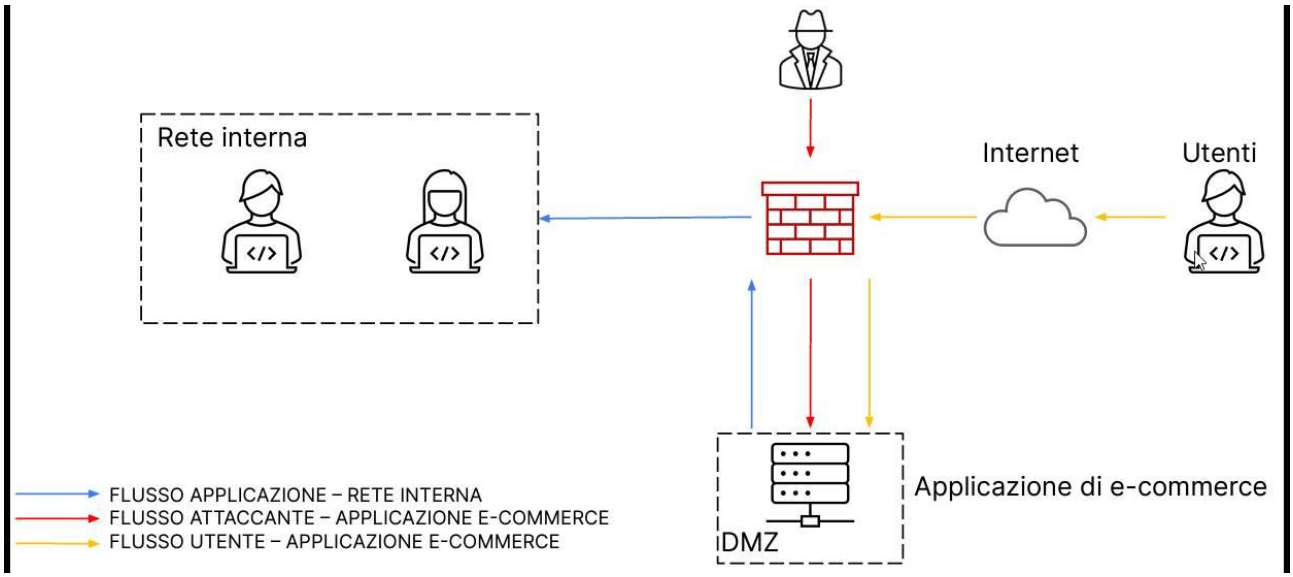
PROLOGO

Data la figura sotto, dobbiamo andare ad illustrare:

- Le azioni preventive che si potrebbero implementare per difendere la nostra Web App da un attacco SQLi e/o XSS;
- Quali impatti può subire il nostro business/e-commerce a seguito di un attacco DDoS che rende irraggiungibile la Web App per 10 minuti;
- Le misure di risposta in caso in cui la DMZ venga infettata da un Malware da un attaccante esterno.

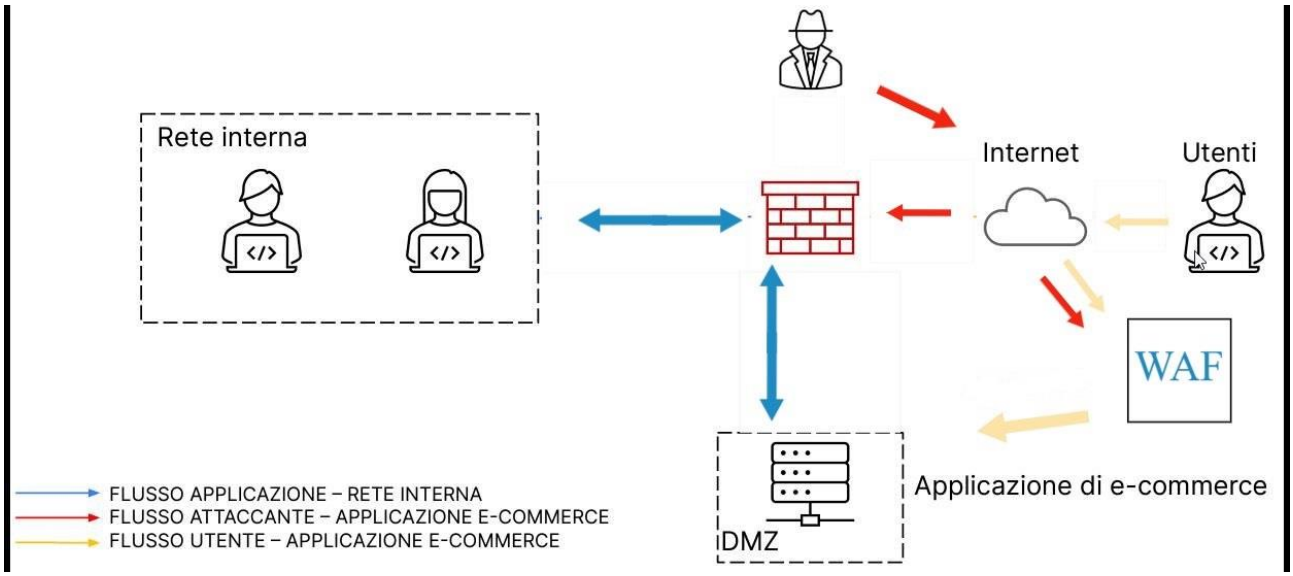


AZIONI PREVENTIVE

Per capire come proteggere la nostra Web App dagli attacchi dati, bisogna innanzitutto definirli:

- SQL Injection: questo attacco va ad agire direttamente sul server che andrà poi a comunicare con il database. È una vulnerabilità dovuta ad una mancata sanificazione del codice da parte del programmatore; in questo modo un possibile attaccante potrà inserire in input un codice SQL malevolo che andrà a restituire nomi utenti e password (in Hash) in output.
- XSS: anche qui la vulnerabilità è dovuta ad un mancato controllo dell'input utente, ma, in questo caso, l'attaccante andrà ad inserire, ad esempio, un link malevolo nella pagina per impossessarsi dei cookies di sessione nel momento in cui un utente cliccherà su di esso (XSS reflected) o andrà ad inserire il codice direttamente sul server così da poterli rubare semplicemente quando l'utente entrerà in quella pagina specifica (XSS stored).

Dopo aver definito gli attacchi, bisogna inserire un WAF (Web App Firewall) per filtrare e monitorare il traffico dall'esterno verso la DMZ (zona accessibile dagli utenti) oltre ad attuare una corretta sanificazione del codice della nostra Web App. Inoltre il FireWall della nostra LAN può essere dinamico e impostato in modo tale che il BlackHat non riesca a bucarlo. In caso, per proteggere la rete interna, si può anche inserire un IPS tra DMZ e rete LAN così da prevenire e bloccare ingressi non desiderati.



IMPATTI SUL BUSINESS

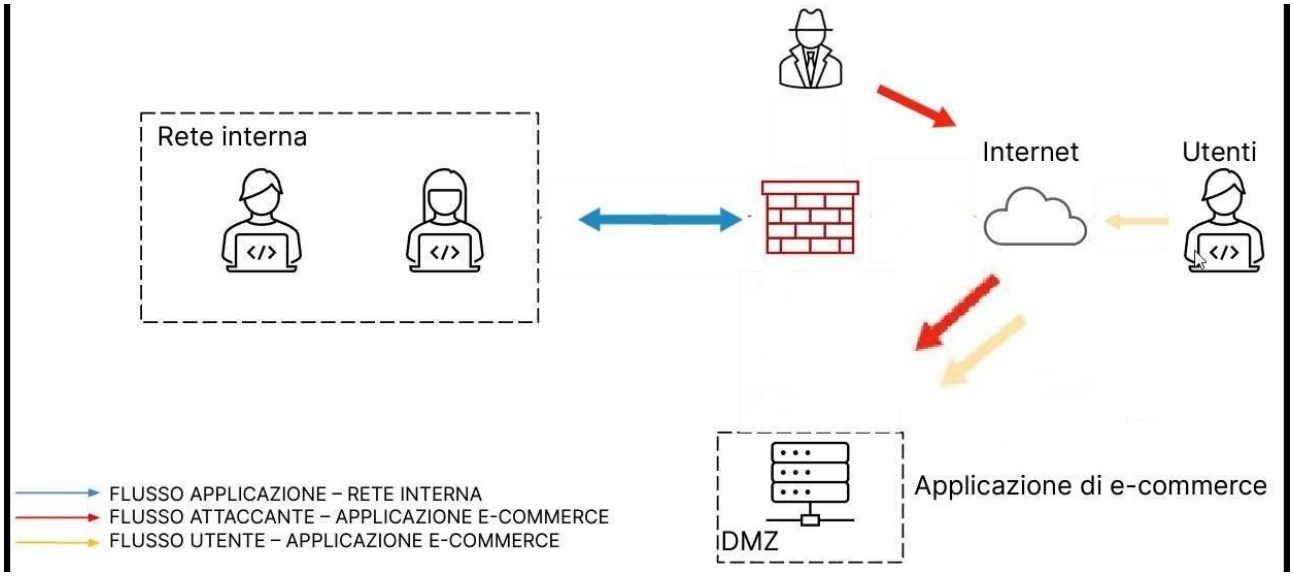
In questo caso la nostra Web App ha subito un attacco DDoS che porta l'applicazione ad essere irraggiungibile per 10 minuti. Questo attacco consente di inviare un grande quantitativo di richieste verso un determinato target tramite l'utilizzo di una rete di macchine infette chiamata 'Netbot'; ciò può mandare in down un determinato servizio rendendolo irraggiungibile. Andiamo a calcolare l'impatto sul business considerando che, in media, ogni minuto gli utenti spendono 1.500€:

- Impatto finanziario = Durata dell'attacco X Spesa media degli utenti al minuto;
- Impatto finanziario = 10 minuti X 1.500€/minuto;
- Impatto finanziario = 15.000€.

Questa analisi viene chiamata anche BIA e ha lo scopo di identificare le risorse critiche che impattano sul business e, in questo caso, è di tipo quantitativo poiché prende in considerazione parametri numerici.

RESPONSE

A seguito di una iniezione di un Malware da parte di un potenziale attaccante, la priorità deve essere quella di intraprendere tutte le operazioni che possono contenere il danno provocato alla nostra azienda. In figura si può notare come agire in fase di contenimento (come richiesto dalla traccia):



Per poter far sì che il Malware non si riproduca e infetti la nostra LAN, l'attività di contenimento inizia con l'isolare l'incidente. Abbiamo quindi isolato il sistema infetto rispetto al resto della rete permettendo comunque all'attaccante di accedere alla macchina compromessa.
Esiste un team apposito che è responsabile di attuare un piano di risposta efficace: il CSIRTs che deve trovare soluzioni.
A valle delle attività di contenimento, il team CSIRT deve passare alla fase di rimozione dell'incidente. In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi, dopodiché inizia la fase di recupero.