

Prevenzione, impatto e risposta in caso di attacco reale

Progetto n°8
Francesco Fuschetto

Azioni Preventive

SQLi

Un attacco di tipo SQL injection è basato su un difetto in fase di programmazione che consiste nella mancata limitazione/filtrazione dell'input utente. Questo permette ad un utente mal intenzionato di poter inserire script malevolo per effettuare un attacco al database e riuscire ad ottenere informazioni e dati sensibili.

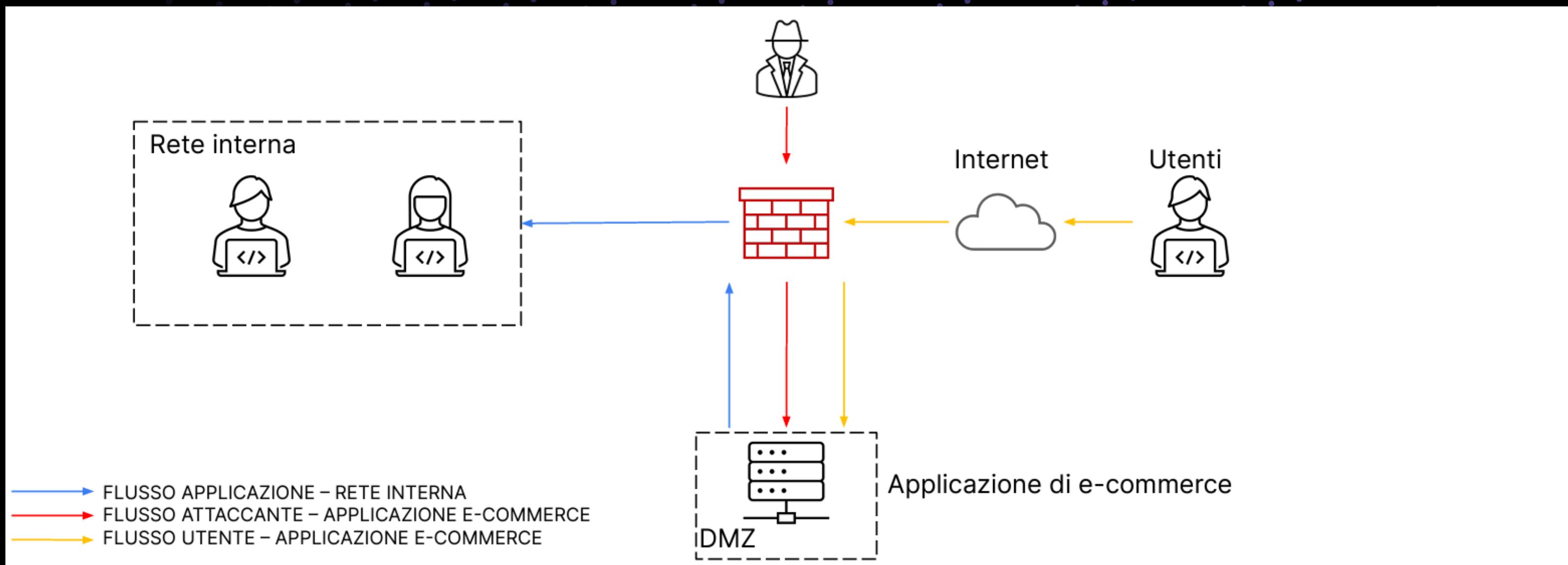
XSS

L'attacco XSS è anch'esso basato su un mancato controllo di input da parte dell'utente. Questa tipologia di attacchi si divide in: Stored e Reflected. Le differenze sono:

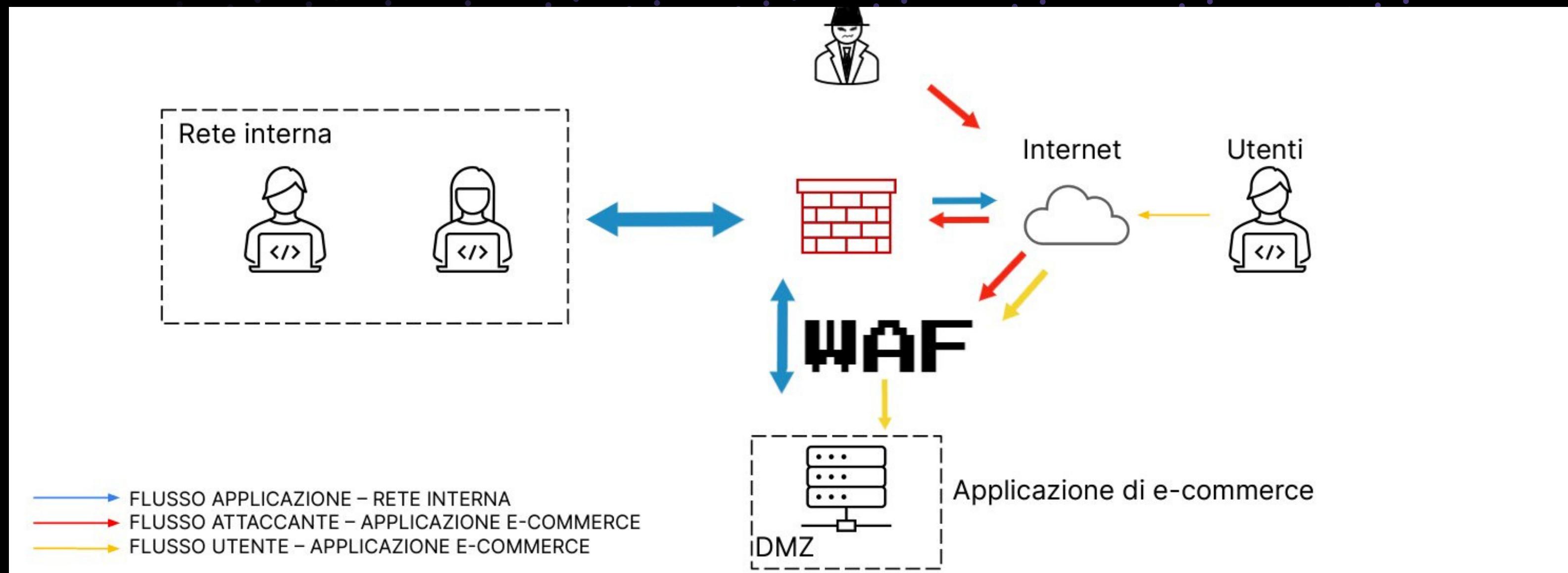
XSS stored attacca il server con l'inserimento di codice malevolo che di ‘aggancia’ alla pagina desiderata. Diventa quindi un attacco multi-target e molto difficile da individuare.

XSS reflected bersaglia un singolo utente con l'invio dello script malevolo. Esso viene solitamente inviato tramite Fishing o Smishing.

Situazione Iniziale



Situazione Finale



Considerazioni Finali

Per dare un senso alla prima immagine sono state modificate quasi tutte le connessioni descritte. Come premessa è stato aggiunto un WAF, il cui scopo è quello di andare a bloccare eventuali attacchi verso la DMZ, infatti tramite lo ‘spacchettamento’ e la lettura dei dati in ingresso è in grado di bloccare attacchi facendo confronti con tabelle di riferimento.

Per iniziare tutte le connessioni derivanti da utenti comuni sono state indirizzare direttamente verso WAF, risulta infatti controproducente il passaggio da un firewall in quanto le connessioni esterne hanno interesse all’accesso dei dati contenuti nella DMZ. Un potenziale attaccante dovrebbe quindi affrontare il WAF per poter attaccare la DMZ ed un Firewall (dinamico) per poter attaccare la rete interna, a quest’ultima è stata concessa la possibilità di una connessione internet per questioni di praticità.

Abbiamo così ottenuto una rete interna sicura e connessa con Internet, una DMZ sicura ed accessibile tramite WAF ma non soggetta al controllo Firewall.

Analisi dell'impatto sul Business

Traccia: 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.

Analisi

L'attacco DDoS (Distributed Denial of Service) consiste nell'invio di un'enorme quantità di richieste da parte di una Botnet verso una singola porta su un server. Il risultato di questo attacco è il crash del servizio e quindi come da nome una negazione del servizio. Le differenze tra un attacco DoS e DDoS sono la quantità di macchine attaccanti coinvolte, nel primo caso sarà un singolo dispositivo a sferrare l'attacco (la potenza di quest'ultimo sarà quindi limitata), nel secondo caso invece possono essere coinvolte anche 20000 macchine (virtuali e non) per sferrare l'attacco, che sarà quindi di potenza incredibilmente maggiore. Per cercare di tutelarsi è possibile creare una distribuzione del carico delle richieste su più server e un rate limiting per cercare di scaglionare le richieste in ingresso.

Per stimare il danno economico derivato dall'attacco è sufficiente eseguire la seguente operazione:

Guadagno WA al minuto = 1500€/min

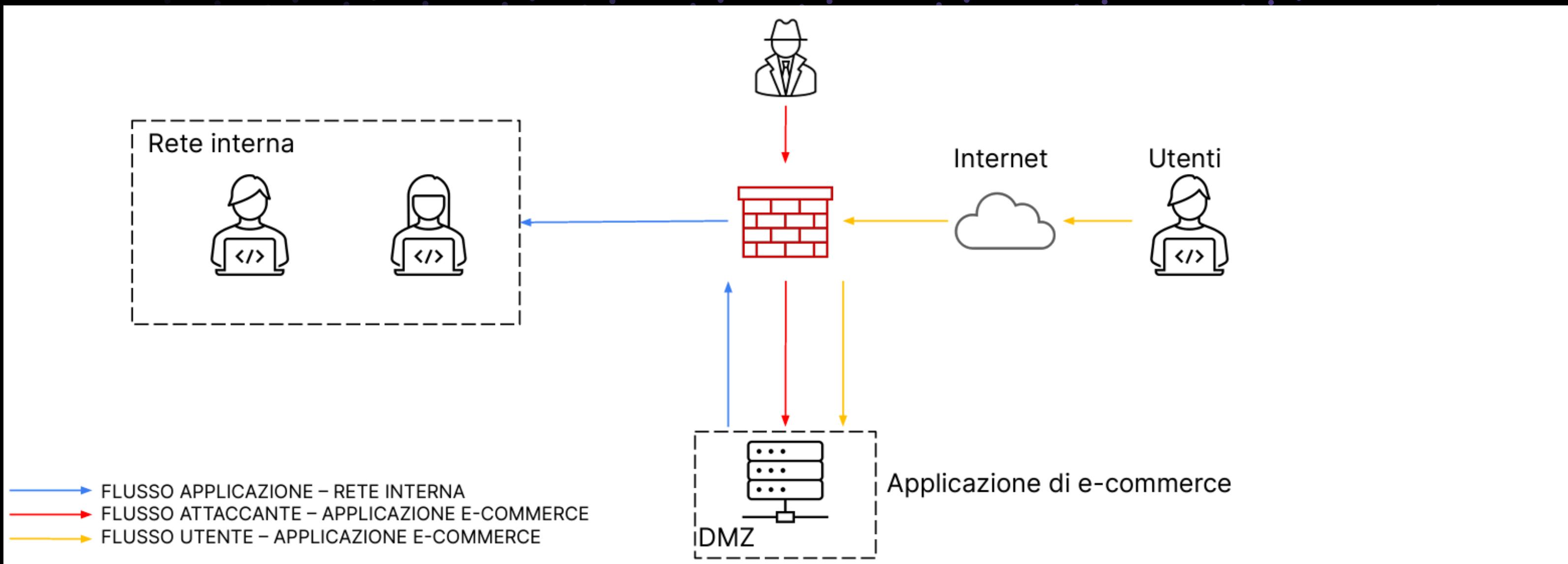
Durata attacco = 10 min

Totale Danno economico = 1500€/min x 10 min = 15000 €

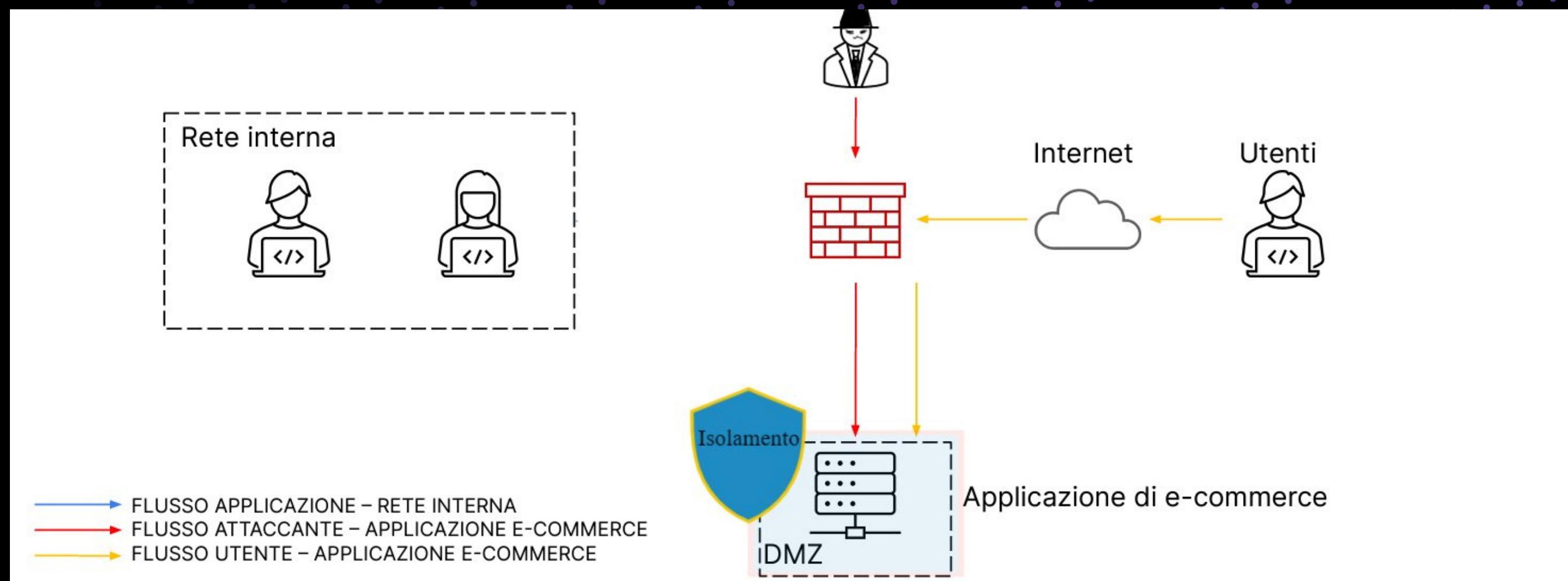
Response

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.

Situazione Iniziale



Situazione Finale



Considerazioni Finali

Per arginare il problema della DMZ compromessa è stato necessario attuare una situazione di isolamento. Così facendo viene prodotta una DMZ completamente isolata dalla rete interna, ma ancora accessibile da internet, è quindi ancora possibile da parte di un attaccante perpetrare le proprie azioni e sfortunatamente è ancora accessibile da parte degli utenti ignari del pericolo.

Quello utilizzato è solo uno dei metodi utilizzati per arginare il problema una volta subito un attacco. Un approccio più sicuro sarebbe quello della rimozione, ossia il completo isolamento della zona ‘infetta’ da qualsiasi tipo rete; così facendo creeremmo l’ambiente ideale per una successiva ‘bonifica’ della zona infetta.
