Armando Battaglino
23/12/2022

Week 9 - TEST Settimanale

Analisi dei Log

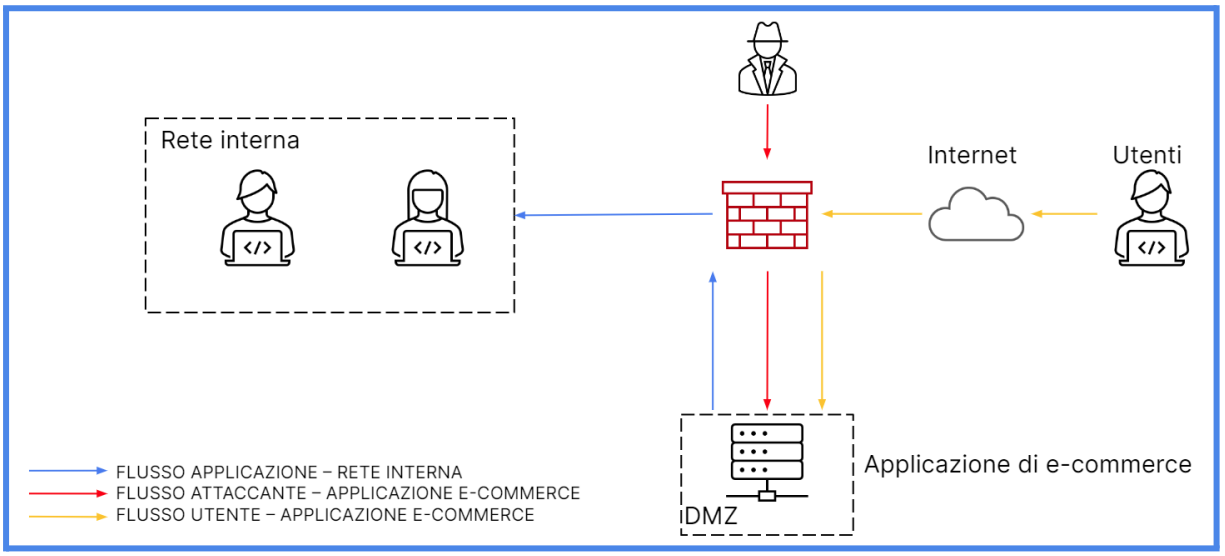
Consegna

Traccia:

Con riferimento alla figura in slide 2, 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
1. **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.
1. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

Procedimento



SQLi è una tecnica di hacking che consiste nell'inserimento e nell'utilizzo di codice SQL non previsto all'interno di applicazioni web per accedere ai dati del database.

AZIONI PREVENTIVE

Per prevenire questo tipo di attacchi, ci sono diverse tecniche che possiamo utilizzare, come ad esempio:

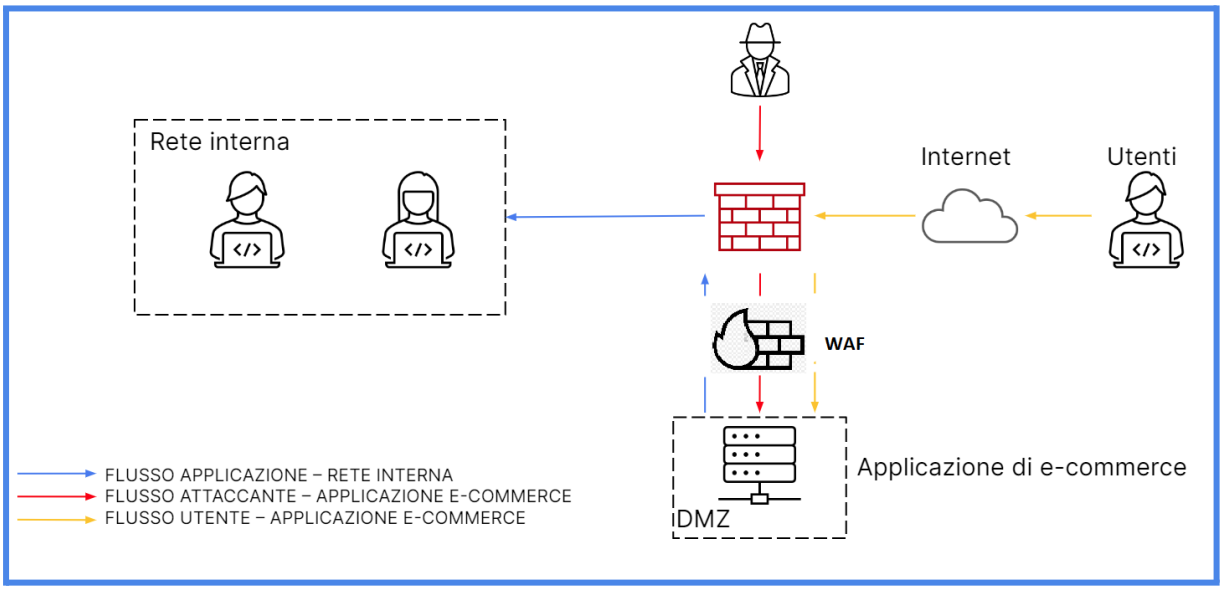
1. **Il Web Application Firewall (WAF)**
   Il WAF protegge le applicazioni web dai danni causati dagli attacchi, tra cui l'iniezione di codice. Il WAF protegge le applicazioni web monitorando e bloccando qualsiasi traffico HTTP/HTTPS dannoso che si dirige verso la nostra applicazione web e impedisce la fuoriuscita di dati non autorizzati. Il WAF applica una serie di criteri che possono essere personalizzati in base alle esigenze della nostra applicazione web. Il WAF analizza le comunicazioni prima che raggiungano l'applicazione o l'utente.

2. **Blocco dei caratteri speciali in input**
   Questa tecnica consiste nell'utilizzo di query parametriche con lo scopo di porre limitazioni al contenuto di alcuni campi, come ad esempio l'input di testo (come username), la password, l'indirizzo email e il textarea. In fase di scrittura del codice, è possibile bloccare caratteri come gli apici, i simboli speciali o gli spazi, che vengono utilizzati nell'iniezione di codice malevolo.

In questo caso, ci concentreremo solo sulla prevenzione tramite WAF. Il grafico qui sotto mostra come si può evitare un attacco al nostro e-commerce tramite azioni preventive utilizzando un WAF.

Come si può notare, il WAF viene inserito in modo tale da controllare e analizzare le comunicazioni prima che raggiungano il nostro sito e, in base ai criteri preconfigurati, l'attaccante non avrebbe accesso al nostro e-commerce in caso di tentativo di attacco SQLi. Con questo, il WAF rappresenta una barriera di protezione cruciale per garantire la sicurezza

della nostra applicazione web e dei dati ad essa associati.



IMPATTI SUL BUSINESS a seguito attacco DDoS

Supponiamo che la nostra applicazione web sia vittima di un attacco DDoS, ovvero un attacco che mira a rendere la pagina irraggiungibile per i clienti mediante l'utilizzo di enormi volumi di traffico e saturando la banda di comunicazione. Questo tipo di attacco ha come obiettivo quello di rendere il sito non raggiungibile con lo scopo di causare perdite economiche all'azienda target.

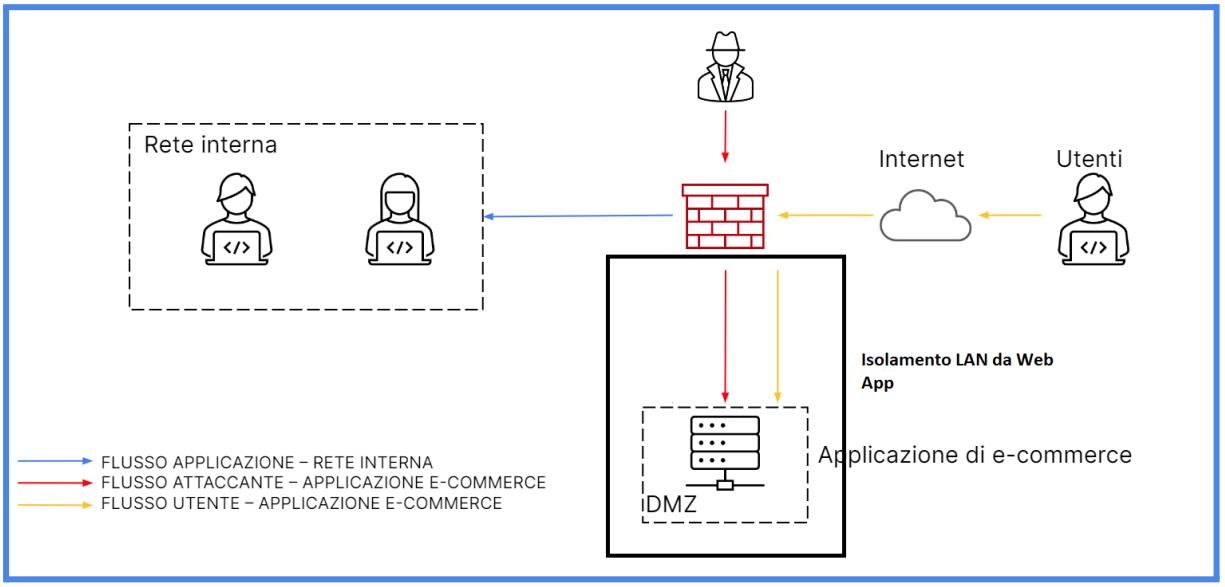
Considerando che in media ogni minuto gli utenti spendono 1500€ sulla nostra piattaforma, possiamo calcolare l'impatto sul business come segue:
Spesa media utenti per minuto = 1500€
Tempo di non raggiungibilità della web app = 10 minuti 1500 x 10 = 15000€

RESPONSE a seguito attacco Malware

Abbiamo subito un attacco Malware e vogliamo evitare che si propaghi alla nostra rete.

A questo punto inizia quindi la fase di **contenimento**, **eliminazione** e **recupero.**

Il primo passo da compiere è **isolare** la web application dalla LAN rimuovendo la regola di routing che mette in comunicazione la nostra LAN con la DMZ. Inoltre, lasciamo aperte le connessioni in ingresso degli utenti-clienti in modo tale che l'e-commerce possa continuare la sua attività ed allo stesso tempo abbiamo la possibilità di studiare i comportamenti del malintenzionato.
Inibire l'accesso agli utenti sarebbe inutile, poiché una volta entrati, l'attaccante avrebbe già il controllo sull'intero database. Questa azione è efficace solo se il malware è stato appena rilevato e non ha ancora compromesso il servizio. In caso contrario, bisogna isolare completamente la web app anche dalla rete internet per risolvere l'attacco.



SOLUZIONE

Viene proposta una soluzione definitiva unendo la difesa da attacchi SQL Injection o XSS alla difesa dalla propagazione del Malware. Come si può vedere, l'attaccante si trova bloccato dal firewall che nega l'accesso alla web app. Noi, come rete interna, possiamo accedere direttamente al sito senza passare tramite la rete internet, mentre l'utente può accedere tranquillamente al sito poiché il suo traffico non è riconosciuto dal firewall come dannoso.

Sarebbe inoltre saggio implementare anche degli **IDS** e **IPS** come metodo di prevenzione e monitoraggio della rete.

Infine è ottimale apportare degli interventi di **Hardening** e **Patching** dei sistemi e delle configurazioni.