PROGETTO M5 GELOSA MATTEO

AZIONI PREVENTIVE

Per implementare efficacemente la sicurezza contro eventuali attacchi XSS o SQL Injection, è essenziale seguire alcune azioni cruciali:

1. Validazione e Sanitizzazione dei dati di input:
La validazione implica l'applicazione di regole precise sull'input dell'utente. Ad esempio, per un indirizzo email, è fondamentale verificare la presenza di "@" mentre per un numero di telefono, solamente cifre. Ciò aiuta a controllare il formato dell'input e limitare i dati inseriti per evitare buffer overflow o attacchi DoS.

La sanitizzazione, invece, consiste nel filtrare i caratteri speciali come ">" "<" ";" "&" che potrebbero essere utilizzati per codice malevolo attraverso un attacco di injection o XSS.

2. Utilizzo di tecniche di codifica per l'URL:
È consigliabile codificare i dati trasmessi via URL per proteggerli durante la trasmissione, riducendo il rischio di manipolazioni malevole.

3. Aggiornamenti tempestivi e patch:
È fondamentale applicare tempestivamente patch o aggiornamenti non appena diventano disponibili per il web server, il sistema operativo o il database. Mantenere sempre il software aggiornato garantisce che le vulnerabilità note vengano corrette e rimosse, riducendo così la superficie di attacco potenziale.

4. La parametrizzazione delle query SQL è essenziale per evitare attacchi di SQL Injection. Quando costruiamo le query, dobbiamo evitare di concatenare direttamente i valori forniti dagli utenti, poiché ciò può renderci vulnerabili. Invece, dovremmo usare parametri e passare i valori separatamente per proteggere il sistema. Ad esempio, nelle query preparate in PHP e MySQL, sostituiamo i valori con segnaposti e li passiamo separatamente per evitare attacchi.

IMPATTI SUL BUSINESS

Per stimare il danno economico a seguito dell'attacco DDoS ho fatto il seguente calcolo:
Durata Attacco * Guadagno Per Minuto = 1.500*10 =15.000€.

Le azioni preventive che si possono mettere in atto in questo caso possono essere:

Diramazione del traffico su più server, in questo caso si ha una gestione del traffico più uniforme e nel caso un server andasse offline i rimanenti possono comunque erogare il servizio.

Monitoraggio della rete, eseguito in modo costante permette di verificare anomalie e tutte le attività presenti sulla rete.
In questo caso si può intervenire tempestivamente in caso di attacco DDos.

Backup, essenziale per conservare i dati più critici dell'applicazione per far sì di essere in grado di ripristinare i servizi nel minor tempo possibile.
I backup si possono anche caricare su infrastrutture esterne come ad esempio ColdSite, HotSite o DRaaS se il problema ha un tempo di risoluzione molto alto. Questo permette di mettere operativo il servizio finché l'applicazione principale non viene sistemata.

Utilizzo di software anti DDoS, per proteggere da attacchi DDoS, utilizzare software come Cloudflare, hardware come dispositivi di mitigazione DDoS per rilevare e bloccare il traffico dannoso in tempo reale, garantendo che il servizio rimanga disponibile.

RESPONSE

In questo caso la priorità è non far propagare il malware nella rete, e dunque mettere l'applicazione infetta in isolamento.
La soluzione può essere:
Utilizzo di una rete virtuale o un segmento di rete separato: Creare una rete separata o utilizzare una rete virtuale per mettere l'applicazione infetta in isolamento dal resto della rete. In questo modo, il malware sarà confinato all'interno di questo ambiente controllato e non potrà propagarsi ad altre parti della rete.

Configurazione di regole di firewall: Implementare regole di firewall specifiche per impedire al malware di comunicare con altre macchine sulla rete. Questo aiuta a bloccare qualsiasi tentativo del malware di diffondersi oltre l'ambiente isolato.

Implementazione di monitoraggio continuo: Mettere in atto un sistema di monitoraggio costante per rilevare qualsiasi tentativo del malware di propagarsi oltre l'applicazione infetta. Questo monitoraggio permette di intervenire prontamente nel caso in cui il malware tenti di aggirare le misure di isolamento.