S9 L5

Risposta ad un attacco alle WEB APP

Daniele Zizzi

In questo progetto, andremo ad effettuare delle azioni correttive, al fine di scongiurare un attacco verso le WEB APP, attraverso l’utilizzo di hardware, software e tecniche apposite.

Per evitare attacchi di tipo SQLI e XSS, bisogna filtrare l’input dell’utente, affinchè non vengano accettati codici malevoli in input. Si può evitare ciò, impostando una regola che, ogni qualvolta viene scritta la parola “<script>” o altro codice malevolo, la sostituisce con degli spazi vuoti o altri caratteri che non permettono l’esecuzione di tale codice.

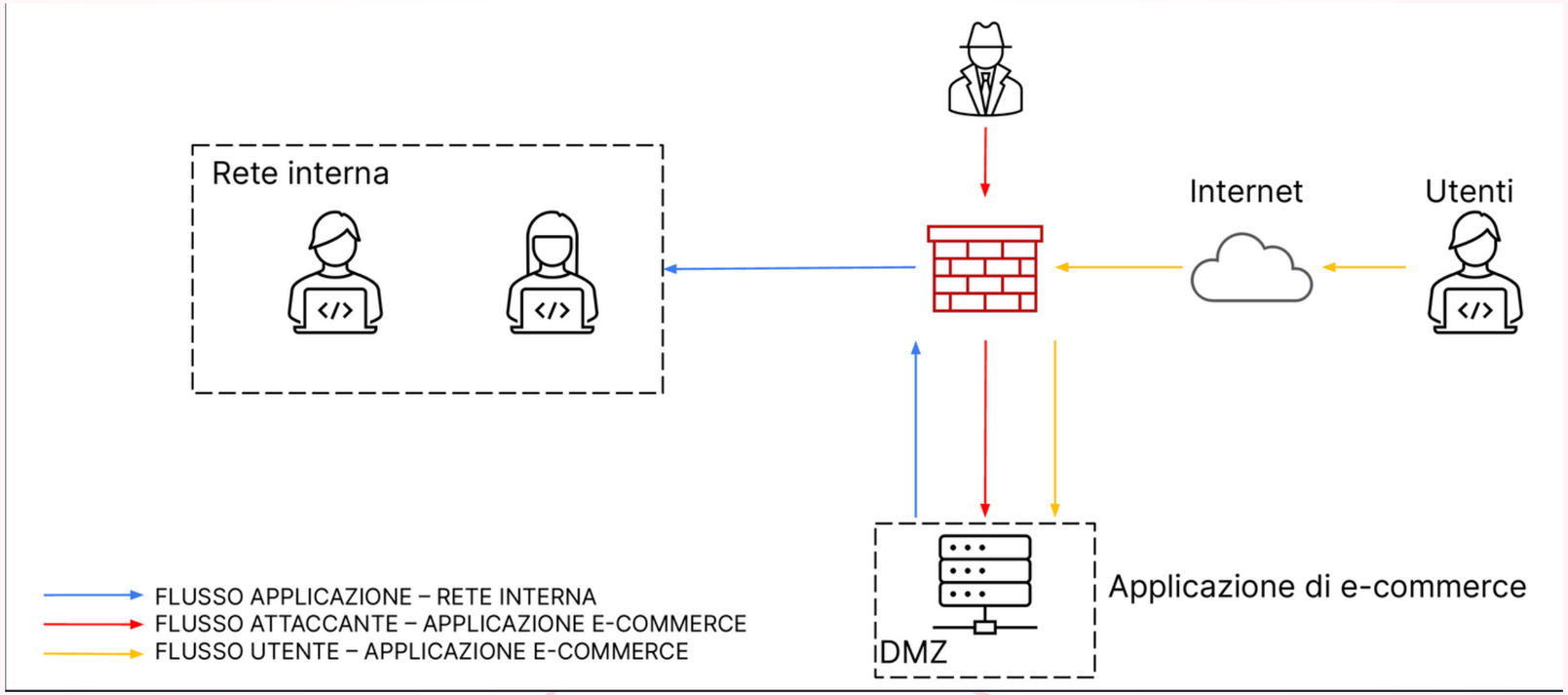
Questo tipo di attacchi, mira a rubare i dati e cookie degli utenti.

Attacchi di tipo SQLI mirano ad estrapolare informazioni da un database SQL.

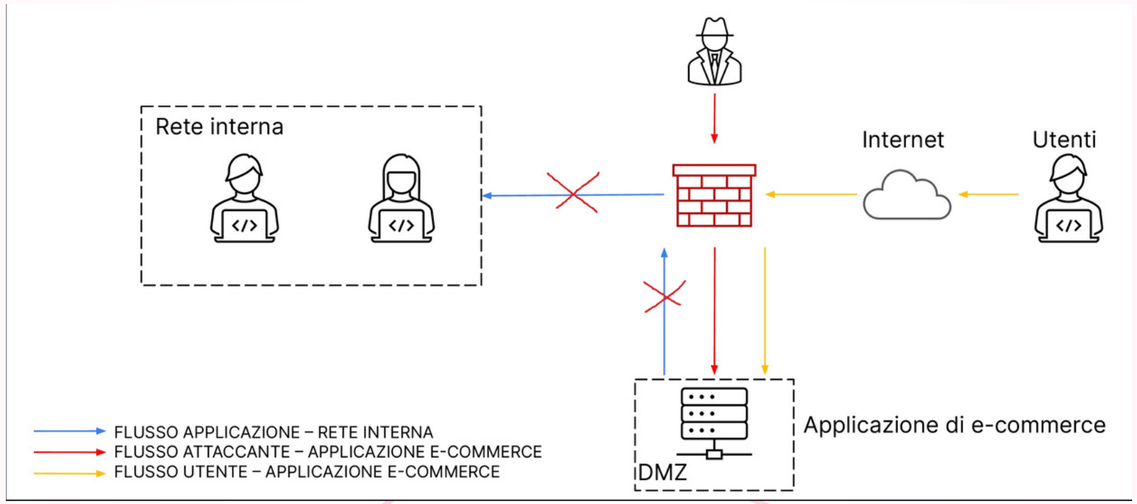
Gli attacchi di tipo XSS reflected e stored, mirano ad attaccare direttamente i dati degli host. Singolo host nel caso di reflected, tutti gli host che si collegano alla pagina web malevola nel caso di stored.

Le informazioni estrapolate posso essere username e password degli utenti, indirizzi di residenza/spedizione, dati delle carte di credito, cronologia degli ordini effettuati.

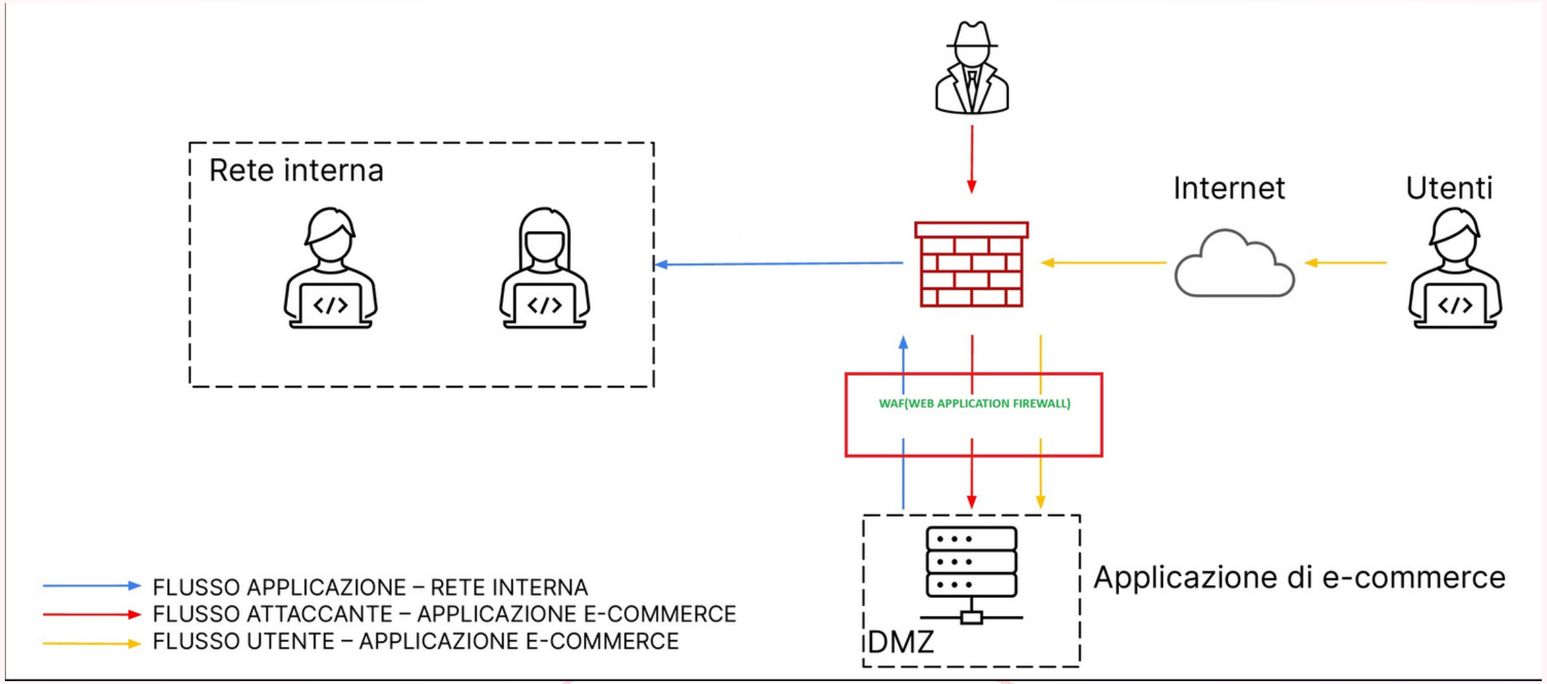
Situazione attuale durante un attacco, dove, l’attaccante, invia pacchetti malevoli verso il webserver da internet. Il web server è in DMZ(DEMILIRATIZED ZONE), pertanto non è possibili attaccare direttamente la rete interna, poichè protetta da firewall perimetrale, che accetta connessioni in entrata solo come risposta a richieste effettuate dall interno.



Una possibile soluzione è quella di isolare il web server. L’accesso all’hacker e agli utenti verrà mantenuto, ma non sarà possibile in alcun modo attaccare la rete interna. Le tecniche di isolamento utilizzabili in questo caso è la segmentazione della rete, con subnetting(creazione di una sotto rete apposita per l’host infetto) e/o creazione di una VLAN apposita e disattivando il transito dei dati dà e verso la VLAN della rete interna.
Il subnetting da solo non è sufficiente, poichè il router, permette lo scambio di dati tra reti diverse. Quindi è necessario utilizzare un ACL(Access Control List) o Firewall, in modo da bloccare l’accesso verso il web server infetto dalla rete interna.



Un altro modo per bloccare l’attacco è l’implementazione di un WAF(WEB APPLICATION FIREWALL), che si occuppa di rilevare codici malevoli nei pacchetti inviati verso il web server. In caso di rilevamento, attraverso interrogazione delle firme presenti in locale e sul cloud, i pacchetti malevoli vengono bloccati.



Dopo l’utilizzo delle tecniche mostrate in precedenza, dobbiamo ripulire il server, rimuovendo processi e file caricati dall’attaccante, al fine di ripristinare l’affidabilità della macchina ed evitare che gli utenti che si collegano alla web application vengano infettati. Dopo aver ripulito il tutto, con l’utilizzo di antivirus e antimalware, possiamo riattivare l’accesso dalla rete interna verso il web server. Un’altra possibilità può essere quella di attivare un server clone che eroga gli stessi servizi, con un stato precedente all’infezione. Oppure grazie all’utilizzo di backup, sempre con uno stato precedente alla compromissione, ma questo comporta un perdita momentanea del servizio, poichè bisogna ricorrere alla formattazione del sistema, affinchè tutti i file e processi malevoli vengano rimossi.

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.

L’attacco DDoS(Distributed Denial of Service), mira ad esaurire le risorse di un sistema, grazie all’utilizzo di botnet. L’attacco avviene da più host contemporaneamente al fine di compromettere l’erogazione di servizi ai client.

Il danno aziendale totale per 10 minuti di disservizio sarà di 15.000 €

È possibile diminuire o addirittura reggere il carico di tale attacco, attraverso l’utilizzo del load balancing, che non fà altro che distribuire l’attacco su più server, al fine di avere più risorse disponibili.

Attacchi del genere posso comportare danni ingenti per il business di un’azienda.

Pertanto è consigliato:

- Tenere aggiornati tutti i software presenti e farlo con tempestività.
- Eseguire backup ad intervalli regolari dei componenti critici
- Avere una rete sicura attraverso l’implementazione di IPS/IDS, WAF, FIREWALL, PROXY.
- Risorse Hardware adeguate, al fine di fronteggiare eventuali DoS e DDoS, anche grazie all’utilizzo del Load Balacing.
- L’utilizzo della virtualizzazione, al fine di rimpiazzare velocemente le macchine virtuali compromesse.
- Sanare l’input dell’utente nelle WEB APP
- Essere sempre aggiornati sugli exploit e minacce presenti attraverso fonti accreditate
- Formazione dei dipendenti al fine di evitare attacchi di tipo Social Engineering

Seguendo questi consigli, si può diminuire drasticamente la probabilità di subire compromissioni dei sistemi.