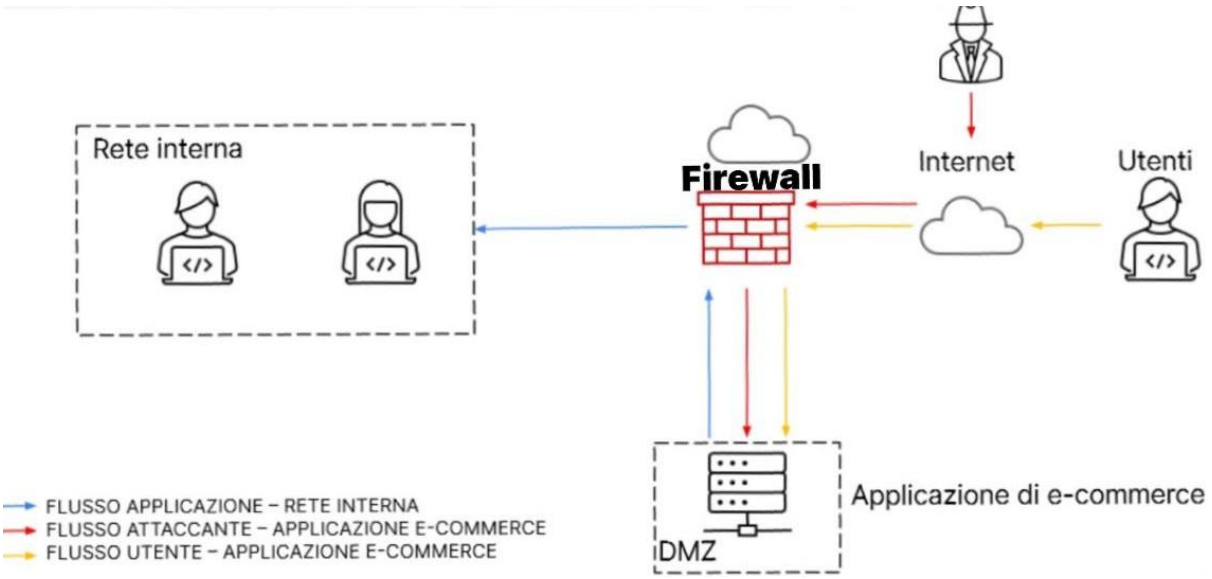
3. Response: L’applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infetta. Modificate la figura in slide 2 con la soluzione proposta.

Alcune delle misure che si potrebbero adottare per la mitigazione di un malware sono le seguenti:

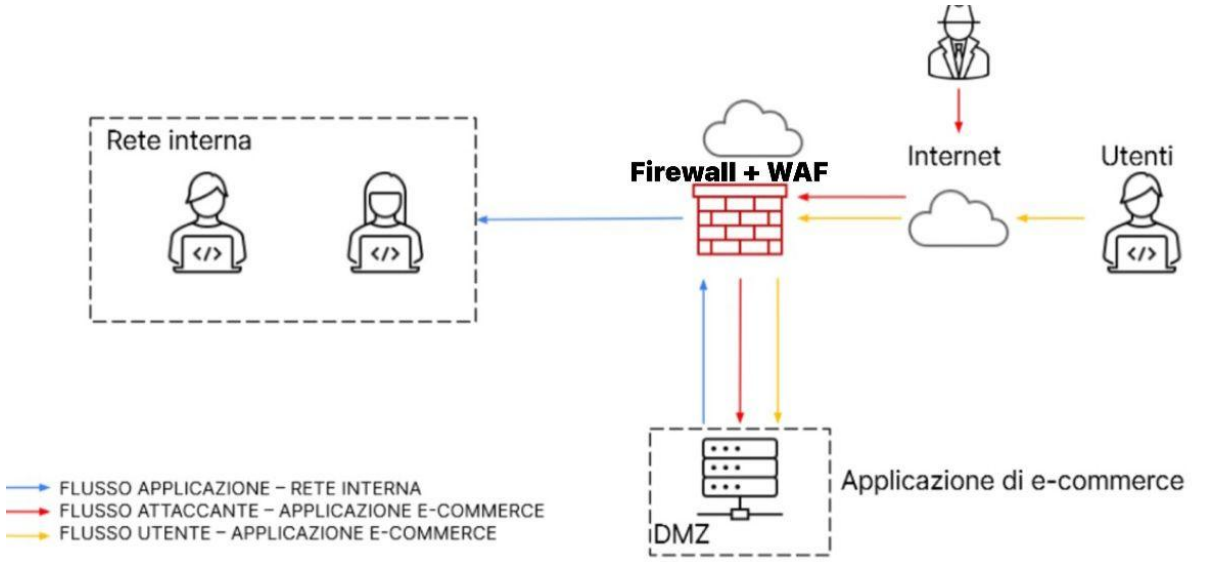
- Isolamento della macchina infetta per via fisica o virtuale, in modo che il malware non possa comunicare con altri dispositivi nella rete. Ciò impedirà la propagazione del malware stesso.

- Implementazione di firewall configurandolo con regole per limitare il traffico in entrata e in uscita dalla macchina infetta, in modo che solo il traffico necessario sia consentito.

- Backup e ripristino in modo che, se necessario, tu possa ripristinare il sistema a uno stato precedente e pulito.



4.Soluzione completa : unire i disegni dell’azione preventiva e della response (unire soluzione 1 e 3)



5. Modifica <più aggressiva> dell’infrastruttura (se neccessario/facoltativo magari integrando la soluzione del punto 2)

Per proteggere la frattura si intraprende un’azione piu aggressiva con l’inserimento di un IPS (come si può vedere nella figura sottostante)