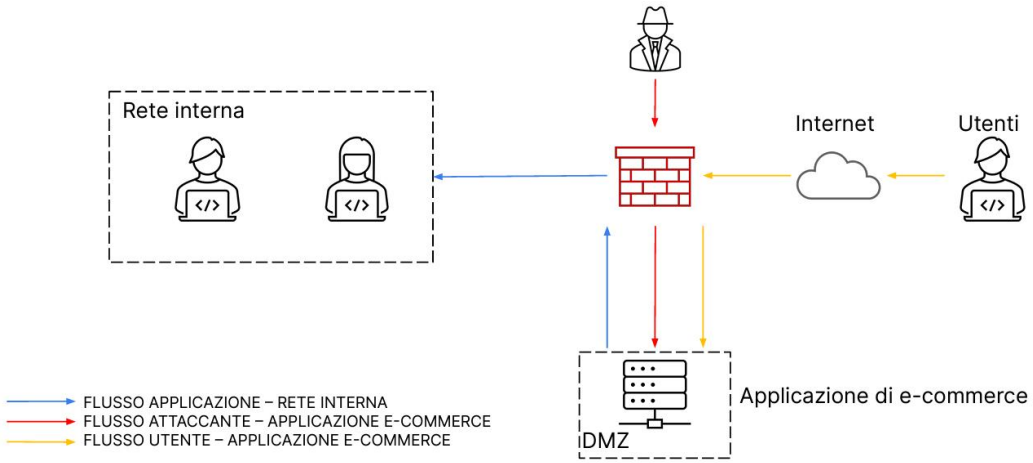
PROGETTO S9

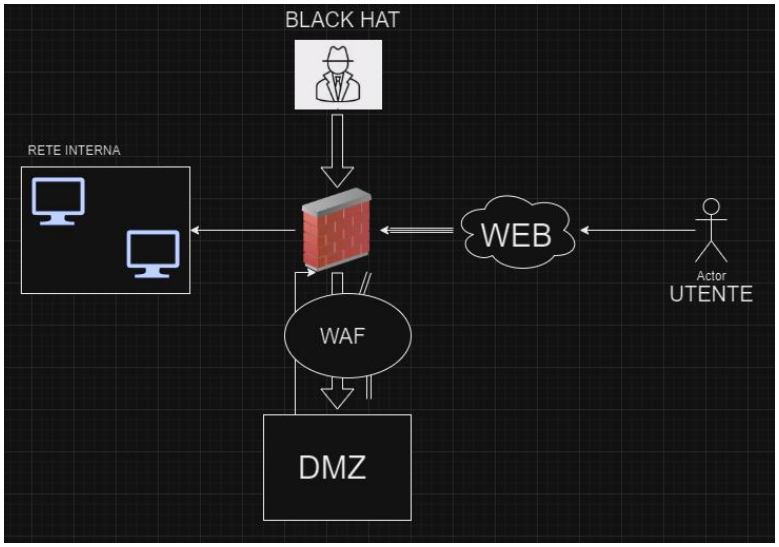
L’applicazione di e-commerce deve essere disponibile per gli utenti internet per effettuare acquisti sulla piattaforma.
La rete è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante raggiungere la rete interna.



AZIONE PREVENTIVA

L’attaccante puo sfruttare SQLi e XSS sul web server.
Possiamo:

- sanificare la pagina web per impedire che SQLi e XSS possano avvenire
- Limitare accesso ai file e alle cartelle sensibili
- Istruire i dipendenti rispetto a queste vulnerabilità per ridurre l’errore umano
- Utilizzare un WAF
- L’imitare l’accesso ai servizi necessari e agli utenti autorizzati



IMPATTI SUL BUSINESS

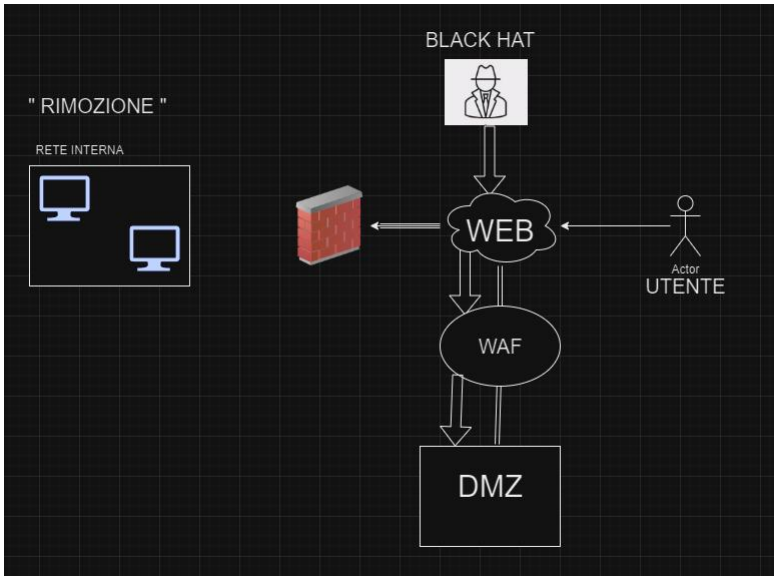
L'application web subisce un attacco di tipo Ddos dallesterno che rende l'applicazione non raggiungibile per 10 min (in 1 min gli uteti spendono 1500e).

IMPATTO = 1.500 * 10
IMPATTO = 15.000

Per evitare tali perdite possiamo ridurre l'accesso solo ai servizi necessari, effettuare regolarmente test per controllare le vulnerabilità, aggiornare sempre.

RESPONSE

L'applicazione web viene infettata da un malware.



Per impedire che il malware infatti la rete interna rimuoviamo la rete da tutto il resto isolandolo, cosi possiamo riparare il danno.

È da tener presente che il black hat continua ad essere attaccato alla DMZ e che quindi il malware puo invece attaccare gli utenti.

Il WAF impedira lo sfruttamento di SQLi e XSS.