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?

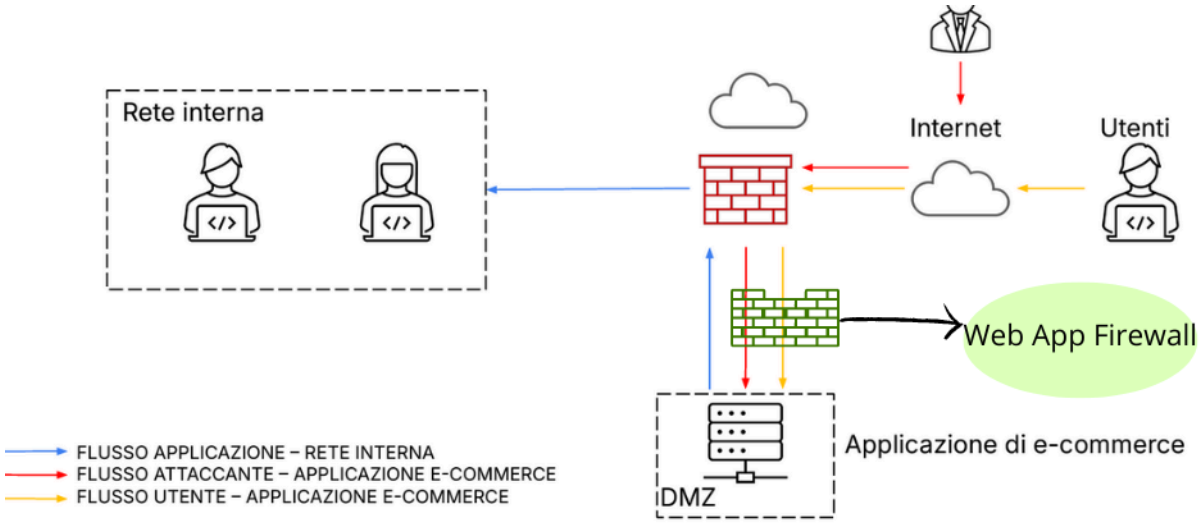
Per esempio nel nostro caso l'azienda nel contesto della web-app con DMZ potrebbe implementare un WAF, cioè un firewall per Web App. Si tratta di una soluzione sviluppata appositamente per proteggere le Web app da XSS e SQL injection.
Naturalmente il WAF si interpone fra la Webapp e internet, allo stesso modo del firewall normale, solo che è strutturato per un monitoraggio più specifico.
Il WAF può essere di tipo hardware, che è in genere la soluzione più costosa e più veloce, oppure software quindi va a incidere sulle prestazioni della macchina che lo ospita. La soluzione più ottimale dal punto di vista dei costi/benefici è il WAF basato sul cloud.

Se pensiamo che il firewall normale che in questo schema si pone su livelli di rete, quindi più bassi nella scala ISO/OSI, dobbiamo invece immaginare il WAF come uno strumento posto nel livello applicativo e in grado di entrare nel merito delle richieste HTTP.

Molti WAF sono programmati per effettuare un'analisi comportamentale, basandosi sullo storico delle richieste che gli utenti della web-app effettuano di solito e riconoscere anomalie. In quel caso si possono impostare policy attive o solo passive quindi di ascolto e salvataggio dei log. Ovviamente sappiamo che le stringhe contenute nelle richieste per la natura dei caratteri contenuti possono essere indice di attacchi. Questo comporta che possano essere impostate o trovarsi già pre-impostate delle regole finalizzate a filtrare i caratteri sospettabili.

Chiaramente, al di là del WAF che dovrebbe coprire gran parte dei problemi a seconda delle configurazioni disponibili, sarebbe possibile fare qualcosa a monte, in fase di programmazione della web-app. Eseguire *l'escaping* dei dati prima di inviarli al browser, per evitare che contenuti malevoli possano eseguire codice JavaScript non autorizzato. Altro esempio, una sanitizzazione dell'input è cruciale per validare e pulire i dati provenienti dagli utenti, soprattutto in campi di testo, utilizzando blacklist di caratteri per prevenire l'inserimento di valori pericolosi.

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

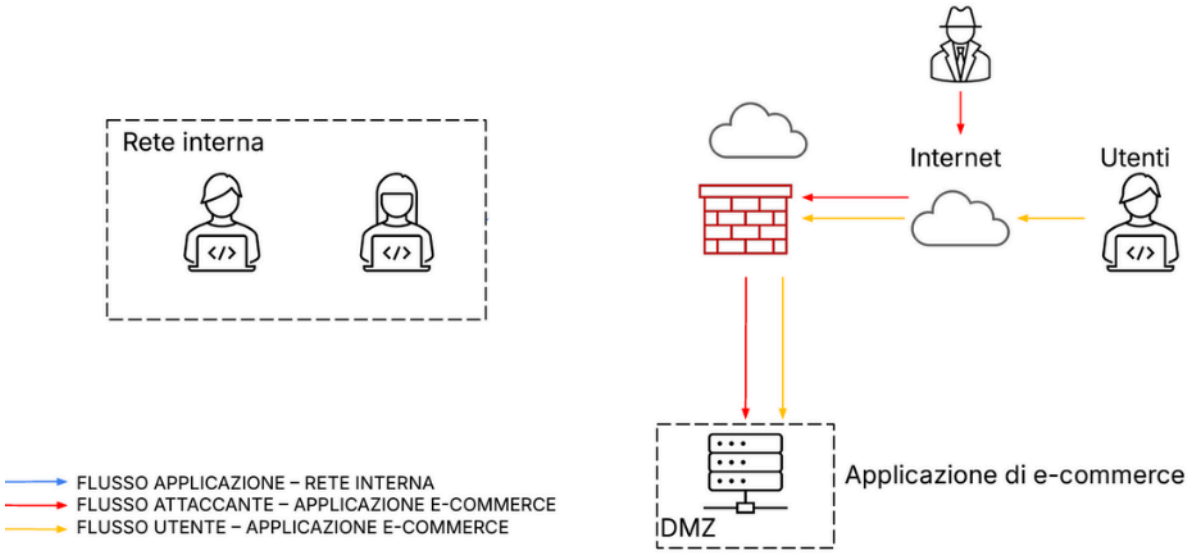
1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Una corretta BIA, Business Impact Analysis, deve tenere in considerazione il MTD ovvero il tempo massimo di inoperatività, e l'RTO quindi il tempo necessario a tornare operativi. Se il secondo è maggiore del primo è chiaro che l'incidente va considerato più grave e la risorsa minacciata più prioritaria da proteggere. C'è un tema di valore dell'asset danneggiato e di percentuale di danno, la BIA, Business Impact Analysis può aiutarci anche a valutare l'impatto quantitativo e qualitativo degli incidenti di sicurezza sul business. La singola perdita attesa (SLE) è direttamente proporzionale al valore (Asset Value) e a questa percentuale (Exposure Factor).

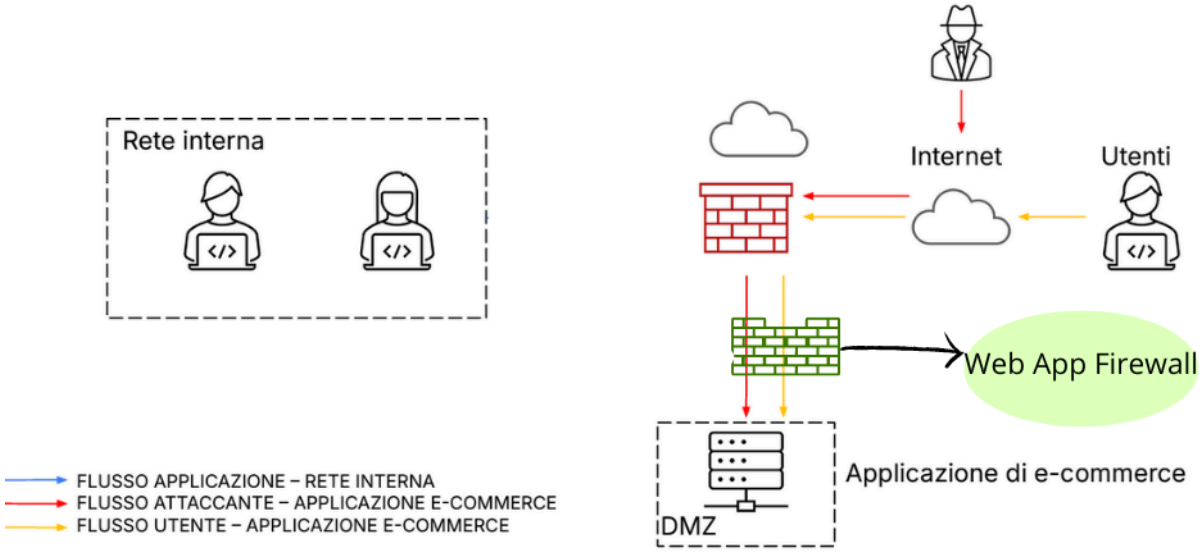
Tuttavia, i dati disponibili ci permette solo di dire che 1.500 euro moltiplicati per 10 minuti fanno di media 15.000 euro persi.
Un attacco DDoS dà inevitabilmente segnali che bisogna intercettare tempestivamente al fine di scongiurarlo. Con degli strumenti di monitoraggio passivo o router-based si possono notare tante richieste TCP simili che provengano contemporaneamente da diversi IP. Stiamo parlando di IoC, indicatori di compromissione. Inoltre dal momento che stiamo parlando di un e-commerce potrebbe essere anche interessante vedere se c'è un numero inusuale di richieste provenienti da paesi dove l'azienda non ha un mercato di riferimento, questo indicherebbe meccanismi di mascheramento dell'IP.

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.

In questo caso l'incident response, segue le procedure prestabilite in fase di foundation. Una soluzione sarebbe quella di isolare la macchina che ospita l'applicazione web dalla rete interna, continuando invece a permettere l'accesso a internet.



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



3