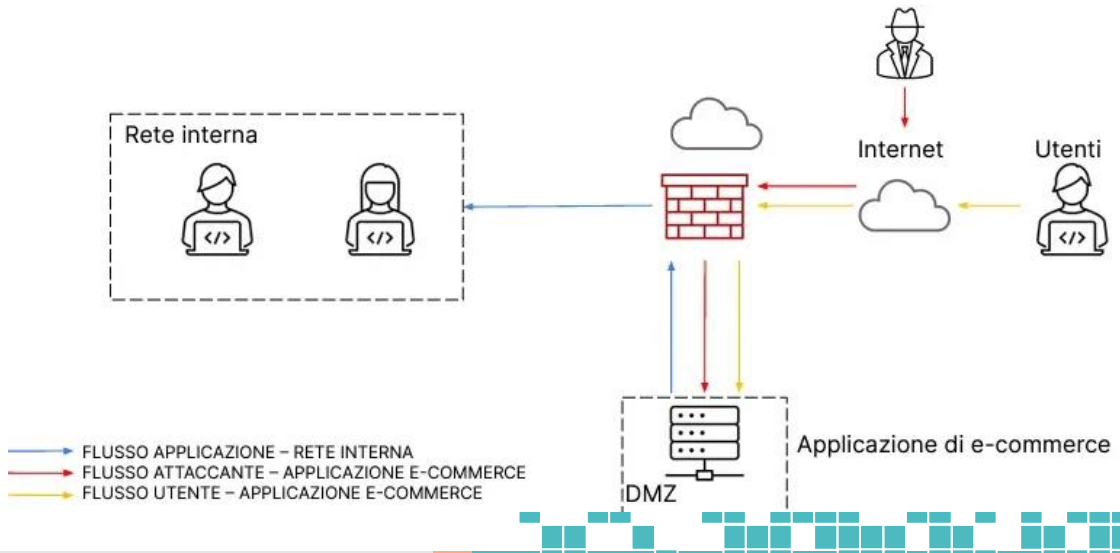
W20D4 – PEPPOLI

Traccia: Con riferimento alla figura in slide, rispondere ai seguenti quesiti.
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? 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
3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide con la soluzione proposta.
4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)
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 venisse compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

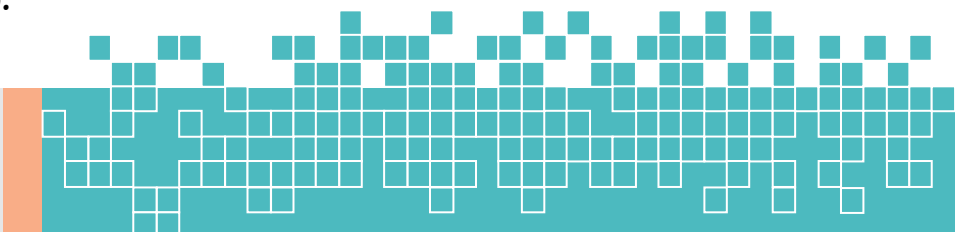


Le azioni preventive per difendere l'applicazione web da attacchi di tipo SQLi e XSS potrebbero prevedere:

- l'implementazione di un Web Application Firewall (WAF), posto davanti all'applicazione di e-commerce per filtrare e bloccare richieste malevole contenenti payload SQLi e XSS.
  Un WAF si inserisce come muro perimetrale, che consente di controllare gli accessi alle risorse di un sistema, filtrando tutto il traffico che viene effettuato da un ambiente interno ad un ambiente esterno.
  La specializzazione di un WAF è proprio il fatto di intercettare e analizzare il traffico HTTP. Inoltre, può implementare un modello di sicurezza positivo, che consente il passaggio se e solo se la transazione è valida, oppure analitico, che ferma ogni messaggio, lo analizza alla ricerca di possibili minacce e giudica se inserirlo in white o black list, confrontandolo con database noti di policy, firme o stessi di white/black list. L'ultima tipologia di WAF è il 3.0, un WAF a 360°, in grado di prevenire determinati attacchi, attivando un sistema protettivo che localizza e identifica le vulnerabilità, ricostruendo la catena degli eventi durante particolari sessioni.
- Assicurarsi che l'applicazione effettui dei controlli adeguati di validazione e sanitizzazione degli input utente prima di utilizzarli nelle query o negli output HTML.
- Applicare la protezione delle vulnerabilità note tramite patch di sicurezza e aggiornamenti dei software.
- Abilitare meccanismi di difesa come la protezione HTTP CSRF (cross-site request forgery): si tratta di una vulnerabilità a cui sono esposti siti web progettati per ricevere richieste da un client, senza meccanismi per controllare se la richiesta sia stata inviata intenzionalmente oppure no.

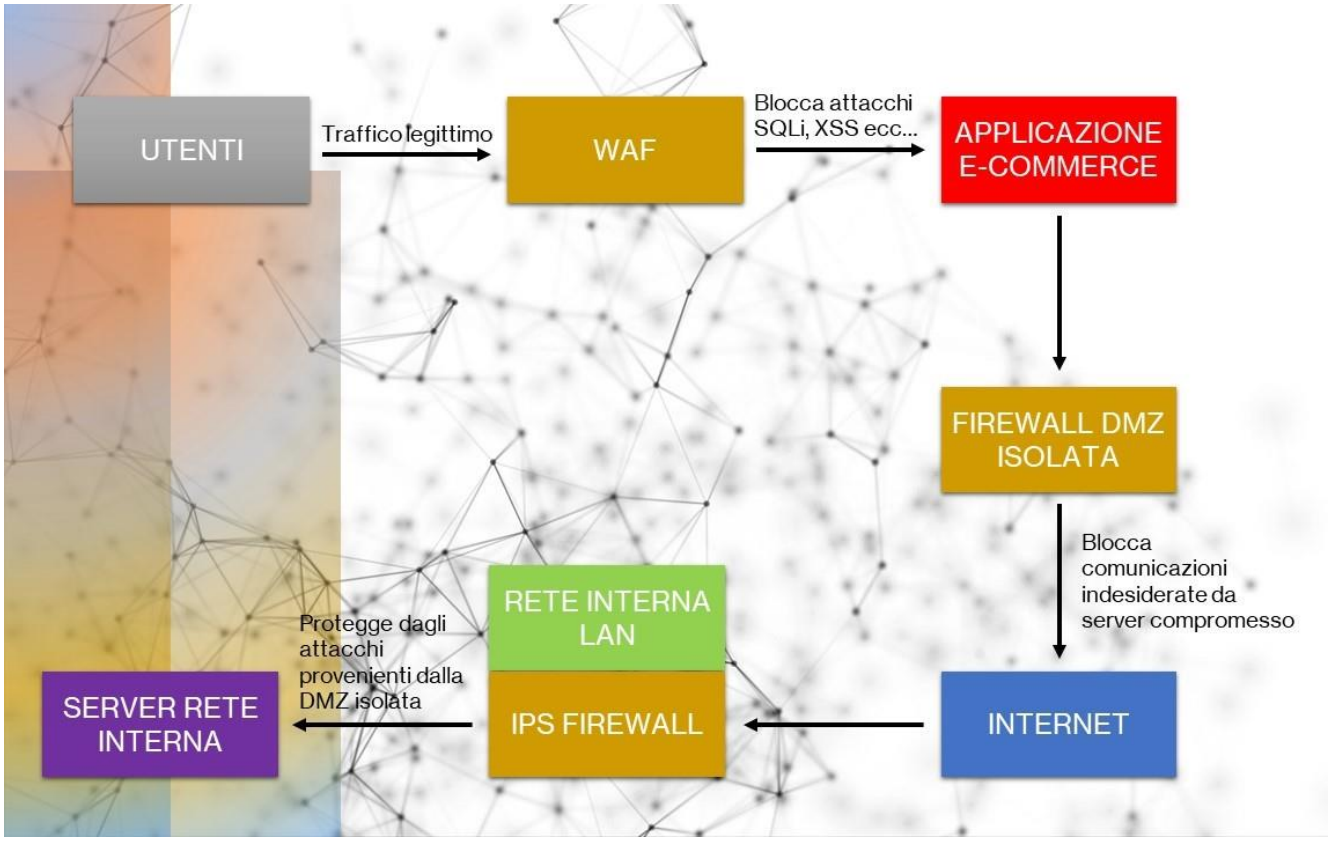
L'impatto sul business di un attacco DDoS di 10 minuti, con una spesa media di 1500€ al minuto degli utenti, causerebbe una perdita di:
10 minuti * 1500€/minuto = 15000€ di perdita.
Le azioni preventive per non permettere un attacco di questo tipo, o per far si che succeda molto raramente possono includere:

- Implementazione di soluzioni anti-DDos come servizi cloud o appliance dedicate a mitigare gli attacchi.
- Assicurarsi di avere una banda sufficiente e una capacità di scalabilità per gestire dei picchi di traffico.



- Configurare correttamente i firewall e i sistemi di rilevamento delle intrusioni per bloccare traffico malevolo.

Per evitare la propagazione sulla rete interna di un malware dannoso, la soluzione sarebbe isolare il server web compromesso dalla DMZ tramite un firewall dedicato che blocchi tutte le connessioni in ingresso/uscita ad eccezione del traffico legittimo verso Internet per l'e-commerce.



In questa soluzione:
È stato implementato un Web Application Firewall (WAF) di fronte all'applicazione di e-commerce per bloccare attacchi di tipo SQLi, XSS e altre minacce a livello applicativo.
Il server dell'applicazione di e-commerce è isolato nella DMZ tramite un firewall dedicato che blocca tutte le comunicazioni indesiderate provenienti dal server, nel caso in cui venga compromesso.
La rete interna aziendale (LAN) è protetta da un IPS/Firewall che impedisce qualsiasi attacco proveniente dalla DMZ isolata, bloccando la potenziale propagazione di malware o accessi non autorizzati.

In questo modo, l'infrastruttura è protetta sia a livello dell'applicazione web che a livello di rete, isolando efficacemente eventuali compromissioni e limitando i danni a quel segmento specifico.

Una modifica che porterebbe ad un livello di sicurezza più avanzato, sarebbe quello di spostare l’applicazione e-commerce su cloud dedicata e isolata, separata dalla rete aziendale. In questo modo, anche in caso di compromissione, l'attaccante non avrebbe alcun modo di raggiungere la rete interna. Sarebbe necessario un accesso VPN o simili per la gestione amministrativa.