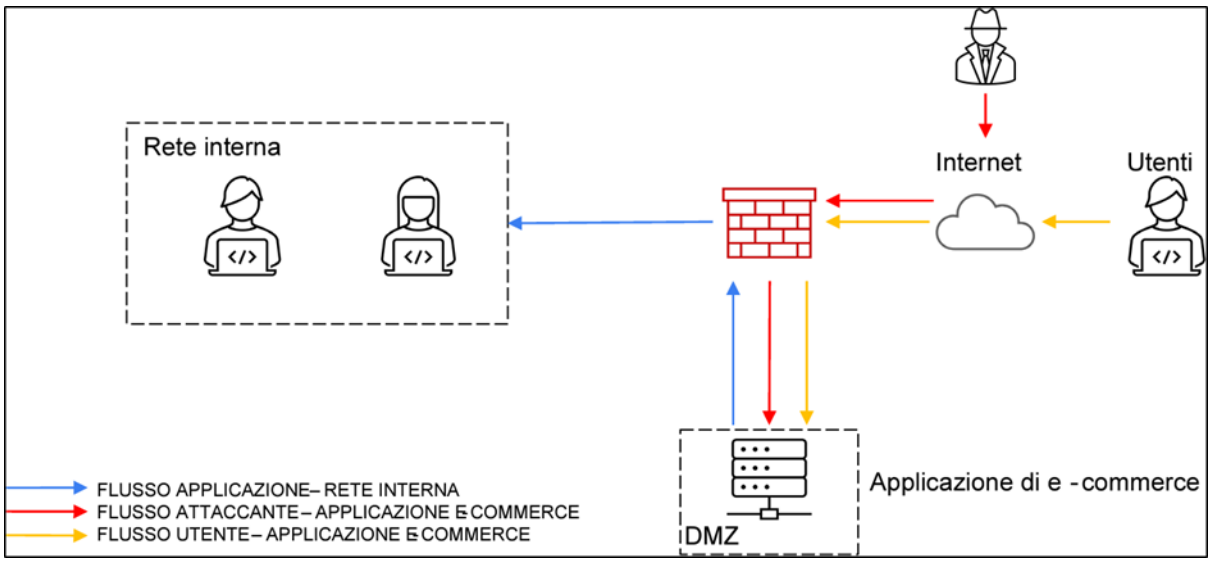
Incident Prevention and Response

Traccia

Oggi ci viene chiesto di prendere come riferimento la seguente figura e rispondere a dei quesiti



1. **Azioni Preventive**: Definire azioni preventive per difendere la Web App da attacchi SQLi e XSS modificando la figura sopra.
2. **Impatti sul Business**: Ipotizzando che la Web App subisce un attacco DDoS che la rende irragiungibile per 10 minuti, Calcolare l'impatto sul business considerando una media di 1500€ spesi al minuto e fare valutazioni di azioni preventive per questo problema.
3. **Response**: La Web App viene infettata da un Malware. Trovare una soluzione per non far propagare il Malware nella rete senza rimuovere l'accesso alla macchina infetta all'attaccante e modificare la figura sopra con la soluzione proposta.
4. **Soluzione Completa**: Unire disegni di Azione Preventiva e Response.
5. **Modifica Aggressiva dell'Infrastruttura**: Integrando altri elementi di sicurezza.

Azioni Preventive

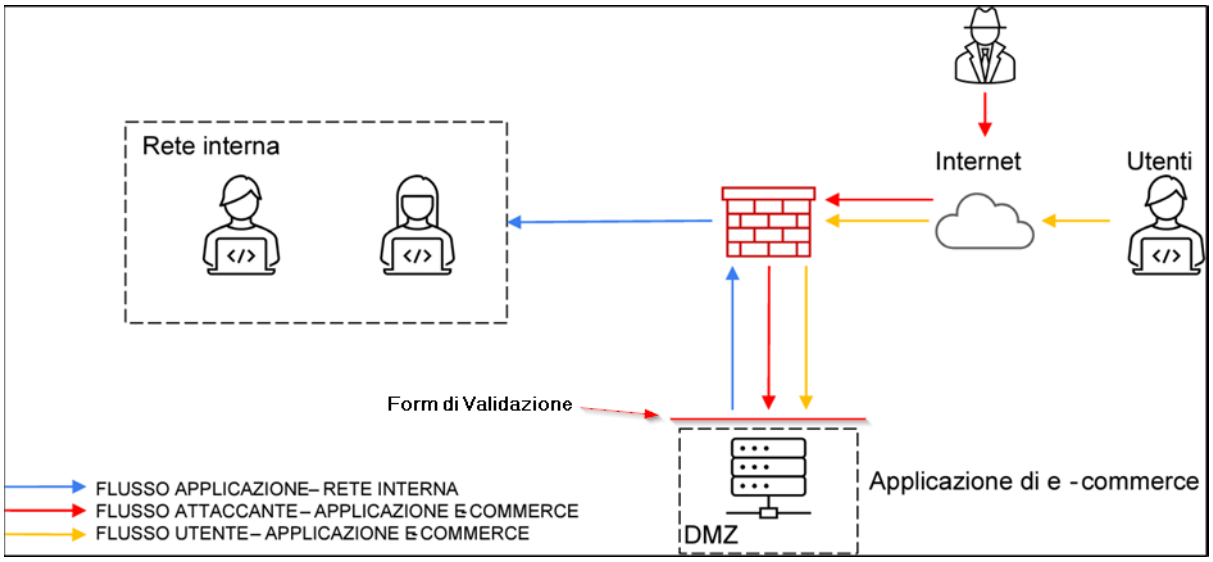
Spiegazione attacchi SQLi e XSS

Le SQLi (SQL Injection) sono attacchi che sfruttano vulnerabilità nelle Web App per iniettare codice SQL malevolo nel database di un server e manipolare, cancellare o rubare dati da quest'ultimo.

XSS (Cross-Site Scripting) sono attacchi che iniettano script malevoli in pagine web col fine di rubare cookies, token di sessione, altre informazioni sensibili o reindirizzare l'utente su un sito malevolo che può contenere ad esempio del Malware.

Prevenzione

Per prevenire questi attacchi è fondamentale implementare una rigorosa validazione dell'input tramite form. Questi form devono escludere caratteri speciali non necessari, garantendo, ad esempio, che l'input per un indirizzo email contenga solo caratteri come '@' e '.' e escluda quelli non validi per gli indirizzi email, come '<', '>', '?' e altri.



Impatti sul Business

Spiegazione attacco DDoS

Un DDoS (Distributed Denial of Service) è un tipo di attacco informatico che mira a rendere inaccessibile un servizio online facendo sì che diventi sovraccarico di traffico illegittimo.

Calcolo Impatto e Misure Preventive

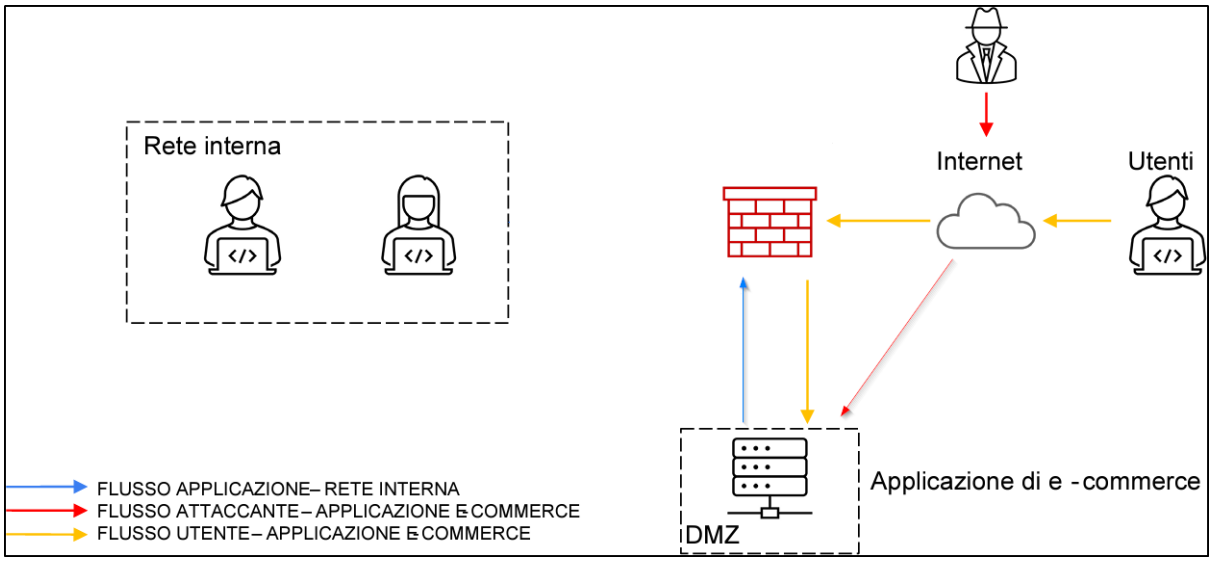
In questo caso un attacco DDoS della durata di 10 minuti comporterebbe una perdita di circa 15000€ (10 minuti x 1500€ guadagno medio al minuto).

E' possibile prevenire tali attacchi impostando un rate limiting nel firewall, ovvero limitare il traffico in ingresso, basandovi sul traffico medio del sito per evitare di intaccare l'esperienza dell'utente legittimo.

In alternativa potete investire in un servizio come CloudFlare che offre protezione contro gli attacchi DDoS ed ha piani di iscrizione di vario livello (incluso uno gratuito) in base alle vostre esigenze.

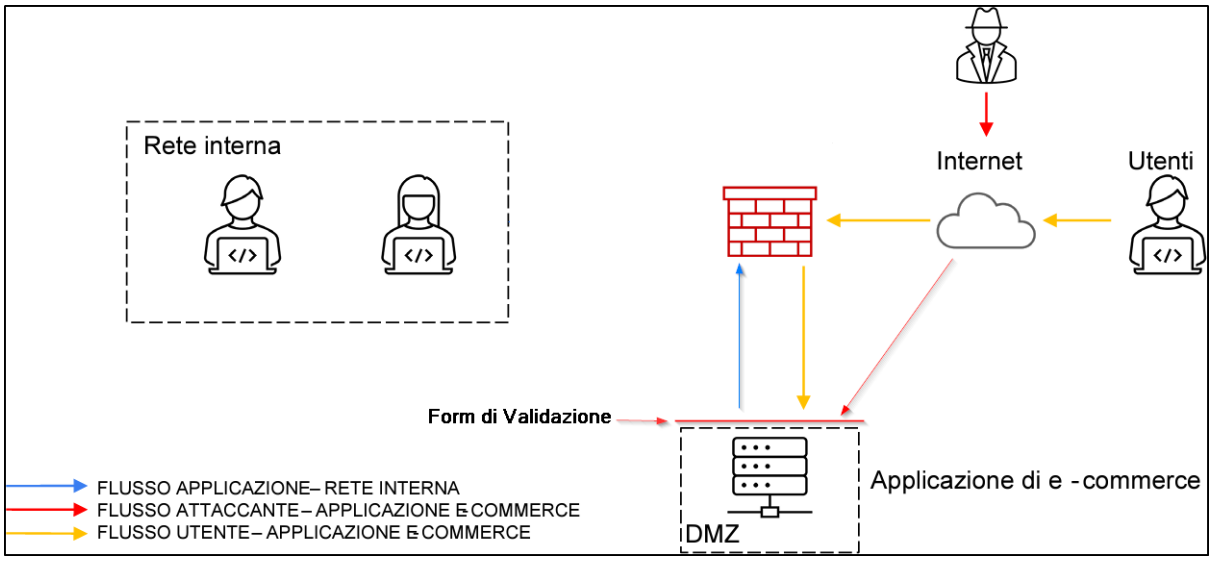
Response

Per isolare la rete interna dalla Web App compromessa la soluzione migliore sarebbe disconnettere fisicamente il sistema infetto dalla rete interna, se ciò non è possibile si possono apportare modifiche alle regole del firewall al fine di prevenire la comunicazione del server infetto con gli altri dispositivi all'interno della rete interna. Questa operazione può essere attuata bloccando specifiche porte o indirizzi IP associati al server compromesso.



Soluzione Completa

Andiamo a unire il form di validazione come difesa da SQLi e XSS e l'isolamento della rete interna in un unica soluzione come rappresentato nella figura seguente



Modifica Aggressiva dell'Infrastruttura

Per migliorare la sicurezza dell'azienda consigliamo l'implementazione di un WAF (Web Application Firewall) come AWS WAF che è un WAF fornito da Amazon e protegge sia contro attacchi SQLi, XSS e se configurato correttamente anche da attacchi DDoS.

Da quali tipi di attacco protegge AWS WAF?

AWS WAF aiuta a proteggere i tuoi siti Web da tecniche di attacco comuni quali SQL injection e cross-site scripting (attacchi XSS). Inoltre, è possibile creare regole per bloccare o limitare la velocità del traffico da un agente utente specifico, da un indirizzo IP specifico o che contiene particolari intestazioni di richiesta. Consulta la AWS WAF Developer Guide per vedere

Si può usare la regola basata sul tasso per mitigare gli attacchi DDoS al layer Web?

Sì. Questo nuovo tipo di regola è progettato per proteggere da casi d'uso come attacchi DDoS al layer Web, tentativi di accesso di forza bruta e bot dannosi.

Abbiamo stimato una spesa media di 211$ (circa 200€) al mese per implementarlo usando il calcolatore di AWS WAF.

1 Web ACLs per month x 5.00 USD = 5.00 USD (WAF Web ACLs cost)
1 Web ACLs per month x 200.00 Billable Rules per web ACL per month x 1.00 USD = 200.00 USD (WAF Rules cost)
10 requests per month x 1000000 multiplier for million x 0.0000006 USD = 6.00 USD (WAF Requests cost)
5.00 USD + 200.00 USD + 6.00 USD = 211.00 USD
WAF cost (monthly): 211.00 USD

Inoltre consigliamo di investire su un IPS, simile a quello mostrato di seguito, da mettere fra il firewall e la rete interna per avere un ispezione dei pacchetti più approfondita.