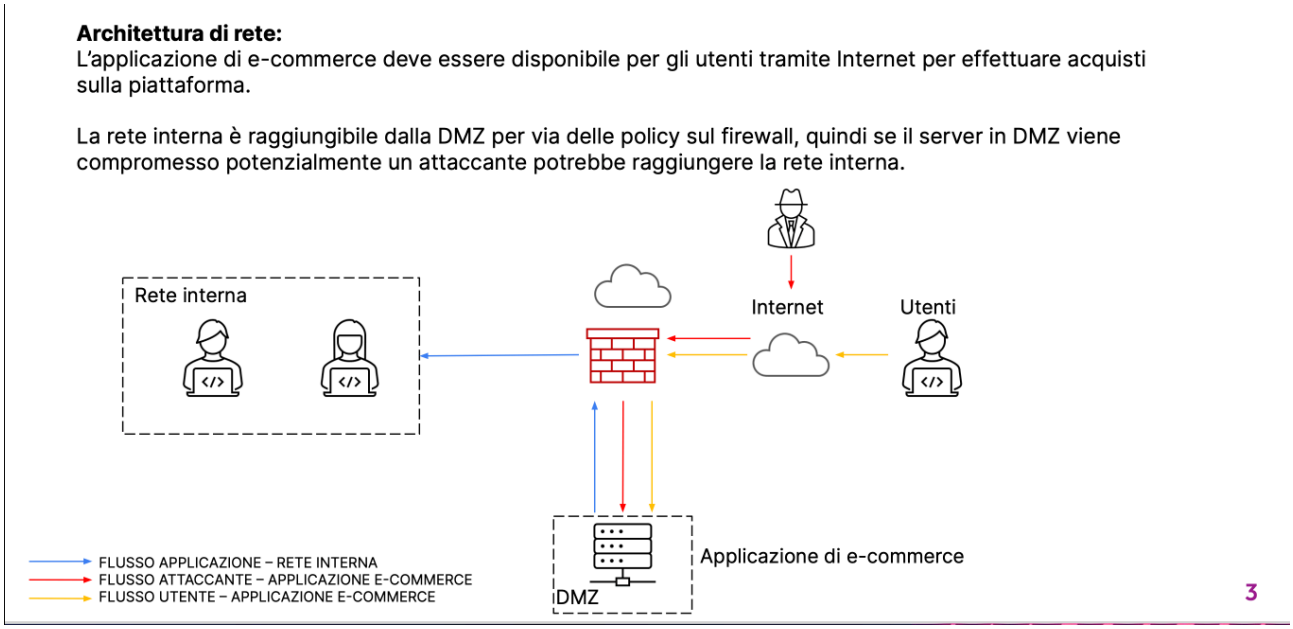
SOC - TI - Incident Response

Situazione di partenza:



1) **AZIONI PREVENTIVE:** come prima cosa, per proteggersi dagli attacchi XSS e SQLi, bisogna che i siti web su cui su appoggia l'applicazione di e-commerce siano costruiti in maniera adeguata, con una dovuta sanificazione dell'input degli utenti da parte della web app. In più possiamo utilizzare un WAF (Web Application Firewall). Quest'ultimo, con una dovuta configurazione, consente di proteggerci da eventuali minacce (appunto XSS, SQLi, bots..)

2) **IMPATTI SUL BUSINESS:** Se l'e-commerce in questione fosse non raggiungibile per 10 minuti ci sarebbe una perdita di circa 15.000€, visto che ogni minuto in media gli utenti spendono 1.500€. Questo incidente ovviamente avrebbe un alto impatto negativo sull'azienda e bisognerebbe quindi in maniera preventiva adottare delle misure di sicurezza. Mitigare un DDoS però non è certamente una cosa semplice. Anche qui l'utilizzo di un WAF potrebbe essere utile in quanto va a bloccare il traffico proveniente da botnets (di solito usati per gli attacchi DDoS). Inoltre l'azienda potrebbe avere un team CSIRT interno pronto in caso d'incidente, monitorando il traffico e bloccando gli indirizzi IP dell'attaccante, oppure ci si potrebbe avvalere di azienda esterna che fornisce servizi di DDoS Mitigation, come Cloudlflare e Barracuda.

3) **RESPONSE:** Se un malware colpisce l'applicazione web nella DMZ e non ci interessa rimuovere l'accesso da parte dell'attaccante possiamo usare la soluzione dell'isolamento. In tal modo andremo a disconnettere il server infetto dalla nostra rete, per evitare che il malware possa colpire la rete interna.

Se applicassimo invece una totale rimozione del server, risulterebbe in un DoS in quanto non sarebbe più raggiungibile neanche dai normali utenti.

4)**SOLUZIONE COMPLETA**

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.