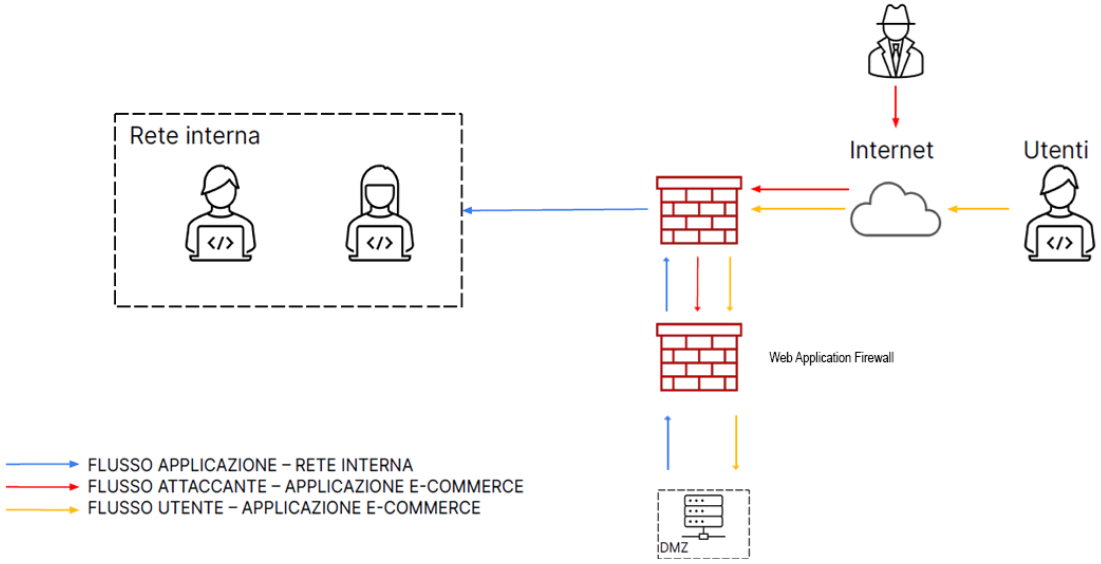
1. Azioni preventive

Le vulnerabilità derivanti dal Cross Site Scripting possono essere mitigate con varie metodologie.
Secondo la guida "OWASP Cross Site Scripting Prevention Cheat Sheet"[1] ad esempio è possibile diminuire l'esposizione a tale attacco controllando estensivamente tutti gli input passati dall'utente tramite l'ausilio di librerie apposite. Le guidelines forniscono informazioni utili al fine di implementare azioni quali Framework Security Protections, Output Encoding e HTML Sanitization.
Per diminuire l'impatto degli XSS è possibile mettere in atto anche le seguenti azioni come:

- usare il flag HttpOnly per i cookie in modo da evitare che JavaScript e i browser possono interagire con essi;
- adottare policy di tipo CSP (Content Security Policy[2]) come ad esempio attraverso una *allowlist* che impedisce il caricamento di contenuti malevoli;
- Elaborare un sistema di difesa comprensivo di WAF (Web Application Firewall) per bloccare i payload.

La fondazione OWASP mette a disposizione anche delle linee guide al fine di prevenire attacchi di tipo SQL injection[3]. La guida fa distinzione tra difese primarie quali ad esempio l'utilizzo di *prepared statements* e difese aggiuntive come una policy di *least privilege*.



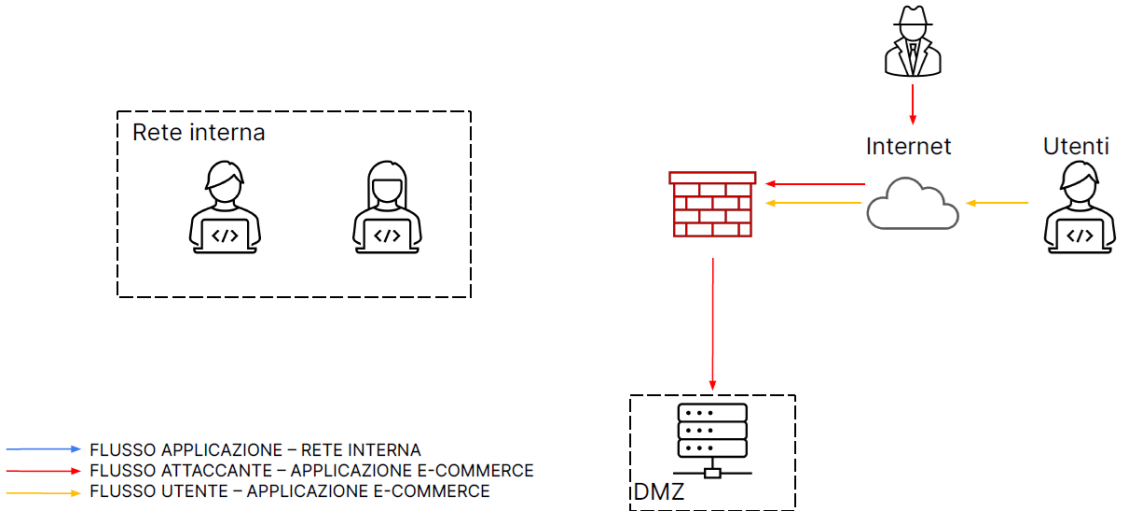
2. Impatti sul business

Attacco DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti.
Ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

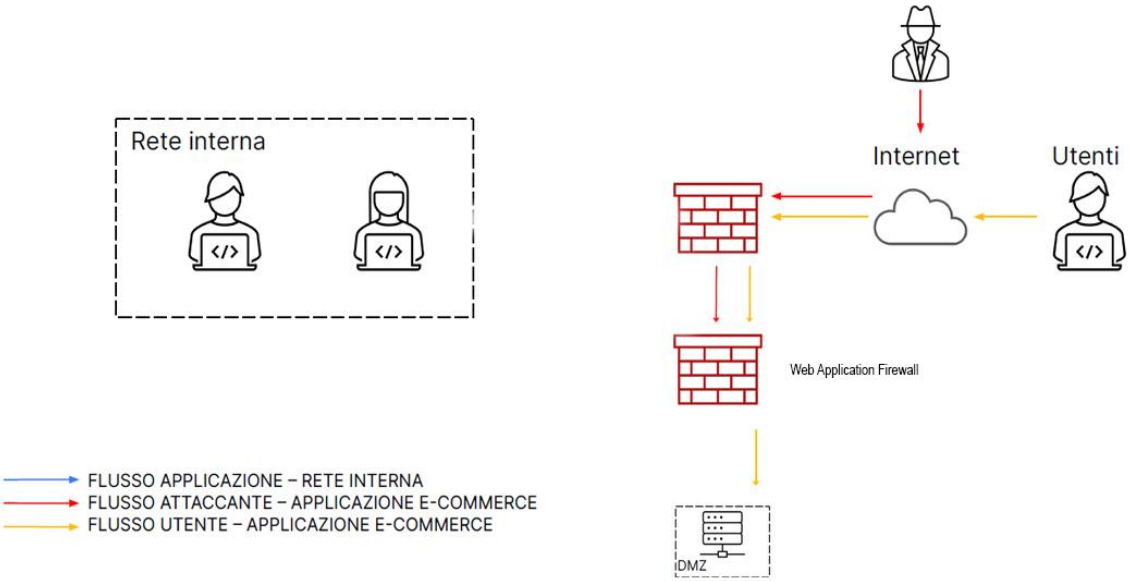
Considerando le variabili sopra descritte si avrebbe una perdita monetaria dovuta al mancato incasso delle vendite non effettuate a causa dell'attacco DDoS pari ad euro 15.000,00.
Nella prevenzione a questi tipi di attacco rientra l'analisi del traffico di rete così da poter notare flussi inaspettati o comunque sospetti attraverso ad esempio soluzioni software che permettono di individuare i segnali rivelatori di un attacco DDoS come ad esempio un incremento incomprensibile delle richieste a una singola pagina. Un'altra azione praticabile potrebbe essere quella di implementare una Content Delivery Network utilizzando il caching su altri server diversi da quello di hosting aiutando a impedire l'interruzione del servizio.

[1] https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
[2] https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
[3] https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

3. Response



4. Soluzione completa



5. Modifica più aggressiva